IAEA-TECDOC-550

SAFETY OF NUCLEAR INSTALLATIONS: FUTURE DIRECTION

PROCEEDINGS OF AN INTERNATIONAL WORKSHOP
ON THE SAFETY OF NUCLEAR INSTALLATIONS
OF THE NEXT GENERATION AND BEYOND
SPONSORED BY THE
INTERNATIONAL ATOMIC ENERGY AGENCY
AND THE
GOVERNMENT OF THE UNITED STATES OF AMERICA
THROUGH ARGONNE NATIONAL LABORATORY
AND HELD IN CHICAGO, 28-31 AUGUST 1989

A TECHNICAL DOCUMENT ISSUED BY THE
INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1990

SAFETY OF NUCLEAR INSTALLATIONS: FUTURE DIRECTION
IAEA, VIENNA, 1990
IAEA-TECDOC-550
ISSN 1011-4289

Printed by the IAEA in Austria
April 1990

FOREWORD

The burning of fossil fuels is a major contributor to the present global warming, the rising of sea levels, and the acidification of the environment. Although scientific understanding of the far-reaching impacts of these phenomena is incomplete, there is agreement that the continuation of current trends could have highly deleterious effects on human health, food production, and global ecosystems.

Ultimately the core of the debate about how to reduce atmospheric levels of CO_2 and other greenhouse gases centers on issues of energy policy. Among preventive responses, international recommendations call for greater energy efficiency and an increasing share of non-fossil energy sources in the total energy mix.

Among the various energy technologies which are currently in commerical use, nuclear fission is relatively safe and environmentally benign; if deployed on a large scale, it can contribute significantly to reducing fossil-fuel based emissions and the associated environmental risks. As has been the case for other technologies, the future deployment of nuclear energy may be expected to be accompanied by an evolution in safety levels.

The workshop provided a timely international forum for exploring safety characteristics both for nuclear power reactors and the nuclear fuel cycle as well as means for improving the public's attitude towards nuclear energy.

EDITORIAL NOTE

CONTENTS

SAFETY OBJECTIVES (Session III)

Panel presentations

SAFETY OBJECTIVES (continued) (Session IV)

Panel presentations

SAFETY ASPECTS OF THE NEXT GENERATION OF CURRENT-TYPE NUCLEAR POWER PLANTS (Session V)

SAFETY ASPECTS OF NEW DESIGNS AND CONCEPTS FOR NUCLEAR POWER PLANTS (Session VI)

SPECIAL SAFETY ISSUES: SAFETY ASPECTS OF NEW DESIGNS AND CONCEPTS FOR NUCLEAR POWER PLANTS (continued) (Session VII)

SAFETY ASPECTS OF NEW DESIGNS AND PROCESSES FOR THE NUCLEAR FUEL CYCLE (Session VIII)

Panel presentation

CLOSING PANEL

POSTER PRESENTATIONS

OVERVIEW OF THE WORKSHOP

J. Anderer

Division of Nuclear Safety
International Atomic Energy Agency
Vienna

The Window of Opportunity

From the discussions at the workshop it was clear that most experts expect nuclear power to be deployed globally on a larger scale over the next few decades. Several explanations were given for this cautious optimism.

Many believe that the increasing concerns voiced by scientists, politicians and the public about fossil fuel combustion and the threat to the environment posed by climate warming, stratospheric ozone depletion and acid rain have prompted these groups to think again about the circumstances under which nuclear power might be part of an environmentally sustainable energy strategy. Others argue that the accelerating demand for energy and for electricity in particular, together with increasing societal awareness of the economic and lifestyle problems associated with every significant source of energy service (energy efficiency inclusive), will gradually lead people to opt for an energy mix that includes nuclear power.

For its part the nuclear power community has recognized the international dimensions of nuclear safety, putting in place a wide range of international agreements for accident notification and emergency response, and for broad information exchanges to enhance the safety profile of nuclear power now and over the coming decades. Gradually, the community is acknowledging the importance of properly addressing the concerns many people have about the health and environmental impact of radiation exposures associated with the varied uses of nuclear technologies.

Even so, the key question hanging over the nuclear community is whether it will be able to treat the current window of opportunity to (re)build broad public confidence in nuclear technologies as safe, well-regulated and non-detrimental to human and environmental well-being. While the challenge of the 1980's was to ensure technologically the safety of nuclear power installations, the challenge of the 1990's will be to prevent societal rejection of nuclear power, an essential energy source. How the nuclear community could respond to this new challenge was at the core of the workshop discussions.

The Need for Nuclear Power: A Quantitative Perspective

The 1989 Jülich CO_2 Reduction Scenario for the Year 2030 developed by scientists in the Federal Republic of Germany offered a perspective on the magnitude of a possible future supply role for nuclear power in a global energy system constrained by internationally recommended reduction targets for carbon dioxide and driven by the forces of population and economic growth. While the scenario exhibits a number of features deemed impossible in today's terms, provocatively it addresses the question: how impossible is the "impossible". To this end, it assumes a shift towards the uses of hydrogen-rich fossil fuels, of recycled biomass and non-carbon alternative energy sources, of nuclear power, as well as the introduction of significant energy conservation.

The scenario findings point to an increase in the global contribution of nuclear power mainly for electricity generation but also for high temperature process heat. Expressed in terms of total installed capacity, this would require the operation of some 2000 power reactors (each 1000-megawatts) by the year 2030 -- an increase by a factor of six over the existing installed capacity. Should all optimistic assumptions about supply from non-nuclear/non-carbon primary energy sources not materialize, the nuclear contribution would be even higher.

The expansion of the nuclear generating capacity along such lines would have major implications for the nuclear fuel cycle, such as the ratio between breeder-type reactors and burners, reprocessing capacities, and resource requirements. As a yardstick, the operation of some 2000 power reactors would necessitate an increase in the number of nuclear waste disposal facilities at the approximate rate of one facility per year indefinitely. Without the use of breeder-type reactors, by the year 2030 the amount of plutonium requiring storage could be in the broad range of 1000 tonnes. Accordingly, safeguard procedures would have to be re-evaluated.

The findings of other energy demand scenarios considered -- extending to the year 2060 -- were essentially in accord with the above supply pattern painted for nuclear power over the coming decades.

Demonstrating Safety

Substantially expanded use of nuclear power would call for a correspondingly higher level of safety at all nuclear fuel cycle installations worldwide. The reason for this lies partly with the large increase in the number of facilities and partly with societal expectation of lower risks for all nuclear technologies. In keeping with the theme of the workshop, attention focused primarily on safety issues associated with nuclear power production.

The expert consensus was that existing nuclear power plants are safe, although not all plants have as of yet met in full detail the basic safety principles for nuclear power plants established by the IAEA's International Nuclear Safety Advisory Group (INSAG) in its pioneering report known as INSAG 3. There was also broad consensus that, in line with the above arguments for higher safety levels, the next generation(s) of nuclear power plants would have to be "demonstratively safer" in the eyes of the owner utilities, regulatory bodies, politicians, and the public. The challenge of demonstrating safety would call for concerted action at both the technological and institutional levels.

For summary purposes, technological developments applicable to nuclear power plants have been broadly classified into the following three groups. While such groupings are convenient for discussion, in practice it is difficult to make such clear-cut distinctions, particularly for evolutionary and innovative reactor designs.

The first group comprises the current generation of operational nuclear plants or those under construction. These are characterized by large-sized power reactors of various types which exploit the benefits of widespread operational feedback for improvements in safety and performance.

The second group is made up of evolutionary reactors which represent modifications of current reactor designs and which could be available in the near term. These include pressurized water and boiling water reactors that achieve an enhanced margin of safety generally through lower power densities, smaller size and simplier design features than current ones, as well as through passive safety systems such as gravity and heat convection for delivering emergency coolant to the core and for containment cooling in the event of an accident. Also included in this group are the modified designs of the liquid metal fast reactor (LMFR) being developed, for example, in France, Japan, the Soviet Union and the United Kingdom. Generally, these evolutionary reactors rely on proven components and systems.

The third group consists of advanced reactors characterized by revolutionary or innovative designs, which might show promise after a longer period. The reactor concepts that drew the most attention were the advanced modular high temperature gas-cooled reactor (MHTGR) systems being developed in the Federal Republic of Germany, Japan, the Soviet Union and the United States; the Swedish process inherent ultimate safety (PIUS) reactor based on the principle of entirely passive safety systems; and the mid-sized innovative power reactor inherently safe module (PRISM) being developed in the United States. Most of these advanced reactor concepts are modular designs that would promote engineering and manufacturing simplicity, economy, and demand-response flexibility. By their very nature, these advanced reactors are not proven by testing and experience, and it will be many years before applicable safety analysis, experiments, codes and standards become available. As design work continues and additional designs are proposed, the open question is whether existing safety criteria would cover all features of the new designs or whether more stringent criteria will be necessary to handle issues raised by these advanced technologies. One possible implication of the INSAG-3 report would be the need for prototype testing of new reactor designs before regulatory approval and utility commitment. Indeed, the proponents of these revolutionary reactors face a dilemma: designers need funding now, which may be difficult to obtain until funders have greater confidence that innovative reactor designs can meet stringent safety criteria.

The importance of the defence-in-depth strategy for achieving international safety objectives at all nuclear power plants was underscored. The subject of maintaining containment integrity -- the last safety barrier in a defence strategy -- figured prominently in the discussions of safety targets for limiting significant environmental releases of radioactivity and the concurrent need for off-site emergency response. Several countries reported progress in the development of sturdy containment systems capable of maintaining their function even in the event of hydrogen detonation, steam explosions or other causes of extensive overpressure. Many of these developments would also apply to breeder-type reactors.

There was strong support expressed for the use of probabilistic safety assessments (PSAs) in defining safety issues for the next generation(s) of nuclear plants, especially with methodological advances in human reliability assessments and in treating common-cause failures and uncertainties of external events. The example was given of how the combined application of deterministic and probabilistic safety analyses has promoted design consistency for the new European Fast Reactor (EFR) project and also allowed for flexibility in response to different national safety requirements.

At the institutional level the goal of higher safety levels for future nuclear installations would require an even firmer commitment to safety on the part of the "safety culture" -- the designers, manufacturers, operators, maintenance personnel, regulators and the host of other professionals whose work bears directly or indirectly on the safety of nuclear power plants. Education and training were considered the key to this all-pervasive safety thinking, so that the strategic planning of training programmes was strongly endorsed, not only for maintaining existing skills and capabilities but also for meeting the anticipated heavy demand worldwide for qualified personnel at nuclear power plants.

Irrespective of these developments, the participants agreed that the best strategy for gaining utility and regulatory acceptance of the next generation(s) of nuclear power plants should be a consistent global trackrecord of safe, reliable and cost-effective operation of today's nuclear power plants. In contrast, the strategy for gaining public acceptance would have to go beyond these criteria.

Building Public Confidence

From the discussions it was evident that members of the nuclear community are well aware of the problems frustrating a constructive dialogue with the public about the future of nuclear power and are bent on resolving these. Less clear is how to (re)build the confidence of an increasingly skeptical public in the uses of nuclear technologies.

The nuclear industry's communication effort has often been guided by utility organizations, which in many countries operate both nuclear facilities and coal-fired plants. Thus many of these organizations have adopted a rather delicate approach to informing the public about the relatively high health and environmental risks posed by coal combustion and the use of coal by-products.

The technical jargon of nuclear specialists has served as a barrier to communication with the public. Frequently, terms used to describe safety improvements for nuclear power plants, such as "inherently safe", "walkaway safe" and "transparently safe", have been misinterpreted by most of the public who are not well-versed in this terminology. When used indiscriminately, these terms have painted a negative picture of the safety performance of today's plants and held out the promise of a "perfectly safe" or "zero risk technology" that is impossible for any industry to keep, no matter how far it goes in its safety pursuits.

The well-intended use of PSA findings as a vehicle for communicating the safety message to the public has been largely counterproductive. Based on their experiences with communication on nuclear issues, several participants reported that people want reliable and comprehensible information about what is being done to prevent accidents and to respond to a radiological emergency, not bland statements about the mathematical improbability of occurrence. Indeed, the severe accidents at Three Mile Island and Chernobyl represent the improbable actually happening, for which the consequential environmental impacts and mitigating measures taken have mattered most to people. For many participants, the practical answer to the public's question of "how safe is safe enough" would depend on whether the institutions involved could foster confidence in their ability to manage an accident and mitigate its consequences, and not on any quantitative assurance derived from safety assessments.

To (re)gain credibility and trust, the nuclear industry will also have to properly address people's misconceptions about the radiobiological and radioecological impact of nuclear power, and nuclear accidents in particular. In effect, the realities of the radiation environment must become part of the public consciousness.

Towards a Higher Radiation Literacy

Many people, and even some scientists and engineers, were believed to lack a broad picture of radiation as an inherent part of life, one that encompasses the patterns and magnitudes of exposure, the defined radiobiological risks, and the tangible benefits from the seemingly unlimited uses of radiation. And yet, paradoxically, people have always lived in a radiation environment. The paradox extends further: nuclear power, a negligible contributor to the average dose of radiation people receive, is the target of most public concern, whereas radiological medicine, the largest and increasingly most common man-made source of radiation exposures, is calmly accepted for its acknowledged benefits. There is even less public apprehension about the most prodigious and least controlled sources of exposures, such as the naturally occurring radionuclides in soils and dwellings.

A proposal was made for accelerating the communication process about the realities of the radiation environment through a concerted international effort. Three complementary objectives were advanced that would provide an informed basis for individual and collective decisionmaking about a given rdiation practice. First, low-level radiation should be viewed as a fact of life. The second objective would be to help people understand that the real impact of low-level radiation on human health and the environment is so minor that it should have little relevance for the individual and society as a whole. This may require acknowledging that the current costly philosophy governing radiation safety decisions is not necessarily the best for the public interest.

The third and most encompassing objective would address the comparative health and environmental impact of nuclear power along with those of its viable altenatives. It would require demonstrating that while nuclear power in normal operation is environmentally benign, this is not so for the alternatives. Specifically, it would address many people's excessive anxiety about a nuclear accident by showing that the real consequences of a severe accident are tolerable both in terms of health effects and environmental contamination and the resultant need for evacuation and relocation.

For its part, the International Atomic Energy Agency is seriously considering a new activity devoted to radiation acceptability, an area not yet properly explored at the international level. A first step would entail establishing an advisory group on radiation acceptability composed of credible scientists and scientific communicators who would openly and comprehensibly explain risk-related statistics and comparisons and aid in the formulation of practical radiation safety principles. Their work could help lay the foundations for a major international conference on radiation, health and society. A profitable second step would have this group, with some haste, reassess the past and on-going suitability of the radiation safety response to the Chernobyl accident, within the framework of a fuller and more comparative view of the effects of low level radiation, with the full benefits of hindsight. A new IAEA programme on comparative assessments of nuclear power with alternatives aims to establish a reliable and authoritative repository of information on the health and environment risks posed by the total cycle of the global energy system.

OPENING SESSION

INTRODUCTORY REMARKS

M. Rosen

Division of Nuclear Safety
International Atomic Energy Agency
Vienna

I am pleased to welcome you to this meeting sponsored by the IAEA and the Government of the USA on the safety of tomorrow's nuclear installations. The topic is exceedingly relevant for the ongoing examination of energy sources which can preserve our environment. Any subject touching on the environment is an especially "in" topic. A major meeting a week worldwide is one of the current reactions to the acknowledged environmental crisis.

I could spend the brief minutes of this introduction focussing on the Agency's current and future involvement with nuclear power and environmental issues, some of which are already visible and others of which will grow. The Agency being the specialized inter-governmental body whose statute requires it to both promote and ensure the safety of nuclear energy, is at the core of many efforts in safety, radiation protection, waste management and advanced reactors. But as I will touch on several of these activities in my presentation later today, the next few minutes are better spent on what I perceive as the real challenge for this meeting.

For nuclear power to be a viable energy source, the safety goals and safety designs you will propose must not only be technologically sound, but must also be a basis for public acceptance. Convincing the public of nuclear power's acceptability is the challenge. Convincing many of you in this audience, that a continued and expanded use of nuclear power can contribute significantly to reducing destructive emissions which are damaging our earth and its atmosphere, is not the challenge. The Programme document you all received states the benefits of nuclear power with conviction. It supports nuclear power by accenting the view that among the various energy technologies currently in commercial use, it is relatively safe and environmentally benign.

But, I ask you, if nuclear power is so safe and so clean, why is it so difficult to convince the public? A survey of the world situation gives us a picture of nuclear power which is bleak, whether it is due to increased energy efficiency, lack of demand, over building, regulatory delays or the skillfulness of the opposition. With some possible exceptions, perhaps the

UK, France and several CMEA countries in Europe, along with a few Asian countries, the nuclear lights are dimming almost everywhere. Nuclear power has stagnated and some phase out plans are set to become reality. There is now little nuclear light at the tunnel's end, except for the true believer.

This workshop should face reality. As you proceed to examine the basic objectives and safety concepts that could underlie a future large-scale deployment, keep in mind the questionable nature of the future, a future which is unclear, unless we regain the confidence of an unsure and unwilling public.

During the next four days you will discuss safety features that will certainly enhance the safety profile of nuclear energy. If we scan our programme we see the evidence of these serious efforts to further safety. They will be explored at length by this high level audience. But we cannot continue to speak solely to ourselves. We must make the effort to reach the public. My remarks this evening will focus on the unsure public, on the urgent need to convince them that nuclear power is not fundamentally unsafe, and on an appraoch to do this.

I am sure that all of us look forward to Thursday's final panel discussion which will tackle the question "Where Do We Go From Here?". The experience and knowledge in this audience undoubtedly can guide us towards the constructive direction.

SAFETY OF NUCLEAR INSTALLATIONS OF THE NEXT GENERATION AND BEYOND

J. Tuck

United States Department of Energy
Washington, D.C.
United States of America

Good morning ladies and gentlemen. I would like to thank Doctor Herbert Kouts for his gracious invitation. It is a pleasure to be here with you this morning to discuss how a new, safe generation of nuclear power plants can contribute to our energy security and environmental well being.

From an energy policy perspective, no available energy resource should be considered an unsatisfactory energy source. As energy demand increases throughout the world, we must consider all possible options while remaining conscious of the environmental, health and safety concerns facing us.

The United States Department of Energy is attempting, through the machanism of a national energy strategy, to explore all possible energy options, while paying close attention to the environmental ramifications of each resource. The national energy strategy will serve as a blueprint for energy policy and program decisions, and will guide the United States in achieving ample supplies of competitively priced energy in a manner sensitive to the environment, security and health needs of the American public.

Oil will probably continue to play a major role in our energy economies for many years to come. Indeed, oil will be utilized as long as it remains available at a reasonable price. However, for energy security reasons, we must attempt to reduce our dependence upon imported oil.

Natural gas use will likely increase. This clean and readily available fuel will fill some of the near term electricity needs and should do so in a manner suited to new environmental requirements. Additionally, the use of natural gas in the transportation sector will probably expand; displacing oil when economics and environmental concerns dictate.

Coal use also must increase as developed and less developed countries look for low cost and readily available energy alternatives. It is recognized that coal faces severe environmental challenges. However, the promise of clean coal technology should result in a new generation of efficient, clean and economic energy systems which will help meet the ever-growing demand for coal while satisfying environmental considerations.

The list of options extends well beyond fossil fuels. Conservation and renewable energy sources like solar, geothermal and hydroelectric will all play important roles.

Nuclear power, too, must and will play an important role in meeting our energy needs and environmental demands. We in the U.S. Department of Energy think that nuclear power will have a significant role in solving our energy needs in the future. DOE believes that we stand at the threshold of a new era of nuclear power. Nuclear power is, and can remain, the economically competitive, plentiful, clean alternative which will fulfill our energy requirements in the coming years.

International cooperation in nuclear safety is of the utmost importance in achieving satisfactory safety standards and performance on a worldwide basis. A serious nuclear accident anywhere is an accident everywhere, not only because radioactive fission products do not respect national borders, but also because the political fallout rains on every nation. The government of the United States stands ready to continue and extend its programs of international cooperation in nuclear safety in such areas as research, training, and information exchange. This was recently emphasized by President Bush during his remarks at The Karl Marx University in Budapest, Hungary.

To give a simple example of how interrelated the planet has become, consider the incident at Chernobyl. Just slightly less than two weeks after the explosion and fire at Unit Number 4 at Chernobyl, particles of radioactive fallout reached Atlanta -- about 10,000 miles away. And the political shockwaves engendered by Chernobyl are still reverberating throughout the industrialized world.

There are four elements related to nuclear energy that we believe must and will be settled before nuclear power can take its place as a clean and productive energy source for the next century.

First, it must be realized that the main concern for some within the industry is the question of what kinds of things must be done in order to secure plant life extensions. There are over 400 nuclear power plants in operation worldwide, and certainly we should concentrate at least some of our efforts on extending their life. Additionally, certain plants need to be modified to be brought into line with contemporary thinking on design safety.

I believe that the industry should use the opportunity provided by plant extension to discover how it can make nuclear power plants operate better. The industry could also use this opportunity to consider incorporating design features into the next generation of reactors to produced uncomplicated, straightforward plant designs.

Second, before nuclear power can enjoy a worldwide surge, the persistent question of waste management must be resolved. The fuel cycle must be closed in a manner that is satisfactory to the industry and, more importantly, to the general populace. Despite the fact that technical approaches are available to solve this problem, the nuclear industry still faces institutional obstacles, political obstacles, and obstacles related to the public's perception of risks associated with waste management. The demonstration of continued progress on the waste management would greatly enhance nuclear power's image for safety and reliability.

Third, we believe that the development and implementation of advanced reactor technologies is of the utmost importance. Advanced reactor systems offer the potential for significant improvements in safety through passive and inherently safe systems. They should also provide advantages in the realm of economics, and waste management. The technologies we are developing feature modular, factory-fabricated, standardized designs which enhance safety, provide for lower construction costs, improve quality assurance and give greater flexibility for utilities to meet load growth.

We think that three advanced reactor technologies are very promising. In the short-term, the most promising technology is the Advanced Light Water Reactor. It is expected that the passive, mid-sized Advanced Light Water Reactor designs will be available for deployment around 1995.

The next segment of the advanced reactor program centers on the Modular High Temperature Gas Reactor, which offers a unique containment approach featuring high temperature coated fuel particles providing a redundant and diverse barrier to the release of fission products under all conditions. The heat removal system is completely passive to assure no overheating of the fuel system.

We envision that what may be the most exciting technology, the Advanced Liquid Metal Reactor, will be moving steadily toward implementation early in the 21st century. The Advanced Liquid Metal Reactor has the unique ability to "burn" the longest lived nuclear waste, including recycled waste from light water reactors, thereby simplifying waste management and disposal. The development of this technology would reduce the highly radioactive life of stored waste from hundreds of thousands of years to hundreds of years.

An option related to this reactor design is the on-site location of the fuel recycle facility, where spent fuel is treated in a pyro-electric process, reclad, and recycled into the reactor again. The Advanced Liquid Metal Reactor is also unique in that it is the only reactor technology that can extend uranium resources if operated as a breeder reactor.

The Department of Energy believes that all three technologies could have a dramatic, positive effect on energy supply in the 21st Century. Each has its own purpose and timetable and each can make its own contribution.

Finally, despite all the technology, we must realize that it is the balancing of design features and the human factor which will determine the success or failure of the nuclear option. In places as different as the Soviet Union and the United States, nuclear power is suffering from a lack of credibility among the populace. The citizens have lost faith in the technical ability of the industry to manage the designs. Invariably, when dealing with nuclear energy the industry must be aware that the people operating the plant can complicate and in some cases retard the safety systems.

The industry should concentrate not only on improved design features, but also adhere to a high standard for skilled operators and alert and involved management. The industry should not tolerate complacency. The dominant factor in assuring safety is the human element involved in reactor operations. Demonstrated safety performance is dependent on people who are knowledgeable and skilled in their jobs.

Simply put, the role of human performance, both managers and operators, is the foundation of reactor safety, and therefore integral to the restoration of public confidence in the nuclear option.

Not coincidentally, when an operation is dedicated to safety and excellence in operations, and marked by competent managers and employees, it usually enjoys superior capacity factor performances.

The industry needs to reflect upon the possible vulnerabilities in the designs, especially as those weaknesses complicate, and are complicated by, human error. We should recognize the limitations of design and engineering in light of the human element. It is imperative that we take the necessary steps to balance the risks inherent in the use of nuclear energy. We need to conduct more probabilistic risk assessments and encourage critical self-examinations which identify possible problems, with both the engineering and the human factors, before they occur.

This is not something that can be regulated or legislated, it must come from a commitment by the industry. Organizations such as the Institute for Nuclear Power Operations and the World Association of Nuclear Operators are most helpful industry initiatives, but are no substitutes for individual attention to safety concerns.

For our part, the U.S. Department of Energy has recently announced a ten point plan for environmental protection and waste management activities at DOE's production, research and testing facilities. The Department's ten point plan is part of a series of strong actions designed to assure full personal accountability in the areas of environment, safety and health through changes in the departmental organization, management and contractual procedures.

CONCLUSION

It is imperative that a vital and thriving nuclear energy industry remains an important part of our energy strategy. With the resolution of plant life extension concerns, the satisfactory settlement of the waste management issue, and the promise and potential of the advanced reactor technologies coupled with increased attention to the human factor, nuclear power can be one of the best responses to the environmental uncertainties that face us.

INDUSTRY LEADERS AND MORE FACTS: WELCOME TO BOTH

A. Schriesheim

Argonne National Laboratory
Argonne, Illinois
United States of America

Ladies and Gentlemen, it is a pleasure on behalf of Argonne National Laboratory to welcome you to Chicago and to this Conference. Serving as a Host to the meeting is especially important to Argonne for a variety of reasons.

One is the prestige and the intellectual eminence of the attendees. Some of the best minds in the worldwide nuclear power community meet here to address key issues facing our industry. The future towards which Argonne research is directed lies in your hands.

In addition, we have an historically vested interest in this meeting. Argonne traces its' roots to the world's first nuclear reactor developed by Enrico Fermi. Developing advance nuclear power sources has been central to our operation from that time to this. Some of you and many of your staff were trained in nuclear science and technology through courses at Argonne as part of the ATOMS FOR PEACE initiative in the 50's and IAEA courses since then.

Argonne has a current vested interest in this meeting as well. We are now the nation's only full capability center for research and development of nuclear reactors. Our areas of expertise range from supporting basic research in chemistry, physics, and materials through design, safety, testing, and waste disposal.

And, as you will hear later in your meeting, we are developing one of the most promising concepts for an advanced liquid metal reactor, the Integral Fast Reactor. The theme of this meeting, "safety of nuclear installations of the next generation and beyond", represents our bread and butter.

Actually, Argonne has a broader mission. But it too coincides with the agenda of this meeting. Our concern includes operating safety and the prevention of harmful by-product release for a variety of energy sources.

Specifically, we have been concerned with the combustion of fossil fuels, how emissions are transported, how they are chemically converted in the atmosphere, and how they affect life forms and structures. Greenhouse effect, ozone, CO-2, and acid rain, have been the focus of our research efforts for many years.

We are glad to host this Conference because it provides what the world most needs right now: more information.... more facts.... and less panic.

We in the nuclear community have paid a heavy penalty over the last ten years as the result of emotional, sometimes irrational attacks. Although the bulk of the world's population is not panic-stricken about nuclear power, the activist fringe element has planted enough doubt and generated enough political pressure to significantly slow the growth of our industry.

Now the public and the activists have become acutely aware that the primary alternative to nuclear power -- fossil fuels, especially coal -- have the potential for environmental damage which is not just theoretical, but is measurable.

I believe, along with the rest of you, that it is incumbent upon us to analyze objectively and scientifically the potential for environmental threats from fossil fuels....just as it is to study the risks and remedies involving nuclear safety. Injecting emotion into either of these topics is going to distort the results of our studies and the action plan that our governments will develop based on our results.

I recognize that in suggesting this, I'm going against conventional wisdom which holds that emotion is the best way to move people. We are told that we can't overcome emotion with fact. But I believe on the basis of Argonne's experience, that the public is ready for more factual information and less emotion.

Reaction to the reports that we have been putting out on the Integral Fast Reactor confirm my faith that this is true. The press, which is ostensively anti-nuclear, and the general public which is at least suspicious of nuclear, have responded positively and broadly to our announcements of test results.

These announcements go back three years. It was then that we demonstrated that our Breeder Reactor in Idaho, rigged in the Integral Fast Reactor configuration, shut itself down without human or mechanical intervention after we turned off the pumps while it was operating at full power.

When we announced that IFR fuel had reached a 19% burnup, and was still continuing under test, we again got very favorable results. And most recently when we described the capability of the IFR to consume its own high level waste as fuel, that information was broadly and positively reported in the press. We take this as evidence that the public is conscious that it faces difficult energy choices. The public is hungry for information on which to base those decisions.

This does not mean the anti-nuclear activists are going be any less fanatical. But they have been beating on the same drum for nearly two decades. I believe that opinion leaders and the general public have become sophisticated to their scare tactics -- especially when they can be contrasted with credible scientific facts.

Those scientific facts and economic realities are driving us toward a more important role for nuclear power in the broad portfolio of energy options to meet our needs. We haven't achieved broad general recognition of that trend yet. But conferences like this one are advancing us....one patient step at a time....in that direction.

That is why we are pleased and proud to serve as your Host for this meeting. Again I want to thank you for coming and welcome you to Chicago.

ENVIRONMENTAL IMPACT OF FOSSIL FUEL ENERGY TECHNOLOGIES

(Session I)

Chairmen

A. GAUVENET
France

W. LOEWENSTEIN
United States of America

THE GREENHOUSE EFFECT AND GLOBAL CLIMATE CHANGE

P. MOREL
WMO/ICSU World Climate Research Programme,
World Meteorological Organization,
Geneva

Abstract

The ongoing increase in the concentration of infrared-absorbing gases in the atmosphere is already causing and will continue to cause a growing unbalance in the radiation budget of the earth, and consequent warming of the lower atmosphere and earth surface. This climate phenomenon is the manifestation of the greenhouse or blanketing effect of absorbing gases (also know as "greenhouse gases") in the earth atmosphere. The main chemical species responsible for the build-up of the greenhouse effect are carbon dioxide, methane and chlorofluorocarbons (CFCs) or freons. Despite new regulatory efforts made by governments to slow down the emission of these gases, the combined atmospheric burden could be equivalent to doubling the pre-industrial concentration of carbon dioxide ($2xCO_2$) by the middle of next century. The global warming of the earth surface would eventually reach about 4°C if the $2xCO_2$ concentration then was maintained constant for a long period. As it is, the transient response of climate to an increasing greenhouse effect is delayed by 50 to 100 years. For this reason, we observe now a much smaller climate warming than would occur for climate equilibrium with the present atmospheric composition, i.e. 125% the pre-industrial concentration of CO_2. Impacts of this phenomenon will range from disturbances of the existing hydrological regime of the planet to rise of the global mean sea-level. A warmer atmosphere means more rain but also faster evaporation: consequences in terms of the availability of water resources are unclear at temperate and high latitudes, but an aggravation of aridity in sub-tropical latitudes is probable. Sea-level rise may reach 50 cm by 2100. In general, the rate of climate warming when the climate system starts responding to the greenhouse effect could be 0.3°C per decade, far exceeding the ability of natural ecosystems to adapt effectively to the change.

---

1. INTRODUCTION

If the emergence of the industrial civilization had occurred some 18,000 years earlier, a trivial length of time compared to the 3 million year history of man's evolution as a sentient being and even more trivial compared to geological time-scales, the present concern for inadvertent modification of the global environment by human activities would have been raised at the climax of the last glaciation of our planet. One could imagine that a similar conference would have together brought environmental scientists like myself and responsible experts on energy production. The meeting would have been held in some ice-age auditorium but not in Chicago, since the Great Lakes were at that time covered by a 3 km thick sheet of ice, and undoubtedly, the scientists would have warned the conference of the possibility of an impending climate change and its shocking consequences. They would have predicted that the annual and global mean temperature of the earth surface could rise by as much as 5°Celsius, changing climate everywhere and, in particular, making summer conditions in the American mid-west so intolerably hot as to force extensive and continuous use "air-conditioning" techniques to minimize discomfort to human beings. They would theorize that changing weather and rainfall could cause widespread desertification in sub-tropical regions and the death of vegetation in the Sahara. And even more dramatically, they would warn that the unavoidable retreat of the northern hemisphere ice-sheet would release enormous amounts of meltwater which would flow into the ocean, causing an unbelievable 120 m rise in global sea-level and generalized flooding of lowlands with incalculable loss of land and property. The interesting point is that these scientists would have been right: the climate change and sea-level rise did occur, not as a result of man's actions but as a consequence of natural change in the atmospheric concentration of carbon dioxide, related to as yet unknown geo-biochemical processes in the ocean and terrestrial vegetation. Thus, on can harbour no doubt of the reality of climatic changes and the effectiveness of atmospheric greenhouse gases, such as carbon dioxide, as causal agents of climate variations.

2. GREENHOUSE GASES

Many human activities, agricultural and industrial, cause the emission of increasing quantities of polyatomic molecules into the global atmosphere. As a result, the concentration of these chemical substances in the air has already risen substantially and continues to rise. Polyatomic molecules absorb the infrared radiation emitted by the earth surface and are therefore "greenhouse gases" which contribute to the overall greenhouse or blanketing effect of the earth atmosphere.

The best known and also the most important contributor to the augmentation of the greenhouse effect is carbon dioxide (CO_2). Figure 1

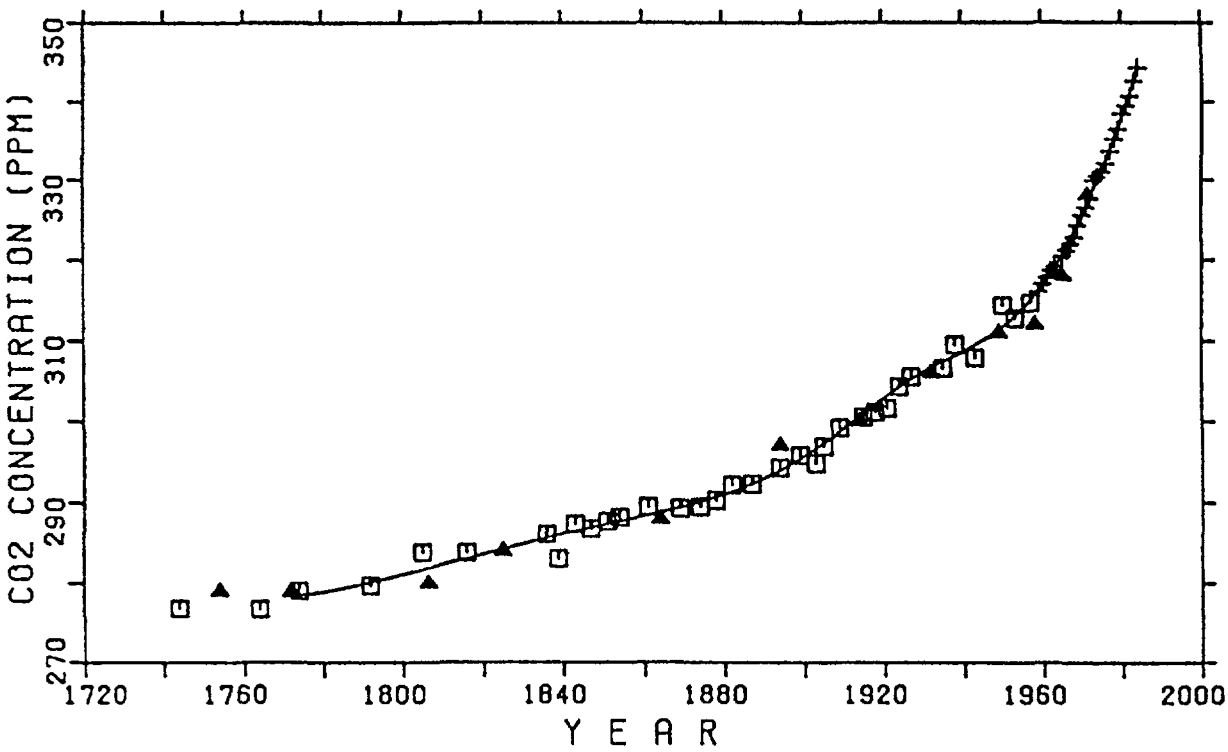


Figure 1. Concentration of carbon dioxide in the atmosphere, from the analysis of ice-cores (1745-1960) and direct measurements (1958-1985) according to Siegenthaler and Oescher (1987).

records the concentration of this gas over the period 1740 to 1980 (Reference [1]). The amount of CO_2 present in the atmosphere has already increased from about 280 ppm (parts per million) before the beginning of industrialization, to 350 ppm in 1988, and continues to rise at the rate of 1,4 ppm per year according to very precise measurements made at the Scripps Institution of Oceanography Mauna Loa observatory.

This annual increase corresponds to the addition of 3.3 gigatons (billion tons) to the total mass of carbon contained in the atmosphere in the form of carbon dioxide. This is to be compared to the current annual emission of 5.5 gigatons of carbon in CO_2 molecules produced by the combustion of fossil fuels, plus an extra amount of the order of 1 gigaton, resulting from the combustion or oxydation of wood and other biomass. Thus, we know that only a fraction, about 50% of the total amount of carbon dioxide released into the atmosphere, actually remains airborne. It should be emphasized that anthropogenic emissions and the corresponding annual increase of atmospheric carbon dioxide are but small increments of large fluxes exchanged between the atmosphere and the ocean or the land surface, which altogether exceed 200 gigatons of carbon per annum. Thus, relatively minor readjustments in the world ocean circulation and chemistry, or in the life cycle of terrestrial vegetation, could affect significantly the airborne fraction and the amount of CO_2 added each year to the atmosphere, even when emissions will be stabilized. In particular, ocean warming is likely to decrease the net uptake of carbon dioxide by sea water.

Furthermore, it is known that the atmospheric concentration of many other trace gases, all of which contribute to the greenhouse effect, is rising even more rapidly. Although their proportion by weight is very much smaller, several trace gases are much more effective absorbers of infrared radiation, molecule for molecule, than carbon dioxide. They will therefore contribute materially to the further augmentation of the greenhouse effect.

This is particularly true for methane (CH_4) and the various chloro-fluoro-carbons (CFCs), also known as freons. The concentration of methane has been rising steadily since several centuries, keeping pace with the increase of the world population. Methane is produced by the anaerobic decomposition of cellulose (i.e. vegetal materials) in wetlands, rice paddies and also in the stomach of cattle, and therefore related to the development of agriculture and animal husbandry. Freons, on the other hand, are strictly artificial substances produced by chemical industry: their sources are exactly known and can be controlled.

3. FUTURE TREND IN GLOBAL ATMOSPHERIC POLLUTION

Further trends in the concentration of CO_2 and other greenhouse gases can only be surmised. Proven reserves of fossil fuels are sufficient to allow pursuing extraction at the present rate for a long time, 30 years for oil and more than 200 years for coal, so that consumption will not be limited by the available supply. Furthermore, the exploitation of fossil carbon deposits is an essential component of the world economy: in 1988, 88% of all commercial energy production was based on the combustion of fossil fuels, the rest being provided by hydroelectric plants (7%) and nuclear reactors (5%). Emissions of methane (agriculture, animal husbandry) and nitrous oxide (fertilizers) are likewise linked to the expansion of the economy.

Rotty and Masters (reference [2]) report that, except for world wars and the Depression crisis, the consumption of fossil fuels (oil, gas and coal) has consistenly grown at the rate of 4.2% per year or more, from 1860 to 1973. Thereafter, the rate of increase of global annual carbon dioxide emissions has only been 1.5% per year, as a result of the rise in oil prices and the inception of a serious energy conservation drive in most industrialized countries. A study by the US Department of Energy (reference [3]) concluded that, in order to maintain carbon dioxide emissions by the USA at the level of 1985 (1.26 gigaton per year) until the year 2050, it would be necessary to achieve universal adoption of the best available techniques for energy conservation and energy efficiency and to accelerate substitution of fossil fuel electricity with nuclear and solar electric power for fossil fuel fired plants. Under all other more conservative scenarios, based on the USA Natural Energy Policy Plan, CO_2 emissions would continue to increase significantly. While the assumed rate of economic growth is the most significant determinant of CO_2 (and other greenhouse gases) emissions, it is by no means the only determinant. For example, a higher rate of economic growth makes possible the accelerated penetration of advanced, less polluting, technologies. On the other hand, slow economic growth and continuing population explosion may lead to increasing rates of deforestation.

One should be aware of the fact that the potential for further increase in global CO_2 emissions, as a result of growing energy use by less industrialized countries, is truly enormous. Only the most stringent policy decisions supported by substantial international assistance, could possibly abate the legitimate desire of these countries for accelerated development of their own industries and use of their substantial fossil fuel reserves, especially coal. The most obvious case is that of China, now the third largest source of CO_2 emissions in the world.

Altogether our present knowledge of the sources and sinks of greenhouse gases, and the assessment of the possible rates of emission consistent with known economic objectives and societal trends, indicate that considerable increase in the atmospheric concentration of most if not all greenhouse gases is likely to occur in the next century. Based on this knowledge, the greenhouse gases increase scenario adopted by the WMO/UNEP Intergovernmental Panel on Global Change, is leading to a total atmospheric burden equivalent to doubling the early 20th century amount of carbon dioxide present in the atmosphere (from 300 ppm to 600 ppm) by the year 2060 with $\pm$30 years uncertainty.

4. THE GREENHOUSE EFFECT

We know that the increasing concentration of absorbing gases in the air will cause a general warming of the lower atmosphere and the earth surface, and a compensating cooling of the upper atmosphere. This phenomenon, known as the greenhouse effect, is the result of a change in the transfer of radiation, whereby the earth's atmosphere absorbs and retains a larger fraction of the long-wave (infrared) radiation emitted by the earth surface, thus allowing the surface to be significantly warmer than would be true in the absence of absorbing gases. In the recent (pre-industrial) past, the greenhouse effect of the earth atmosphere had been due mainly to absorption by water vapour and carbon dioxide, and had produced a steady 33 degree Celsius warming of the earth surface temperature.

Well-established methods exist to compute the primary greenhouse effect, i.e. the net energy gained by the earth surface, for various specified distributions of absorbing gases in the atmosphere. These computations show that doubling the early 20th century concentration of carbon dioxide (from 300 to 600 ppm) would produce a net energy gain of about 4 Watt/m^2. One should understand that the increase in the greenhouse effect due to carbon dioxide and other greenhouse gases accumulated in the atmosphere since the eighteenth century, is already causing a significant unbalance of the mean global energy budget of the earth, about 2 $Watt/m^2$, in excess of that which has been the primary cause of quaternary climatic variations. On this account, we are already committed to a significant warming of the earth climate.

5. THE STEADY-STATE RESPONSE

The earth climate has changed only minimally during the last fifty years, certainly much less than could be inferred directly from the imbalance in the radiative energy budget. The reason is that the climate regime is controlled by a fast system and a slow system. The fast system is the atmospheric "heat engine" which drives the whole earth environment, by transforming the heat derived from the sun into kinetic energy, and determines the ultimate amplitude and geographical patterns of climate change. The slow system is the global ocean which sets the pace for climatic change and may introduce a delay of 50 years or more in the transient response of the earth's climate to greenhouse forcing. Interactions between the fast and the slow components are relatively sluggish because the upper-ocean layer, constituting a "warm water shell", sits on the colder and denser deep ocean water. The warm water is separated from the deep ocean by a sharp temperature gradient where vertical mixing is weak, except in some restricted geographical regions at high north and south latitudes where mixing penetrates down to the bottom of the ocean and "deep ocean water" may be formed or conversely rise to the surface. Consequently, the "ventilation time" necessary for properties to equilibrate between the atmosphere and the deep ocean, may be several decades or even centuries, depending upon the location within the world ocean circulation.

The studies conducted so far have, for reason of simplicity, ignored the transient behaviour of the full climate system and considered only the steady-state response of the fast climate system alone to switching-on different environmental conditions, e.g. doubling the concentration of atmospheric carbon dioxide. Even then under these simplified conditions, the steady-state climate response is complicated by a bewildering variety of re-adjustments which occur in the atmosphere and at the surface of the earth. These adjustments can be very complicated and constitute either positive or negative feedback loops, which amplify or conversely reduce the primary greenhouse effect. The combined result of these feedback processes is a considerable augmentation of the climatic response, i.e. a multiplication by a factor 2 to 4. This response affects all aspects of climate, and, first of all, the temperature of the lower atmosphere and earth surface. The effects vary according to geographical location and season, but the results can be condensed in a single characteristic number by taking the annual average over the whole earth, of the warming obtained after switching-on a doubled concentration of carbon dioxide.

Climate Model	Average Surface Warming
GFDL (1987)	4.0°C
GISS (1988)	4.2°C
NCAR (1984)	3.5°C
UKMO (1987)	5.2°C

The basic physical relationship between temperature and the saturation pressure of water vapour is such that a warmer climate entails a wetter atmosphere and thus a general increase in precipitation. On the other hand, a warmer climate causes faster evaporation. Existing model simulations lead to expect that the increasing greenhouse effect will exacerbate soil aridity and the depletion of ground water in the dry sub-tropical zone, but the sensitivity of hydrological processes upon many poorly determined factors is, at present, an insurmountable impediment against reliable computation of impacts on water resources. On the other hand, this very sensitivity is an indication that undesirable climatic impacts would be amenable to amelioration, at least in some regions, by appropriate management of soil hydrological properties and vegetation. A central component of the World Climate Research Programme is precisely aiming to elucidate these problems (Global Energy and Water Cycle Experiment).

Finally, it should be emphasized that even the general agreement obtained for global equilibrium-climate in recent model studies with a steady doubled concentration of carbon dioxide, may be more an indication of the state-of-the-art in atmospheric modelling than a real proof of accuracy. To illustrate this point we recall that a further development introduced by the UK Meteorological Office in the formulation of physical and optical properties of clouds in their climate model, has produced a drastically reduced estimation of global warming associated with a doubled CO_2 concentration, 1.9°C instead of 5.2°C.

6. PREDICTING THE TRANSIENT CLIMATIC CHANGE

If the fast system alone was involved in climate change, the response of the earth climate would follow essentially the increase in the primary

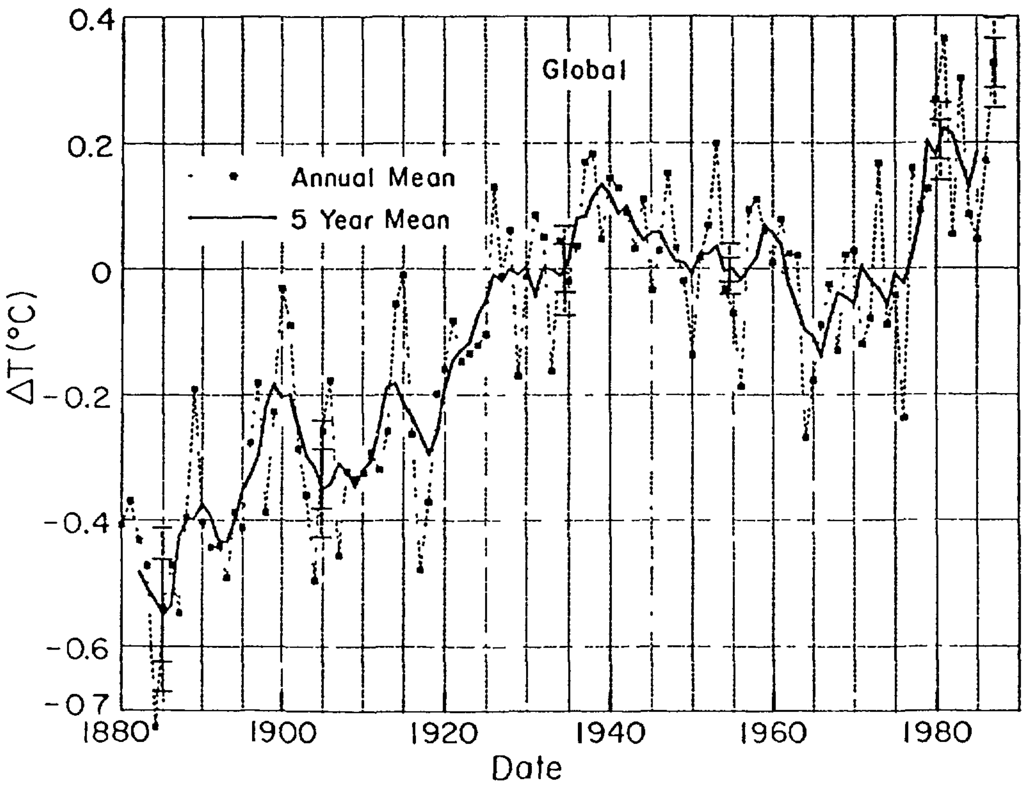


Figure 2 Mean annual global air temperature at the surface of the earth, according to Hansen and Lebedeff (1988).

greenhouse effect and we would already observe a substantial warming of near-surface air temperature, in excess of 1°C over the ocean and 1.5 to 2°C over land. Such a highly visible climatological change has not occurred yet, as demonstrated by Figure 2, showing a record of the global surface air temperature (over both land and sea) assembled by Hansen and Lebedeff (reference [4]). This record indicates a 0.6°C warming over the last hundred years. However, one will notice that most of the warming has occurred during the first fifty years of the period when the greenhouse forcing was actually too small to be counted as a probable cause. The global warming observed during the period 1940-1990 is only 0.2°C. In short, it is amply clear that the real world is behaving quite differently from the fast climatic response of a planet endowed with only a very shallow ocean.

In simple terms, the response of the slow climatic system is controlled by two basic parameters: first, the net flux of energy at the surface produced by a specified increase in the concentration of greenhouse gases and subsequent readjustments of the atmosphere and second, the heat capacity of the part of the global ocean which is effectively subject to warming over a period of several decades. The first quantity can be estimated from suitably designed numerical experiments with models of the fast system only (Bryan et al, 1988). The effective heat capacity of the system is determined by the diffusion of heat into the ocean, which can be inferred from the observed penetration of ^{14}C isotopes disseminated in the atmosphere during the mid-1950s series of thermo-nuclear explosions.

The combination of these two parameters yield a characteristic response-time for achieving a given fraction (e.g. 70%) of the computed global warming for steady doubled CO_2 conditions. This single number, called the e-folding time, indicates the delay of the response of the whole climatic system, compared to that of the fast component alone. The best estimates of this delay are in the range 50 to 100 years.

The evolution of the earth climate in the next fifty years will result from ongoing natural variations combined with a warming trend forced by the man-made modification of the atmospheric concentration of greenhouse gases. Natural variations are caused by the internal dynamics of the earth climate system, the atmosphere, ocean and ice. The warming trend is caused by the steady increase of the greenhouse effect. This warming is being delayed by the thermal inertia of the world ocan, but it will also continue long after the composition of the atmosphere is stabilized. No matter how drastic the actions taken to control the atmospheric burden of greenhouse gases, the global warming to which we are already committed will be realized in the next fifty to hundred years. Global environmental change is inevitable.

The greenhouse warming realized so far is still well within the range of natural variability and cannot be distinguished from natural variations. It is possible, however, that this threshold could be exceeded in the not too far future (10-20 years). The properties of the earth system are such that global warming can then be expected to proceed at a much faster rate, of the order of 0.3°C per decade, shortly after passing the threshold of detectability.

7. PREDICTING SEA LEVEL RISE

In past historical times, variations of the mean sea level in front of a particular shore have been caused mainly by local tectonic effects which force the land to sink or rise locally with respect to the global reference geoid, without much change in the mean ocean surface. The rapid increase in greenhouse effect and consequent climate warming is expected to cause, in the

21st century and thereafter, a global mean sea level rise which will result from an actual increase in the volume of the world ocean due to the addition of meltwater from mountain glaciers and polar ice caps, and also to the thermal expansion of sea water. The climate-induced global sea level rise could reach 50 cm by the end of the next century but this estimation is fraught with large uncertainties.

If all mountain glaciers and small inland ice caps were to disappear entirely and add their meltwater to the ocean, they would cause the global sea-level to rise by 33 cm only. On the other hand, the interplay between snow accumulation on the large ice caps and melting or iceberg calving, when the discharge of ice takes place in the sea, could in principle entail much more substantial excursions in global sea-level. Increased ablation is expected to dominate the ice budget of the Greenland ice cap, yielding a general decrease of the inland ice mass and a total of 13 to 26 cm rise in mean sea-level due to the release of meltwater during the next century. On the other hand, temperatures are and will remain well below freezing on Antarctica, so that melting can be altogether neglected. The ice budget of the Antarctic ice sheet is therefore balanced by snow accumulation and iceberg discharge in the ocean. Because the horizontal extent of the ice sheet is limited by the size of the Antarctic continent, its budget under warmer climate conditions will be dominated by more abundant snowfall and accumulation, yielding a thicker ice sheet and an attendant lowering of mean sea level, by - 20 to - 90 cm over the next century (reference [5]). For lack of more precise knowledge, one can conclude that various changes in land ice caps and mountain glaciers, due to a warmer climate, will largely compensate each other, or yield a small negative contribution to global sea-level change, until the year 2100.

The global ocean, on the other hand, has been storing energy since several decades and will continue to do so at an even faster rate during the next century as the greenhouse effect increases . The net heat gain by the ocean translates directly into global sea-level rise. Noting that the thermal expansion coefficient of sea-water is nearly uniform, one finds that the linear expansion of a water column will be independent of its depth and simply proportional to the total amount of heat stored in the column. With a reasonable estimate of about 3 Watt/m^2 for the hundred-year mean net energy gain by the global ocean during the next century, one finds that thermal expansion of sea water could produce a global sea-level rise of 40 cm by year 2100, and continue at essentially the same rate thereafter.

8. IMPACTS OF CLIMATE CHANGE

Many different forms of socio-economic impacts will undoubtedly result from a major readjustement of the earth climate, such as foreseen in the 21st century. Warm moist climates generally facilitate the spreading of airborne and waterborne communicable diseases, triggering faster reproduction and survival of pathogenic bacteria, viruses, parasites and their vector. Also, some ailments are directly related to warm weather, particulary cardiovascular diseases for which exposure to temperature above 27°C is regarded as critical. Thus climate change will have consequences on human health.

Likewise, changes in hydrological processes associated with greenhouse warming will affect agriculture and food production. But in such matters, climate is but one factor influencing the outcome: human health like crop yield are very much influenced by human management, societal behaviour and economic constraints. Extrapolations into the future concerning these complex matters have such a wide margin of uncertainty that it seems unprofitable to spend much time on them. Thus, one should turn to the two effects which could be most reliably foreseen among the wide range of potential impacts of the anticipated climate change: global sea-level rise and stress on natural ecosystems.

Sea-level rise brings several kinds of risks, the most obvious of which is the rapid loss of land to the sea. This is nothing new in human history. Many islands have disappeared altogether in the last 15,000 years, due to the melting of the northern hemisphere ice-sheet, and are now submerged seamounts. The Netherlands and south-east England are sinking at the rate of 25 cm per century, and the Dutch people have a long experience of building ever-bigger sea-defences. What is new is the prospect of considerable acceleration of the process with increased stress on coastal settlements and consequent economic losses. Most at risk are low lying tropical islands: a rise of 2 metres in sea-level would essentially submerge the entire 1,190 small islands which constitute the Republic of the Maldives. Low-lying tropical coasts are usually protected by coral reefs and mangroves. Both are already under pressure from human activities ranging from pollution, sedimentation due to improper land-use, dynamite fishing, cutting mangrove for fire-wood, quarrying coral blocks for construction, etc. The important factor is the ability of coral reefs to adjust to anticipated sea-level rise. Since the growth rate of coral is 30 to 60 cm per century in exposed locations and 80 to 150 cm per century in sheltered conditions, it would appear that low-lying coral atolls are in no immediate danger during the next century.

An engineering and economic survey of the Republic of Guyana, where most of the population lives in the low-lying coastal zone, showed that without a systematic programme for raising and strengthening coastal protection and improving drainage, greenhouse-induced sea-level rise could cause serious loss of agricultural land, agro-industry, housing and infra-structure. Rising sea-level also increases the intrusion of salt water into surface water systems and ground aquifers. The result can be the loss of agricultural capacity of the soil, and the need to expand water supply from elevated terrain. In the case of Guyana, there would be space enough to resettle the population inland. The situation could be far more critical in densely-populated, deltaic areas like Bangladesh. In such places, vulnerability to disastrous flooding cannot be isolated from the need for alternative livelihood to that provided by hazardous farming in the low-lying deltas.

A warmer climate is likely to be a wetter climate and the increased rainfall is expected to largely offset the effect of higher evaporation rates and even yield increased soil moisture at least at temperate and high latitudes, and possibly even in the equatorial forest, but increased aridity must occur in the already dry sub-tropics. Carbon dioxide is the raw material of the photosynthesis of vegetal matter and a carbon-dioxide rich atmosphere will be "more fertile". In other words, plants will be able to absorb the same amount of carbon with a less active respiration rate, with correspondingly reduced loss of water. This effect, augmented by judicious selection of water-efficient vegetal species could go a long way towards alleviating the water-stress on agricultural (managed) ecosystems. Unmanaged natural ecosystems, on the other hand, are geographically determined by the temperature and precipitation regime. At temperate latitudes, it can be asserted that a 1°C rise in mean air temperature can be offset - very crudely - by a meridional displacement of vegetation types or biomes 100 to 150 km towards the pole. At the projected warming rate of 0.3°C per decade, the required adjustment of 3 to 5 km per year would exceed the ability of tree species to adapt by natural migration, as they have obviously done in the past (we can deduce that spreading of natural vegetation into a new habitat takes place a maximum natural rate of 2 km per year, even for trees with light, wind-dispersed seeds). Thus, there is real danger that rapid warming could overstress the ability of natural ecosystems to adapt to climatic variations and cause widespread loss of living species in the affected ecosystems.

Altogether, direct human assault on natural life, such as widespread clear-cutting or burning of tropical forests, and indirect stress imposed by rapidly changing climate conditions, are causing the extinction of many living species, bacterial, vegetal or animal, at an estimated rate of one every half-hour. If these losses were to continue unabated, it would appear that the aggression of man against the global environment could cause the disappearance, within the span of one century, of 50% of all living species extant on the earth. Such devastation can only be compared with the catastrophic event, possibly the collision of a comet or a small asteroid with the earth, which occurred 65 million years ago and marked the end of the cretaceous period and beginning of the tertiary era, when the big dinosaurs and half of all other species known at that time became extinct. One can only hope, and do our personal best to ensure, that man fares better than the dinosaurs.

REFERENCES

[1] Siegenthaler, U. and Oeschger, H., Biospheric CO_2 emissions during the last 200 years reconstructed by the deconvolution of ice core data, Tellus, Vol. 39B, pp. 140-154 (1987).

[2] Rotty, R.M. and Masters, C.D., Carbon dioxide from fossil fuel combustion. Atmospheric Carbon Dioxide and Global Carbon Cycle, US Department of Energy ER-0239, 1985

[3] US Department of Energy, A preliminary analysis of US CO_2 emissions reduction potential from energy conservation and the substitution of natural gas for coal in the period to 2010, Technical Report DOE/NBB-0085, 1989

[4] Hansen, J. and Lebedeff, S., Global surface air temperatures, update through 1987, Geophysical Research Letters, Vol. 15, pp. 323-326 (1988).

[5] Bolin, B. et al. (Eds), The greenhouse effect, climatic change and ecosystems, SCOPE 29: John Wiley and Sons Publisher (1986).

LONG TERM WORLDWIDE ENVIRONMENTAL EFFECTS CAUSED BY ACID RAIN FROM FOSSIL FUELS

B. MANOWITZ, F.W. LIPFERT
Department of Applied Science,
Brookhaven National Laboratory,
Upton, New York,
United States of America

Abstract

Acid rain is regarded as an environmental problem of growing importance in many parts of the world; it is one of the adverse effects of air pollution. This paper presents data on emissions of air pollutants from combustion of fossil fuels and discusses atmospheric processes that act on these emissions, various effects of air pollution and acid deposition, and some of the aspects of regulation of these pollutants. Evidence of worldwide concern is shown by contrasting the perceived adverse effects of air pollution with ambient levels and the status of regulation.

1.0 INTRODUCTION

Acidification of precipitation was recognized as a local air pollution problem well over a hundred years ago [1]. Evidence that acid deposition was a regional phenomenon was presented by Rossby and Egner [2], who measured the ionic composition of rain and atmospheric aerosol at a network of stations in Sweden in the 1950s and suggested that episodes of regionally high aerosol sulfur concentrations were related to air-mass circulation that transported material from the interior of the Eurasian continent. Subsequently, Oden [3] demonstrated that high acid deposition was a regional phenomenon in Sweden and Western Europe by presenting contour maps showing large areas of low annual pH.

Awareness of the environmental concerns of acid deposition came to North America later than to Europe, but once their importance was recognized in the late 1970s there was a rapid and large response in the research and political communities [4].

This paper discusses emissions of air pollutants from combustion of fossil fuels, atmospheric processes that act on these emissions, various effects of air pollution and acid deposition, and some of the aspects of regulation of these pollutants. The worldwide focus is maintained by contrasting the perceived effects with the status of regulation and ambient levels.

2.0 FOSSIL FUEL EMISSIONS

Acid deposition is primarily the result of combustion of fossil fuels, although natural substances such as CO_2 and various organic acids contribute as well. It is commonly assumed that all fuel sulfur is oxidized to SO_2 and that varying amounts of atmospheric N_2 are oxidized to NO during the combustion process. As the combustion gas plume travels downwind in the atmosphere, it is subject to various chemical transformation and removal processes which can have important bearings on the nature of any adverse effects on the environment. The pollutants which are removed from the air can accumulate in surface deposits, which may have varying long-term effects upon their receptors.

Natural sources of atmospheric sulfur and NO_x include biogenic materials, volcanic eruptions, and lightning, but in the developed world, their relative contributions are thought to be small [5]. Other anthropogenic sources that can be important on a local level include ore smelters, refineries, and various chemical plants such as acid manufacturing.

Table 1 Regional Emissions Data (ca. 1980)

Region	Population (million)	Surface Area (mill.sq.km.)	SO_2 Emission (bill.kg/yr)	SO_2/Capita (kg/pers.yr)	SO_2 Density (g/sq.m)	NO_x Emission (bill.kg/yr)	NO_x/Capita (kg/pers.yr)	NO_x Density (g/sq.m)
Eastern U.S. (1)	161	3.08	18	112	5.84	11.6	72	3.77
Rest of U.S.	65	4.73	6.1	94	1.29	5.7	88	1.21
E. Canada (2)	15.3	0.69	2.93	192	4.25	1.04	68	1.51
NW Europe (3)	233	2.41	15	64	6.22	10	43	4.15
NE Europe (4)	76	0.64	11.9	157	18.59	4	53	6.25
USSR	268	22.3	25.5	95	1.14	15	56	0.67
Japan	113	0.372	1.1	10	2.96	1.4	12	3.76
China (5)	1000	9.56	13.6	14	1.42	8	8	0.84

(1) States east of 96th meridian
(2) South of about 50th parallel, east of 96th meridian
(3) Countries N. and W. of Italy
(4) Czech, DDR, Hung., Poland
(5) Estimated from energy use

Data Sources: Ref. 24,25

There are many ways to compare and contrast rates of air pollution emission. On a process level, one might compare mass of emission per unit of useful product output (MW of electric power, ton of steel, barrel of oil, etc.). Maps are often used presenting annual emissions per geographic unit, which can be misleading since large geographic units dominate the visual effect of the map and will usually be associated with large rates of emission. Emission density (tons/km^2) circumvents this problem but may unduly emphasize small areas; the emissions density at the location of a strong point source will be very high in all cases. For a ground level source or group of sources, ambient air quality is directly proportional to emissions density (and inversely proportional to wind speed).

For acid deposition, the scale of transport provides some guidance as to the appropriate size of regions for which emissions comparisons are appropriate. For sulfur oxides, this scale is of the order of 300-1000 km [6]; for nitrogen oxides, it may be somewhat smaller.

Table 1 compares some of these emissions parameters for several industrialized regions and for all of the USSR and China (for which it was not possible to subdivide). We see a large variation in emissions densities, which reflect population densities as well as energy use. The highest densities are for Northeastern Europe, due to the heavy use of coal there. The next level groups the Eastern U.S., Southeastern Canada*, Northwest Europe, and Japan. The lowest densities are found in the Western U.S., the USSR, and China (although localized areas of high emission densities are found in each of these areas). On a per capita basis, Eastern Canada and Northeast Europe have the highest SO_2 levels, and the Western U.S. has the highest NO_x levels. Per capita emissions are low in China because of low levels of industrialization and in Japan because of stringent pollution control regulations. These regulations are required in part because of the high population density in Japan.

3.0 ATMOSPHERIC PROCESSES

3.1 Atmospheric Transformations

Nitric oxide (NO) is nearly insoluble in water and is unreactive in solution; therefore, little if any is dry deposited to the surface or oxidized by reactions in cloud water. Nitric oxide is oxidized to NO_2 on a time scale of hours, by reaction with ozone (O_3) or other oxidants. NO_2 is subject to dry deposition and can be further oxidized to form nitric acid, by gas phase reaction with the OH radical. Nitric acid is quite volatile, highly soluble in cloud and rain water, and is subject to rapid dry deposition [6].

Ozone formation is dependent on both nitrogen oxides and volatile organic compounds (VOCs) which are often hydrocarbons emitted from motor vehicles, solvent usage, and natural sources. Ozone and other oxidants in complex photochemical cycles, with peak concentrations occurring on summer afternoons.

SO_2 can be oxidized to form H_2SO_4 in either the gas phase through photochemical reactions, or in the aqueous phase in cloud water. Clouds can then evaporate, leaving behind sulfate particles. The photochemical reactions are fairly slow, 1-3%/hr, but operate during all daylight hours. Aqueous reactions are faster, but require the presence of clouds. The relative importance of these two sulfate formation pathways will vary with season and climatic factors. The chemical form of airborne sulfur can play a major role in determining the nature and rate of any adverse effects, as discussed below.

Sulfate particles are usually associated with ammonium; larger particles involving calcium or other crustal elements are also found. The acidity of sulfate particles depends on their source and the extent of contact with ambient ammonia. Free H_2SO_4 is found at ground level on occasion.

*The large smelter in Quebec is not included in these figures.

The low vapor pressure of H_2SO_4 and ammonium sulfates is an important property, which ensures that they remain as particles under normal atmospheric conditions. In contrast, nitric and hydrochloric acids exist as vapors, and ammonium nitrate tends to be unstable. For this reason, the term "acid aerosol," which is one of the pollutants of current health concern, relates mostly to acidic sulfates [7].

3.2 Atmospheric Removal Mechanisms

The solubility of SO_2 in water is central to its removal from the atmosphere; this removal is responsible for the maintenance of a steady concentration state (rather than a continuous build-up in response to continuous emissions). Removal mechanisms are termed "wet" if associated with hydrometeors; "dry," if otherwise. SO_2 can readily be removed by dry deposition to vegetation and other moist surfaces, including the oceans. However, it dissolves only slightly in water, according to physical (Henry's Law) solubilities; its solubility is enhanced considerably by dissolution to form bisulfite ion, but this solubility is pH-dependent and quite limited for pH < 5 [8]. Thus the uptake of SO_2 by surface moisture depends on its buffering capacity [9]. Sea water is highly buffered and may be the "perfect" absorber of SO_2. Uptake of SO_2 into cloud water or surface moisture layers may be greatly enhanced by aqueous-phase oxidation, especially by hydrogen peroxide (H_2O_2) [6]. In surface moisture, attack of the surface by H_2SO_3 or H_2SO_4 can provide buffering [9].

Removal of sulfate particles is dominated by wet removal processes, mostly by dissolution into cloud water concurrent with cloud formation, followed by deposition in precipitation [6]. Dry deposition of sulfate particles is limited by the low diffusion coefficient of small aerosol particles.

Removal of NO_2 and ozone are controlled more by chemical reactions than by direct deposition, due to their limited solubility in water.

The pH of precipitation that has absorbed SO_2 or sulfates will depend on the other ions present, which can include NO_3^- from nitrogen oxide emissions and base cations from various dust sources, as well as HCO_3^- from atmospheric CO_2 and organic acids from natural sources. pH values below 5.6 (the value for equilibrium with atmospheric CO_2) have been popularly referred to as "acid rain." Figure 1 maps worldwide isopleths of pH for 1979 [10]; data for the Southern Hemisphere are mainly lacking, although pH values in the range 4.2-5.1 have been reported for cities in Australia [11]. The high values of pH (< 6) seen in Asia are thought to result from the dissolution of dust particles

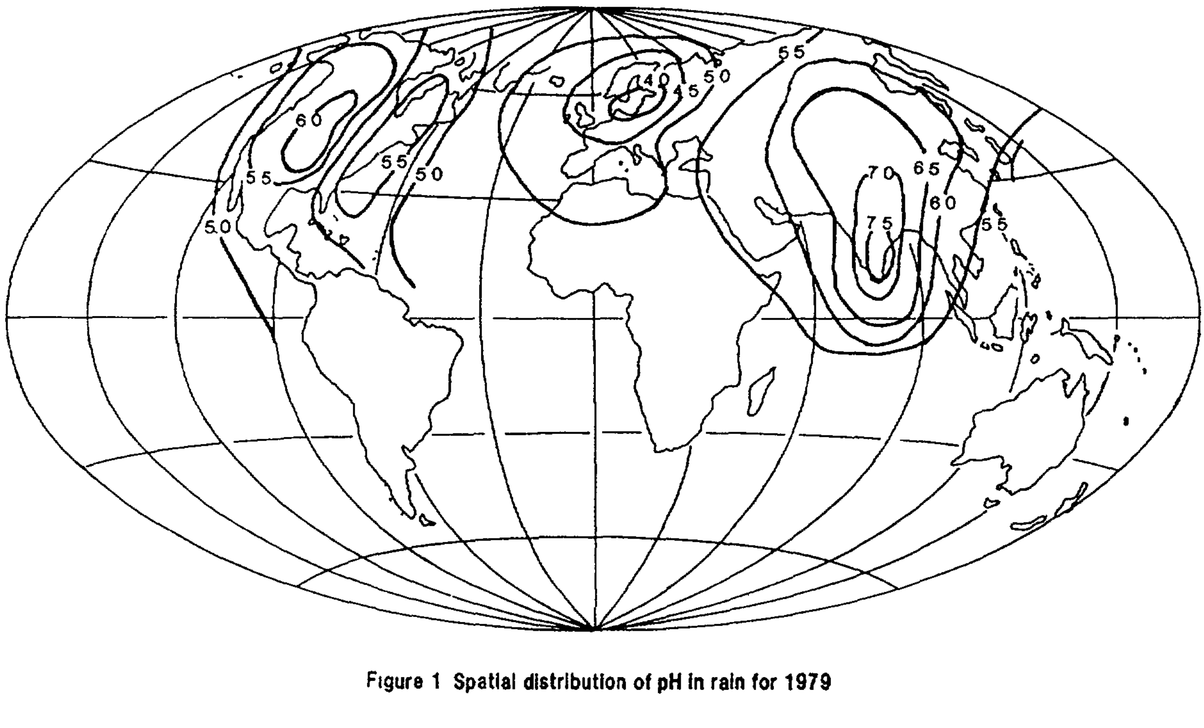


Figure 1 Spatial distribution of pH in rain for 1979

in precipitation. The lowest pH levels are found in the Northeast U.S. and in Northcentral Europe, which is consistent with the emissions density data of Table 1.

Wet removal processes are further controlled by precipitation types and rates. Dry deposition processes on surfaces are affected by atmospheric transport rates that mix fresh pollutant into the surface boundary layers and by the physical properties of particles.

Dry removal processes are generally considered slightly more important than wet, and dry deposition of (gaseous) SO_2 far exceeds that of its sulfate transformation products. This is a result of the characteristic $SO_4^=$ particle sizes (typically 0.1-1 um) being near the minimum for sedimentation and other physical deposition processes. One of the results of this difference in deposition velocities is that sulfur particles will remain airborne and thus travel further from their original sources than SO_2.

Wet deposition data for the Eastern U.S. show about 1-3 g/m^{2}yr for sulfur and 0.6-2 g/m^{2}yr for nitrogen [6]. If we add a like amount for dry deposition and compare deposition rates with emissions densities as given in Table 1, we conclude that emissions substantially exceed deposition and thus that a portion of the emissions is transported out of the region.

3.3 Atmospheric Transport Processes

If an atmospheric constituent is not removed, then it will be transported by the winds, which vary greatly in time and space. The vertical dimension is particularly important, not only because transport speeds increase with height but because the probability of encountering clouds increases with height and the likelihood of being trapped by a ground-based inversion is decreased. Electric utilities tend to use the tallest stacks, up to about 300 m. in North America and 200 m. in Europe. Many European cities use sulfur-bearing fuels for space heating, which are considered to be ground-level releases and are subject to trapping by atmospheric inversions.

Figure 2 Location of GEMS/Air monitoring stations

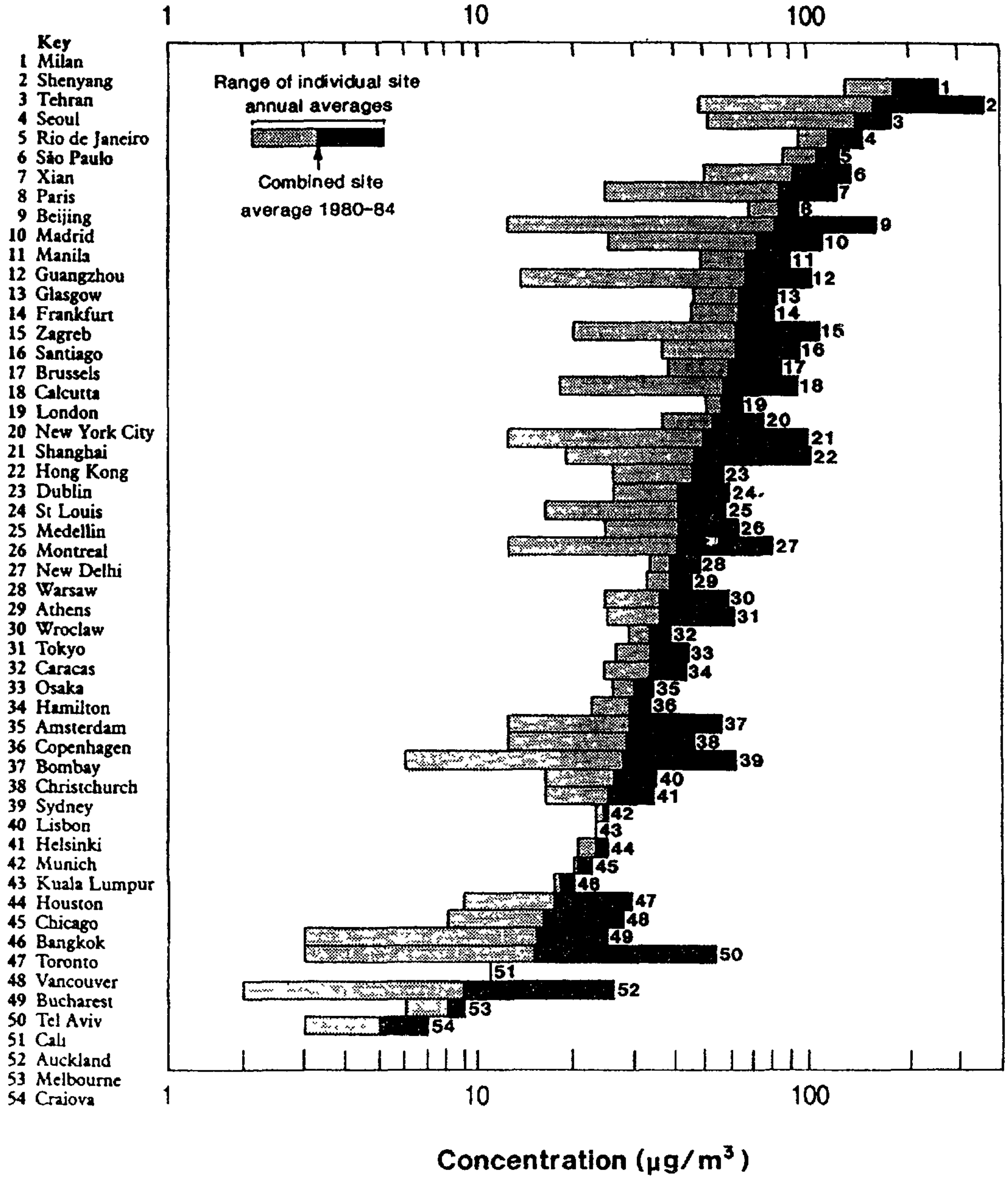


Figure 3 Summary of the annual SO_2 averages in GEMS/Air cities, 1980-1984

Figures 2 and 3 present a picture of global SO_2 and particulate levels in various cities around the world, as determined by the UNEP Global Environmental Monitoring System (GEMS) for 1980-84 [12]. The tremendous variation shown reflects both the range of population densities, the types of fuels used, and the degree of environmental control that has been imposed.

3.4 Ambient Concentration Levels

Air concentration patterns downwind of a source depend on many factors, including stack height, atmospheric conditions, and the presence of aerodynamic obstacles. Tall stacks tend to result in low concentrations (3-50 ug/m^3 for SO_2, for example) when averaged over time periods exceeding several days, due to the dispersive nature of the atmosphere. However, under adverse atmospheric conditions (highly convective conditions which bring the plume to the ground), SO_2 concentrations can approach 2500 ug/m^3 for periods of the order of one hour. These levels should be contrasted with stack exit gas SO_2 concentrations, which are often of the order of 5000 mg/m^3 or more.

NO_2 values can reach 400-600 ug/m^3 for one hour, but annual average values are generally in the range 50-100 ug/m^3. Since NO_2 is secondary pollutant formed in the atmosphere downwind of the primary sources, its concentration patterns are less variable than SO_2 or CO, for example.

Hourly ozone concentrations can reach 300 ug/m^3 or more under adverse conditions, but will drop to near zero at night in urban areas due to reactions with nitrogen oxides.

4.0 EFFECTS OF ACID DEPOSITION

Deposition of sulfur or nitrogen in regions where the soils are deficient in those elements may be considered a beneficial effect; all of the other effects of SO_x and NO_x are considered adverse. They include effects on human health, materials degradation, vegetation, and atmospheric visibility, and acidification of soils, watersheds and freshwaters. These effects can vary according to the characteristics of the receptor, atmospheric conditions, and the presence of co-pollutants.

There are three modes of damages due to sulfur emissions that must be considered, depending on the receptor: damages due to SO_2, due to sulfate particles, and due to acidified precipitation. The effects of nitrogen oxides must be considered in their own right and as a component of ozone and other oxidants.

Table 2 Summary of Global Air Pollution Effects and Concerns

Region	Pollutants	Effects of Concern
Worldwide	CO_2 Greenhouse Gases	Global warming Sea level rise
East. U.S.	Ozone Acid aerosol Acid deposition	Human health, forest damage Human health Lake acidification, materials damage
Cent. U.S.	Ozone Acid aerosol	Human health, forest damage, crop damage Human health
West. U.S.	Ozone Acid aerosol, fog	Human health, forest damage Human health, atm. visibility
East. Canada	Acid deposition Acid aerosol	Lake acidification, forest damage Human health
Cent. America	Acid deposition	Cultural materials damage
3rd World Cities	Ozone Particles, SO_2	Human health
No. Europe	Acid deposition	Lake acidification, materials damage
Cent. Europe	Ozone Acid deposition Particles, SO_2	Human health, forest damage Cultural materials damage
So. Europe	Ozone Particles, SO_2	Human health, forest damage Cultural materials damage
Japan (cities)	Ozone Particles, SO_2	Human health

Table 2 presents a summary of the types of adverse effects of air pollution and acid deposition that are perceived as threats in various parts of the world. In many cases, there is ongoing debate as to the nature and seriousness of these threats, but concerns about acidic species and ozone are seen to be widespread.

The following sections discuss the physical and chemical bases for many of these adverse effects.

4.1 Human Health Effects

SO_2 is considered a mild respiratory irritant, affecting primarily the upper respiratory tract. The evidence for SO_2 health effects comes from animal toxicological experiments, chamber studies of human volunteers, and epidemiological studies. However, in many of the epidemiological studies, it has been difficult to isolate the effects of the various pollutants which tend to occur at the same times and places (for example, SO_2 and particulates) [13].

Early tests of human volunteers at SO_2 levels from 1-8 ppm showed a great deal of variability in their tolerance [14]. Definite but transient effects were shown on pulse and respiration rates. Some people become accommodated to such high levels of SO_2. More recent experiments with asthmatics have shown respiratory sensitivity at levels as low as 0.25 ppm, particularly while exercising [15].

Sulfate particles may penetrate into the deeper airways, depending on their size, the breathing rate, and the amount of hygroscopic growth in transit. Acidic particles can reduce the pH of mucus, which in turn affects the action of the cilia in clearing foreign matter from the lung. This may explain why the combination of sulfur and other particulate matter at high concentrations was so deadly during the notorious air pollution episodes of many years ago [13]. In addition, recent studies have been interpreted to suggest that prolonged breathing of sulfuric acid particles can result in permanent lung alterations [16]. Since industrial H_2SO_4 exposure levels of 500-1000 ug/m^3 are commonly tolerated, it appears that there are marked individual differences in susceptibility.

Ozone and NO_2 are also classed as respiratory irritants, but since they are less soluble than SO_2, they are more likely to reach the lower airway passages. Reductions in lung function are among the types of biological responses that have been shown. Ozone and other oxidants have also been linked to eye irritation.

The health effects of air pollution are still a matter of some debate. Frank [17] pointed out 15 years ago that there was strong epidemiological evidence for the adverse effects of SO_2 and particles, but that normal individuals showed no response to these same levels in clinical chamber experiments; the opposite was true for ozone and photochemical oxidants. To a large extent, this situation is still true [7,13].

4.2 Materials Degradation Effects

Virtually all of the effects of SO_2 on materials are associated with its dissolution in surface moisture [9] as the primary mechanism of deposition. Thus the appropriate environmental index for materials damage should include not only the average ambient SO_2 concentration but also an index of the relative times that material surfaces are wet and thus receptive to SO_2 deposition. Sulfur in the atmosphere has an additional adverse affect on some materials through acidification of precipitation; however, for both "dry" deposition of SO_2 and impact by acid precipitation, the primary damage mode is attack by dilute acids.

The materials known to be sensitive to such attack are primarily those presenting a relatively thin facade of a substance that reacts readily with dilute acids (especially sulfuric). These include zinc (galvanized steel), certain paints, unprotected carbon steel. Copper (bronze) and carbonate stones (marble, limestone, some sandstones) may be attacked by acids, but their "sensitivity" will depend on the stock thickness and the intended service life. In the case of outdoor sculpture, for example, all works of permanent value will be "sensitive" to deposited acids [18].

There is concern in most parts of the developed world about preservation of important monuments and antiquities in the face of continued acid deposition, especially in Europe. Eastern Europe, where high sulfur fuels continue to be used, is thought to be particularly at risk; statues, churches, and gravestones are in danger of catastrophic erosion. A more recent development is the contention that acid rain is damaging ancient artifacts in Mexico and Central America [19]. In these cases, the pollution sources are thought to be oil refineries and motor vehicles such as tour buses, but the worldwide background in acidic species could also be a contributor.

4.3 Air Pollution Effects on Vegetation

High short-term concentrations of ozone or SO_2 can have direct foliar damaging effects on vegetation. In particular, ozone is thought to be responsible for millions of dollars of crop losses annually [20]. In Germany it is claimed that 52% of forests have been damaged, presumably by air pollution, of which 14% are highly damaged and 1% are dead [21]. Acidity has increased in all soils in Germany within the last 20 years.

4.4 Landscape Acidification Effects

Deposition of acidifying substances upon the landscape can have several different types of adverse effects, depending on the buffering capacity of the ecosystem. These acidifying substances include both acid precipitation and dry deposition of SO_2 and sulfate particles. In non-arid regions, precipitation ultimately dissolves all of these deposits and flushes them through the watershed into receiving surface waters, after which they eventually end up in the oceans.

The adverse effects of this chain of events can include direct damage to vegetation, acidification of soils, and acidification of surface waters with attendant impacts on flora and fauna. In the case of managed (agricultural) soils, soil acidification effects may be overcome through use of lime.

Many factors control whether a given water body will become acidified as a result of a given deposition regime. In addition to the deposition rate and the lake residence or turnover time, these include the ratio of water surface area to watershed area, the composition of the lake bottom, the residence time of incident precipitation en route through the watershed, and the buffering capacity of the watershed. The presence of organic material can also be important. One of the important parameters is the solubility of bedrock geology; carbonate rocks (limestone) will buffer acid deposition, given sufficient contact time, whereas silicate rocks (granite) are essentially insoluble. Thus lakes in those regions underlain by granite (Northeastern North America, portions of Scandinavia) may be particularly at risk to acid deposition. Sweden estimates that 18,000 or about 21% of her lakes have become acidified [22]. Similar estimates in the U.S. vary greatly by region and the definition of "acidification."

In response to this threat, Sweden has begun a program of adding crushed limestone to selected lakes to control pH; similar efforts are being considered in the U.S. and elsewhere.

There is considerable debate as to the critical pH or alkalinity level for surface waters, depending on whether the criterion involved include elements of the ecosystem other than game fish. For example, Swedish research [22] has shown that some crustaceans and plankton may disappear from waters at pH values less than about 6, some fish species at pH < 5, and some at pH < 4.5. The conference proceedings from the Scandinavian SNSF project [23] is a useful information resource on acidification effects.

There is currently widespread concern about the potential effects of air pollution and acid deposition on forest health. In the U.S., declines have been noted in red spruce, fir, sugar maple, and hardwoods, for example. The only firm evidence of atmospheric pollution damage comes from effects of ozone and from nearby effects of strong point sources such as smelters or power plants. The current consensus thinking attributes the observed forest declines to a combination of effects, including ozone and possibly acid deposition, along with increased environmental stress from other factors.

5.0 REGULATION OF AIR POLLUTION AND ACID DEPOSITION

Air pollution is regulated in many countries through a dual system of emissions limits and ambient air quality standards. For those pollutants for which ambient standards have been promulgated, sources are prohibited from emitting above certain rates. These limits are often based on technological considerations. When the density of sources becomes too great however, additional emissions controls may be required or further industrial growth may be curtailed. These limits are based on ambient air quality standards. Emissions limits are usually constant in time, although in the past dynamic systems have been tried which seek to tailor emissions to the dispersive capacity of the atmosphere. Ambient standards, on the other hand, are set for certain specific averaging times, typically one hour, 24 hours, and annual, according to the type of adverse effect being considered.

Acid deposition has been difficult to regulate by means of this system, since the deposition often occurs far from the responsible sources, which may be in a different state or country. In addition, it is practically impossible to identify with certainty the pollution sources responsible for a specific deposition event. In the U.S., the Federal Government has proposed to reduce acid deposition by mandating arbitrary reductions in SO_x and NO_x emissions from a large group of specific sources, mostly electric utilities. In this case, uniformity is being imposed on the sources, rather than at the receptors.

Table 3 **Selected Ambient Air Quality Standards (ug/m^3)**

Pollutant	Av'g. Time	USA	FRG	Japan	Sweden	China
SO_2	24-hr	365	140	100	250	
	annual	80				50-250
NO_2	24-hr			100		50-150
	annual	100				
Oxidants	1-hr	236	118			197

5.1 Ambient Air Quality Standards

Ambient air quality standards are usually intended to protect the health of the population, although in some cases other kinds of impacts ("welfare" effects) may enter into the equation as well. Table 3 presents some selected standards for different countries.

In general, these standards are often exceeded in many locations; the approach is to set uniform ambient air quality standards for an entire country, but to expect that different cities or industrial areas will require different lengths of time to achieve these standards. As an example, Norway only recently (1987) closed a copper smelter that was creating annual average SO_2 levels greater than 400 ug/m^3 in the nearby community.

6.0 CONCLUSIONS

The combustion of fossil fuels creates effects on health and the environment which are perceived to be deleterious. In most of the developed world, stringent regulations have been placed on atmospheric emissions resulting from the use of these fuels; through the years these regulations have been tightened further and this process may well continue. The ambient impacts of fossil fuel use are seen to depend on population density as well as on fuel characteristics and pollution controls.

REFERENCES

[1] SMITH, R. A., On the air and rain of Manchester. Mem. Lit. Philos. Soc. Manchester, Series 2. 10 (1852) 135.

[2] ROSSBY, C. G., EGNOR, H., On the chemical climate and its variation with the atmospheric circulation pattern, Tellus 1 (1955) 118.

[3] ODEN, S., Water, The acidity problem--an outline of concepts, Air, Soil Poll. 6 (1976) 137.

[4] REGENS, J. L., RYCROFT, R. W., The Acid Rain Controversy, Univ. Pittsburgh Press, Pittsburgh (1988).

[5] PLACET, M., STREETS, D. G., Emissions of Acidic Deposition Precursors, in Interim Assessment, the Causes and Effects of Acidic Deposition, National Acid Precipitation Assessment Program (undated).

[6] SCHWARTZ, S. E., Acid deposition: unraveling a regional phenomenon, Science 243 (1989) 753.

[7] LIPFERT, F. W., MORRIS, S. C., WYZGA, R. E., Acid aerosols - the next criteria pollutant? Env. Sci. Tech., in press.

[8] SCHWARTZ, S. E., Gas-Aqueous Reactions of Sulfur and Nitrogen Oxides in Liquid-Water Clouds, in SO_2, NO, and NO_2 Oxidation Mechanisms: Atmospheric Considerations, Ed., J. G. Calvert, Butterworth, Woburn, MA, (1984) 173.

[9] LIPFERT, F. W., Dry deposition velocity as an indicator for SO_2 damage to materials, J. APCA 39 (1989) 446.

[10] GEORGII, H.-W., "Global distribution of the acidity in precipitation," in Deposition of Atmospheric Pollutants, (GEORGII, H.-W., PANKRATH, J. REIDEL, Eds.) Dordrecht, Holland (1982) 55.

[11] AYERS, G. P., GILLETT, R. W., Some observations on the acidity and composition of rainwater in Sydney, Australia, during the summer of 1980-81, J. Atm. Chem 2 (1984) 25.

[12] World Health Organization, Global Pollution and Health, United Nations Environment Programme (1987).

[13] LIPFERT, F. W. "Air pollution and mortality," draft chapter for Handbook of Environmental Chemistry, Springer-Verlag, Heidelberg, (1989).

[14] AMDUR, M. O., MELVIN, W. W., DRINKER, P., Effects of inhalation of sulphur dioxide by man, Lancet (1953) ii, 758-759.

[15] SHEPPARD, D., WONG, W. S., UEHARA, C. F., NADEL, J. A., BOUSHEY, H. A., Lower threshold and greater bronchomotor responsiveness of asthmatic subjects to sulfur dioxide, Am. Rev. Resp. Dis. 988, 122, 873-878.

[16] LIPPMANN, M., Progress, prospects, and research needs on the health effects of acid aerosols, Env. Health Perspectives 79 (1989) 203-205.

[17] FRANK, R., "Biologic effects of air pollution," in Energy and Human Welfare, (COMMONER, B., BOKSENBAUM, H., CORR, M., Eds.) MacMillan (1975) 16-27.

[18] LIPFERT, F. W., "Air pollution and materials damage," in Handbook of Environmental Chemistry (HUTZINGER, O., Ed.) Springer-Verlag, Berlin (1989) 114-186.

[19] New York Times, Aug. 8, 1989, p. C1.

[20] ADAMS, R. M., Estimated Economic Consequences of Ozone on Agriculture: Some Evidence From the U.S., in Atmospheric Ozone Research and its Policy Implications (SCHNEIDER, T. et al, Eds.) Elsevier (1989) 869.

[21] HARTWIG, S.G., KRA, R. S., Insufficiencies in Solving Global Environmental Problems by Specialized Scientific Expertise, presented at Conference on Technology-Based Confidence Building: Energy & Environment, St. John's College, Santa Fe, NM (1989).

[22] Acidification Today, Swedish Ministry of Agriculture, Environment '82 Committee (1982).

[23] DRABLOS, D., TOLLAN, A. (Eds.), Ecological Impact of Acid Precipitation, Proceedings of an International Conference, Sandefjord, Norway (1980). SNSF Project, Oslo, Norway.

[24] WETSTONE, G. S., ROSENCRANZ, A., Acid Rain in Europe and North America, Environmental Law Institute, Washington, DC (1983).

[25] RIVERS, M. E., RIEGEL, K. W., Emissions, Costs, and Engineering Assessment, Final Report from Work Group 3B, U.S.-Canada Memorandum of Intent on Transboundary Air Pollution (1982).

SPECIAL INVITED PRESENTATION

F.M. Bernthal

Bureau of Oceans and International Environmental
and Scientific Affairs
United States Department of State
Washington, D.C.
United States of America

Perhaps for the wrong reason, the drought in our own Great Plains, global climate change burst into the American consciousness in the summer of 1988. But whatever the reasons, it was time to pay attention.

Global climate change has suddenly become the most important environmental issue of the day, and may well become the dominant foreign policy issue of the 21st century.

This issue places political leaders in the unenviable position of having to distinguish between a problem that is serious - and this one is - and a problem that is a crisis, which this is not - not yet.

Making that distinction will not be easy. But we may need to make decisions with far-reaching implications, even in the face of important uncertainties about critical aspects of the problem.

Our first priority is thus to increase our understanding of the natural processes we are observing and to develop a better understanding of the potential impacts on our environment and on our social and economic systems.

Because the American people will not forgive us if they are asked to make great sacrifices and we turn out to be wrong. They would be much less likely to listen next time - and I have little doubt that, one way or another, mankind is quite capable of fouling his planetary nest.

Now let me set the record straight on what we think about all this. There is no doubt that so-called "greenhouse" gases are accumulating in the atmosphere of our planet. Most of the effect is anthropogenic - i.e. man-made. That much we can measure. There is also little doubt from the laws of physics that, other things being equal, such gases should warm the planet. Indeed, were it not for the greenhouse effect, ours would be a perpetually frozen world, some 30 degrees C colder than it is now.

Beyond these facts, however, the state of our knowledge becomes much fuzzier. The exact timing, magnitude, and regional climatic effects of the predicted warming are fraught with uncertainty. Current best estimates range from 1.5 to 5 degrees C by the middle of the next century, with corresponding consequences that would range from the expensive and inconvenient to the catastrophic. And therein lies the difficulty for our leaders.

It is never easy to maintain political interest in an issue that will span the careers - indeed the lifetimes - of everyone in this room today. But the single political imperative for this issue is focus and continuity - despite last summer's drought in the Great Plains, despite the New York Times telling us that the 100-year record shows no evidence after all for warming in the U.S., and even despite some future years of cooling that might cause the warmth of the 80's to fade in our memory.

That is why President Bush has said that we will enter into international negotiations late in 1990 on a framework climate convention to set forth the broad principles that should guide world cooperation and attention in the decades ahead.

International scientific, policy and political considerations must proceed in tandem with any decisions we make domestically, because action by us alone would be virtually meaningless should the world need to limit greenhouse gas emissions or mitigate their effects.

Indeed, we are told that China plans to double its use of coal by the year 2000, and India plans a tripling. If that happens, coal use in just those two countries will exceed that of all the OECD countries combined. So while today's greenhouse gases are primarily the product of the industrialized nations, if current trends continue, by the middle of the next century we expect that half of the problem will reside in the developing world.

We are thus working to reach an international consensus on the nature of climatic change and potential response strategies for addressing such change. To that end, the U.S. strongly supported the establishment of the Intergovernmental Panel on Climate Change (IPCC), under the auspices of the U.N. Environment Program and the World Meteorological Organization, to serve as the primary international forum for addressing this issue.

The IPCC has established three working groups: one to review and assess the science relevant to climate change, another to assess the possible environmental and socio-economic impacts of such change, and a third to identify potential response strategies. The U.K. chairs the science group, the USSR the impacts group, and the U.S. the more political Response Strategies Working Group (RSWG).

As you can infer from the structure, the idea is to proceed along parallel paths - nailing down the science while at the same time beginning contingency planning to respond, should the science tell us that action is needed.

The RSWG, which I chair, is considering both short and long term policy options for addressing climate change. Four topical subgroups have been formed: energy and industry; agriculture and forestry; coastal zone management; and resource use and management. The first two sub-groups will consider strategies for limiting the rate of climate change; the second two for adapting to climate change.

And at its next meeting in Geneva in October, the RSWG will discuss mechanisms for five categories of response implementation, many of which are of special interest to the developing world. These include financial measures; technology transfer and development; public education; economic (market) measures; and finally, legal measures, including elements of a possible framework convention on climate change.

Another task undertaken by the RSWG is to prepare greenhouse gas emissions scenarios which the IPCC Science Working Group will use for its climate modeling. The scenarios being explored are for increases in atmospheric concentrations of greenhouse gases equivalent to a doubling of atmospheric CO_2 by the years 2030 (more or less business as usual), 2060, and 2090, the latter to include stabilization thereafter.

A fourth scenario that would explore greenhouse gas increases to a level substantially below doubling, with subsequent stabilization, is also being developed pursuant to the direction of the June IPCC plenary meeting in

Nairobi. But our atmosphere already has CO_2-equivalent greenhouse gas concentrations that are nearly 150% of the pre-industrial level.

The RSWG is also discussing the implied trade-offs among emissions reductions, technological changes, population growth, and growth in per capita GNP. The Japanese delegation presented an analysis which implies that a technological revolution would be required to stabilize the atmosphere by the year 2090, if world economic growth is to be maintained at acceptable levels.

Such a 100-year perspective is needed to determine what our climate future might hold, whether that future is acceptable, and how it might be modified. All of these considerations will form the basis for the IPCC's interim report to the Second World Climate Congress in the fall of 1990.

If the careful, international scientific assessments now underway sound the alarm before the end of the century, as they could, then the domestic policy of all countries, including the United States of America, will be profoundly affected.

Secretary Baker, in his first statement in an international forum last February, made four key points on the climate change issue:

First, we can probably not afford to wait until all of the uncertainties have been resolved before we do act. Time will not make the problem go away.

Second, while scientists refine the state of our knowledge, we should focus immediately on prudent steps that are already justified on grounds other than climate change - what I call the "no regrets" policy: things we will never regret doing, whether or not global warming ever occurs. These include CFC emissions, greater energy efficiency, and reforestation.

Third, Secretary Baker noted whatever global solutions to global climate change are considered, they should be as specific and cost-effective as they can possibly be.

Finally, those solutions will be most effective if they transcend the great fault line of our times - the need to reconcile the human imperative for both economic development <u>and</u> a safe environment.

These remarks have become the cornerstone of current international policy on global warming. They are of particular importance to this workshop, for if global warming is inherently an international problem it is also inherently an energy problem.

Whatever solutions may become necessary, analyzing the cost-effectiveness of proposed measures will be devilishly difficult for a problem that is of uncertain magnitude, decades in the future, and has poorly defined regional climatic consequences. But as Secretary Baker has noted, the economics of any specific proposals must be credibly taken into account.

I am sure we can agree that we will never regret improved efficiency in energy use, as U.S. reserve electricity capacity dwindles and as oil imports spiral toward 8 million barrels a day. And if you are an optimist about long-term natural gas supply, gas produces only half as much carbon dioxide as coal.

But in the long run, we know that energy technologies which minimize greenhouse gas emissions will be essential if action becomes necessary. Improvements in energy efficiency, dealing with CFC's, reforestation - such measures, if undertaken, can shift the base line, delay the onset of the problem.

Permanent solutions that permit continued world economic growth will require a permanent shift in the mix of energy sources. As part of that mix, nuclear power must finally achieve its potential as one of the most environmentally benign of all energy sources. Indeed, nuclear power can and should be part of the "no regrets" strategy.

It is still only whispered that nuclear power is among the few economically competitive alternatives available on a scale large enough to make a difference, should permanent CO_2 reductions be needed within our lifetime. Indeed, measures being discussed in some quarters would amount to a decisively favorable subsidy for nuclear power, a fact which should trouble both scientists and environmentalists less than it might market economists.

Now I needn't remind this group that no new nuclear plants have been ordered in the U.S. since 1978. Moreover, no plant ordered since 1974 has been completed. There is no doubt that in a democracy, and perhaps anywhere, success or failure in a new endeavor ultimately rests on public support. But the history of new technologies is one of early public rejection, and later acceptance - if the fundamentals of economics and safety merit such acceptance.

The American people are remarkably good at weighing such issues and reading the balance. Ironically, I believe the American people are ahead of many of their leaders, public and private, on this issue. Indeed, opinion polls reflect the abiding instinct of a majority of Americans that nuclear power will be "very important" in meeting the nation's future energy needs.

During my tenure on the Nuclear Regulatory Commission, the Commission for the first time began to take an active interest in the safety characteristics of advanced reactors. A new policy was adopted to permit timely, anticipatory NRC safety review of next-generation reactor design concepts, much as the FAA has long reviewed new airframe designs.

That's important because the public and the technical community need to know from a tough, independent, authoritative source whether safety claims being made for new reactor systems have merit. And they need to know early, long before the investment - intellectual, political, and financial - is so great that it develops a life of its own.

As part of its 1986 Advanced Reactor Policy Statement, the Commission also made clear its expectation that next-generation power plants should exhibit enhanced safety characteristics, and it set down broad guidelines for how such characteristics might be achieved.

In short, we anticipated that the next generation of plants would be simpler, more reliable, easier to build, more forgiving in operation, and easier to maintain than the current generation plants. That was not a statement of lack of confidence in the present; it was an expression of confidence in the future. Just as the 767 jetliner is better than the 707, the reactor design of 2000 should be better than that of 1974.

So both here and abroad, alternatives are being sought, many of which you will hear about in this meeting. And while I may not be entirely abreast of the latest wrinkle in "inherently safe" (or is it "passively safe"?) reactors, one thing I do know: we cannot expect society to judge nuclear power by the same standard as it does all other risks. The next generation of plants must therefore convince a skeptical public that they can expect (and I choose the word "expect" carefully, mathematically) to recount TMI-style accidents only to their grandchildren.

And the public has a right to expect that Chernobyl-style disasters will be things you read about only in history books - like the eruption of Krakatoa, or to define the appropriate time scale more clearly, like the great supernova that created the Crab Nebula in the constellation Taurus, as recorded by 11th century Chinese astronomers.

Psychologists tell us that youthful members of the species homo sapiens find it exceedingly difficult to comprehend their own mortality. A similar psychology seems to reside in all of us as we contemplate a planet in the bloom of life. The intellect may warn of the apocalypse, but in the gut, we simply find it hard to believe.

There is some scientific evidence that Venus, the closest thing to hell in our solar system with a greenhouse effect run amok, may once have been a planet with an abundance of water. We should disabuse ourselves of the notion that Providence will surely intervene should mankind somehow contrive to render this planet uninhabitable too.

Finally, let us remember that change is not only inevitable, but the source of new opportunities. The world faced a serious energy crisis in the nineteenth century - it was running out of whale oil. To John D. Rockefeller and Andrew Mellon this was an opportunity, not a crisis. I imagine the whales would agree.

PANEL PRESENTATIONS

ACIDIFICATION AND THE GREENHOUSE EFFECT: A CANADIAN PERSPECTIVE

A.J. MALINAUSKAS
Atmospheric Environment Service,
Canadian Climate Centre,
Downsview, Ontario,
Canada

1. INTRODUCTION

The earlier speakers on this morning's session dealt with the impacts of the greenhouse effect and of acid rain, on a global basis; this paper presents a Canadian perspective on each of these two issues.

In Canada, concern over the environment is rising so quickly that only economic issues such as inflation are listed as more important problems facing the country, according to a poll released on July 31, 1989. Seventeen percent of Canadians named environment as Canada's most pressing problem, up sharply from the four percent in an earlier poll taken in February, 1988. Ninety-four percent of Canadians are either somewhat or very concerned about the environment.

2. THE CANADIAN ACID RAIN CONTROL PROGRAM

2.1 Sources and Effects of Acid Rain

Acid rain is caused by emissions of sulphur dioxide (SO_2) and nitrogen oxides (NO_x). In North America, the main sources of SO_2 emissions are different in our two countries. In Canada, non-ferrous ore smelters are the major source of sulphur dioxide emissions, while in the U.S. the major source is coal-fired power generating stations. The main sources of NO_x emissions, the other element of North America's acid rain problem, are the same in both countries: fuel combustion in motor vehicles.

In Canada, Acid rain is causing serious economic social and environmental problems:

- Economically, acid rain is endangering resources -- fisheries, tourism, agriculture, and forestry -- in an area of eastern Canada that measures one million square miles (2.6 million square kilometres). The resource base at risk sustains approximately eight percent of Canada's gross national product and some 255,000 jobs. The cost of acid rain damage occurring each year in Canada is estimated at $1 billion.
- Over 300,000 Canadian lakes are vulnerable to acidification; rivers too, are at risk. An example of the result of this damage is the fact that there are now 19 salmon rivers in Nova Scotia that no longer support the species.

- At least three-quarters of the most productive agricultural land in eastern Canada annually receives more than the acceptable levels of acid deposition.

- More than 50 percent of eastern Canada's forests, which generate $14 billion worth of products, grow in areas where rainfall is acidic.

- Extensive damage to materials, historic buildings and monuments has been widely documented. Canada's parliament buildings, the Washington Monument and the White House are among the "victims".

- More than 80 percent of all Canadians live in areas with high acid rain-related pollution levels, posing respiratory problems in sensitive populations such as children and asthmatics.

2.2 What Must Be Done

More than half of the acid deposition in eastern Canada originates from emissions in the United States. By the same token, Canadian emissions contribute ten to twenty-five percent of the deposition in areas of the northeastern USA.

To protect the environment, the Canadian federal government has identified a need for a 50% reduction of the 1980 level of sulphur dioxide emissions in eastern Canada and an equivalent reduction in the flow of sulphur dioxide from the United States.

To achieve this objective:

- Total Canadian sulphur dioxide emissions from the Saskatchewan/Manitoba border eastward must be reduced to 2.3 million tonnes per year (50 percent of the 1980 level), and

- The transboundary flow of sulphur dioxide from the United States into eastern Canada must also be reduced to about 2 million tonnes per year, again, about 50 percent of the 1980 level.

2.3 What Canada is Doing

In 1985, Canada's Prime Minister announced the establishment of a comprehensive national acid rain abatement program that will slash Canada's sulphur dioxide emissions, by 50%, by 1994 at the latest. All seven federal-provincial agreements required to implement this program have been signed. Canada's program is already showing results. Current emissions are down to 2.8 million tonnes, almost 40% below 1980 levels.

2.4 USA Plans

In the United States, proposed amendments to the U.S. Clean Air Act call for sulphur dioxide reductions of nearly 50% of 1980 levels by the year 2000. Canada is cautiously optimistic about the proposal.

3. THE CANADIAN CLIMATE CHANGE PROGRAM

3.1 Introduction

In Canada, a national climate program was established in 1979 with the same components (data, applications, research and impacts) as that of the World Climate Programme (WCP). That part which is most directly linked to the greenhouse effects issue is the Impacts component.

3.2 The Canadian Climate Impacts Program

This program, initiated in 1984, investigates the possible socio-economic impacts of climate warming due to increasing concentrations of CO_2 and other radiatively-active gases.

Over twenty major studies, some with multiple phases spreading over two-to-three years, have now been completed. These studies have identified some of the potential direct impacts on: agriculture; forestry; navigation; power generation; fisheries; and recreation and tourism. The impacts of sea level rises on coastal communities have also been assessed.

Nearly all of these studies, into regional and sectoral impacts of possible future climates have been carried out under contract by Canadian universities or private sector consultants. One case study experiment - to assess the impacts of climate change on agriculture in Saskatchewan, Canada - was completed as part of a joint project with the International Institute for Applied Systems Analysis (IIASA) and the United National Environment Programme (UNEP).

We are communicating the results of these studies to the Canadian public through the Climate Change Digest, a publication series implemented in June, 1987. Press releases announcing each issue have attracted considerable media attention and have resulted in increasing demand for the publication; 3500 copies of each issue are now printed.

3.3 An Agenda for Action in the Next Decade

We would propose the following four point framework as our agenda for the next decade - a framework which must be coordinated globally, but implemented locally.

Firstly, particular emphasis must be placed on the understanding of the global climate system, and the sensitivity of society to changes within it. Major scientific uncertainties will need to be addressed; a second generation of impact studies will need to identify in greater detail those natural and human systems most sensitive to climate change; and national climate programs will have to be developed and/or strengthened.

Secondly, appropriate strategies to adapt to possible climate change will need to be developed; these will have to address the question of uncertainty and be included in our assessment of risks and costs. We will need to compare the consequences of preparing ourselves for climate change that may not happen with those of failing to prepare for changes that do occur.

Thirdly, limitation strategies must also be devised, with an emphasis on integrated international conventions and protocols, using existing UN agencies as the mechanism to coordinate development and implementation. This must be accompanied with a domestic program focussing on improvements in energy efficiency and demand reduction.

Lastly, since implementation of policies is dependent largely on their acceptance by the general public, extensive public education is a fundamental part of any action strategy.

In summary, climate change is a priority issue for the Canadian government. As outlined at the follow-up meeting to The Hague Summit, held in Paris, May 9-10, the Canadian approach is to develop a comprehensive international response with full utilization and strengthening, at least initially, of the existing network of international institutions (UNEP, WMO, IPCC) and OECD/IEA Energy-Environment initiatives. Canada is also advocating the development, on an urgent basis, of legal instruments on the protection of the atmosphere, with an emphasis on climate change.

THE GREENHOUSE EFFECT AND ACIDIFICATION

C. VELEZ
Instituto Nacional de Investigaciones Nucleares,
México. D.F.,
Mexico

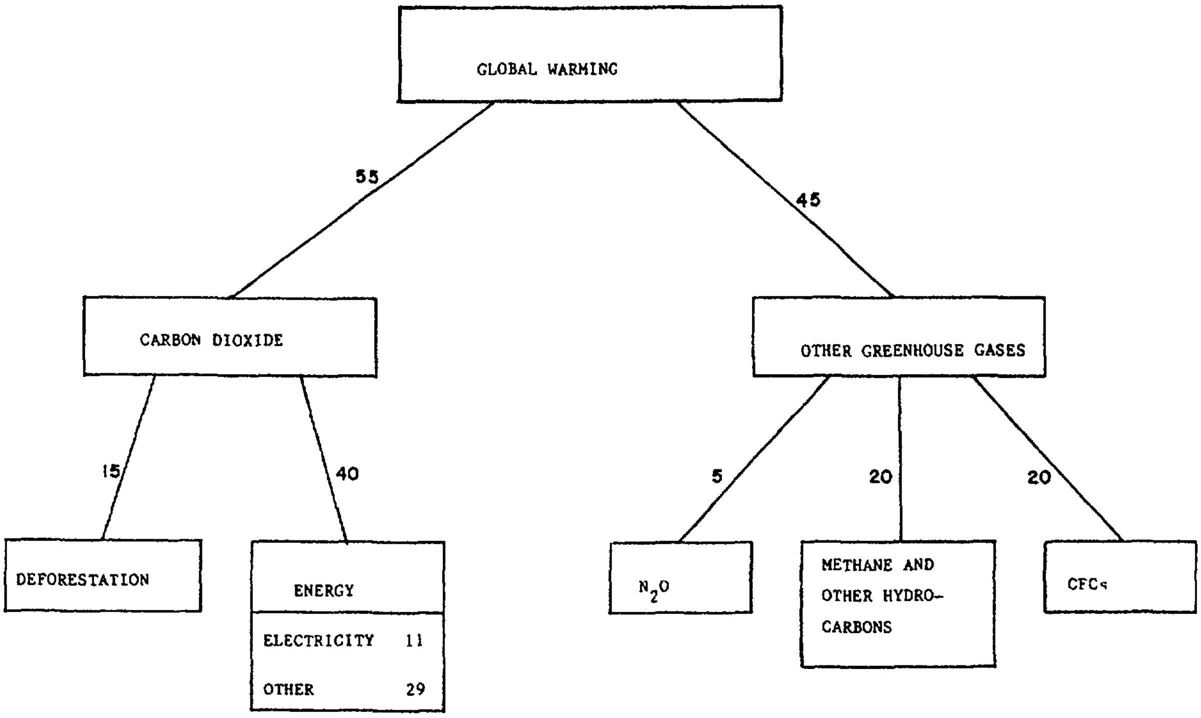
I will say a few words first about acid rain, from Mexico's perspective. In the medium term, Mexico will rely more on the use of coal, national and imported, for power generation. To give you an idea, some forecasts of the electricity that will be produced in Mexico in 2015 show the following composition:

Hydroelectricity	23%	compared with 22% today
Hydrocarbons	27%	compared with 67% today
Coal	33%	compared with 7% today
Goethermal	4%	same as today
Alternate sources	3%	
Nuclear	10%	

That is, fossil fuels will generate 60% of the electricity and nuclear fuel only 10%.

The measures that are being taken in the North American continent to prevent acid rain will eventually have an impact in Mexico, increasing the capital costs of thermal plants and making the competitive position of nuclear plants a little better.

On the increase in the greenhouse effect or global warming, let me say that global warming is not necessarily bad for everybody. Remember that for most people in the world agriculture is more important than ecology. What is menacing is the rate of change that, as shown in the first paper this morning, could be too fast for the living beings, including man, to adapt to.



MAKE UP OF GLOBAL WARMING

(all figures are percentages of the total present global warming effect)

I would like now to show a figure on the different contributions to global warming, that was part of a report by the UKAEA to the House of Commons at the beginning of this year*. I do not know the uncertainties in this figure but I am sure that there are some. In any case, I think it is very revealing to see that electricity production contributed only 11% to global warming. Furthermore, if chlorofluorocarbons are eliminated by the year 2000, that alone will represent a reduction of 20% in the total contribution.

This is not to say that nuclear power cannot play any role in the diminution of the greenhouse effect. According to the IAEA**, nuclear power is already preventing the emission of some 1600 million tonnes of CO_2 per year, compared with 20 000 million tonnes generated by the production of energy. The Toronto Conference last year proposed a reduction of 20%, that is 4000 million tonnes, in the annual emissions of CO_2 by the year 2005. In this context, the virtual reduction of 1600 million tonnes already achieved by nuclear is not insignificant.

---

* "Nuclear Power and the Greenhouse Effect", Atom, 390:33, April 1989.

** "The IAEA's Contribution to Sustainable Development", Vienna, May 1989

FUTURE NEEDS FOR NUCLEAR POWER

(Session II)

Chairmen

S. FINZI
Commission of the European Communities

J.F. MARCHATERRE
United States of America

GLOBAL AND REGIONAL ENERGY SCENARIOS FOR THE REDUCTION OF CO_2 EMISSIONS AND THE ROLE OF NUCLEAR POWER

W. HÄFELE
Kernforschungsanlage Jülich GmbH,
Jülich, Federal Republic of Germany

Abstract

The paper investigates the possibilities for a significant reduction of CO_2 emissions by 2030. The target figure for such a reduction is 4 GtC/year while the present energy related CO_2 emission is at 6 GtC/year. Such a target can only be met if all possibilities are being made use of, that is: a change of the fossil fuel use, the use of recycled biomass, of non carbon alternative energy sources, of nuclear power and the introduction of significant energy conservation. To that end existing energy scenarios are evaluated and a new scenario is introduced, the 1989 Jülich CO_2 reduction scenario for 2030. The Low Scenario of the International Institute for Applied Systems Analysis (IIASA) of 1975 serves a a reference case. Against that case the energy conservation scenarios of Colombo/Bernardini and of Goldemberg et.al. are compared. It turns out that only extreme measures can alleviate the situation of CO_2 emissions. Thus the paper essentially answers the question: "how impossible is impossible?" The difficulties become apparent when not only global figures but sub scenarios in seven different comprehensive world regions are being considerd. It turns out that nuclear energy contributes in the 1989 Jülich scenario not only for electricity generation but also for high temperature nuclear process heat used for the reformation of natural gas. A total of 2 TWe of electricity generation capacity (partly meant as the equivalent of high temperature nuclear process heat) appears as necessary in the 1989 Jülich scenario. It nicely compares with the OECD/IAEA high estimate for 2025 which was 2.16 TWe.

1. Introduction

The present capacity of nuclear power is stalling, within the various countries and worldwide. The capacity of commercially committed nuclear power in 1987 was worldwide a total of 308 GWe producing about 5 % of the thermal total of world energy generation. A more exact figure for 1988 (end of the year) is 331 MWe. By contrast, the OECD/IAEA low estimate for 2000 was 497 GWe, the high estimate 646 GWe [1]. Both estimates were elaborated shortly before the Chernobyl accident and the gap between these estimates thus sheds a light on its consequences. At 360 GWe, a value that was envisaged during the 1988 meeting of the Japan Atomic Industrial Forum -that is after the Chernoby accident - by the author [2] for a saturation type pessimistic after Chernoby worldwide nuclear capacity and at 30 tU/GWe year a total of 3 mio t of natural uranium would arithmetically last for 275 years. Under such conditions the establishment of a closed fuel cycle and of a population of breeder reactors is unlikely to come for reasons of fuel supply. But there are other reasons than Chernobyl for the stalling of world nuclear capacity: a lack of additional demand for electricity and low oil prices.

Into that situation came the message of the Toronto Conference of 1988 [3] concerning the problem of the state and prospect of the global atmosphere in general and its CO_2 contents in particular. A goal for 2005 was given: a 10 % reduction of the 1988 CO_2 emissions from the side of energy production and a further 10 % reduction from the side of energy end uses. Today, 1988/1988, such CO_2 emissions amount to 6 GtC/year, the carbon in the chemical form CO_2. About 1 GtC/year comes additionally from non energy sources thus arriving at a value of 7 GtC/year. By contrast, for the middle of the next century a value somewhere at 2,5 or 3 GtC/year is deemed necessary. Such an amount could possibly be accepted by the dynamics of the oceans connecting the surface to the deep sea, the place of final disposal of such carbon.

In that situation it is necessary to engage all options for the reduction of CO_2 emissions. These options are the following ones:

1.) a change of the mix of fossil fuels towards a higher hydrogen content

2.) the engagement of biomass as a fuel which is considered to permit for the recycling of the carbon atom

3.) the engagement of carbon free solar based energy sources such as hydropower, wind and direct uses of solar power

4.) the large scale engagement of nuclear power

5.) the engagement of energy conservation, primarily through improvements of efficiencies.

Such large scale engagement of nuclear power differs sharply from the pessimistic after Chernobyl saturation type value of 360 GWe envisaged above. It is the purpose of this paper to address the question: how much ? To that end it is helpful to conceive scenarios for the various regions of the world, not only for the world as a whole. Too high a degree of aggregation clouds the issues. Such regional scenarios must identify the contributions 1.) through 5.) with a special attention to 5.), that is the degree of energy conservation This is the case for reasons of substance and in order to understand ongoing political controversies.

2. The IIASA Low Scenario as a reference

At the International Institute for Applied Systems Analysis (IIASA) two Scenarios, High and Low, were conceived and elaborated in considerable detail. That was in 1975. The two scenarios were later carefully documented [4]. In 1975 the reality of the CO_2 effect was still debated and not yet fully accepted. Thus the CO_2 effect was not a view point for their conception while the effect as such was indeed elaborated on and explained in the IIASA Publication [5].

Both IIASA scenarios considered the seven IIASA World Regions. In so doing it was not necessarily geographical proximity that mattered. Instead, their composition reflects features of economy, population growth and resources which they have, to a degree, in common. Fig. 1 illustrates the composition of these IIASA World Regions.

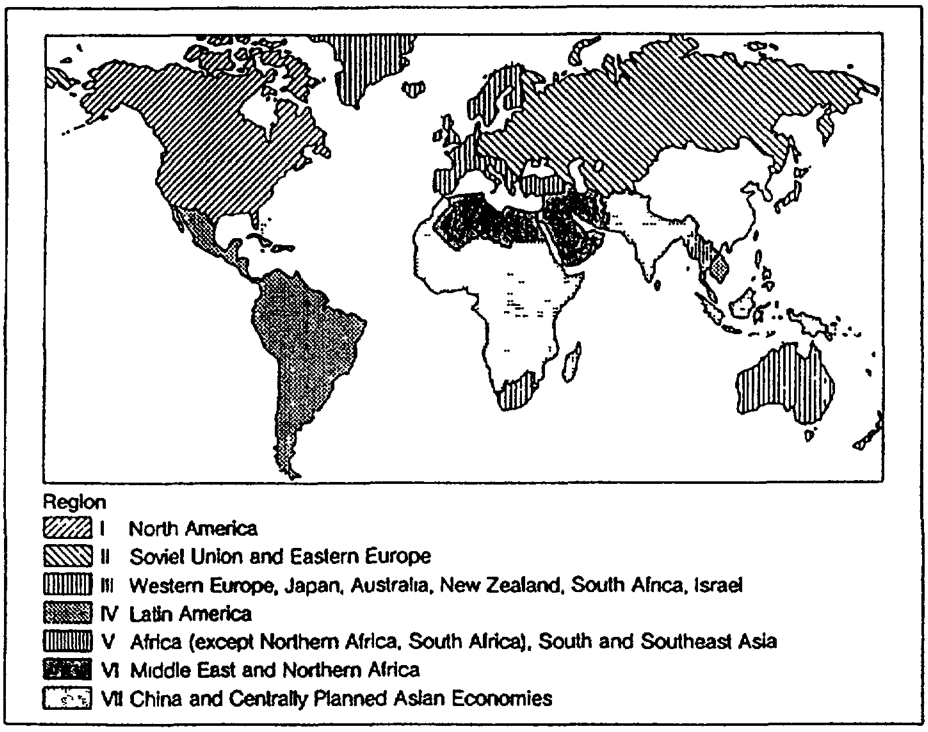


Figure 1: The seven IIASA Regions

TABLE I COMPARISON OF THE IIASA LOW SCENARIO FOR SEVEN WORLD REGIONS WITH THE ACTUAL DEVELOPMENT 1970-1987, CONSUMPTION OF PRIMARY ENERGY (GWyears/year)

Region	1970		1975		1980		1985		1987	
	IIASA	BP	IIASA	BP	IIASA	BP	IIASA	BP	IIASA	Bp
I (NA)	2363	2586	2654	2706	2742	2935	2830	2872	2894	2953
II (SU/EE)	1462	1611	1835	2048	2067	2458	2300	2757	2435	2895
III (WE/JANZ)	1825	1995	2256	2188	2473	2397	2690	2424	2783	2517
IV (LA)	247	268	338	359	449	481	560	542	615	572
V (Af/SEA)	266	361	328	442	449	639	570	811	637	913
VI (ME/NAf)	59	98	126	134	198	168	270	226	309	235
VII (C/CPA)	285	411	461	582	545	735	630	902	677	993
World	6507	7338	8210	8462	9030	9814	9850	10536	10349	11084

Source: For IIASA - V. G. Chant. Two global scenarios: The evolution of energy use and the economy, IIASA - Research Report RR-81-35, 1981
For BP: BP Statistical Review of World Energy, 1988

Note: No adjustments of BP Data to IIASA aggregations are made, the data are given as reported by BP

In 1975 the world consumption was 8.21 TWyears/year. In 1987 the BP Statistical Review gives 11.08 TWyears/year for that year. Table I compares the IIASA Low data with the actual development as given by the BP statistics.

Given the fact that the aggregation of the BP data into the IIASA World Regions poses some difficulties it turns out that the IIASA Low Scenario is indeed close to the real development over the past 12 years, not only for the world as a whole, but also, to varying degrees, for the World Regions individually. Therefore we will from now on refer for reference purposes only to the IIASA Low scenario.

TABLE II. COMPARISON OF ENERGY SCENARIOS FOR 2030 (2020) (I)

	Primary Energy [TWyears/year]			Population [Mio]				
Region	2030 IIASA Low	2030 Colombo	2020 Goldemberg	1975 IIASA	1987	2030 IIASA	2030 Colombo	2020 Goldemberg
I (NA)	4.37	2.52		237	267	315	315	
II (SU/EE)	5.00	2.98	4.3	363	423	480	480	1240
III (WE/JANZ)	4.54	2.45		560	601	767	767	
IV (LA)	2.31	2.23		319	424	797	797	
V (Af/SEA)	2.66	2.50	6.9	1422	1975	3550	3550	5710
VI (ME/NAf)	1.23	1.27		133	160	353	353	
VII (C/CPA)	2.29	2.05		912	1148	1714	1714	
World	22.39	16.00	11.2	3946	4998	7976	7976	6950

TABLE III IIASA LOW SCENARIO OF GLOBAL PRIMARY ENERGY BY SOURCE, 1975-2030 (TWyears/year)

Primary Source[a]	1975 IIASA	1987 BP[e]	2000 IIASA Low	2030 IIASA Low
Oil	3.83	4.19	4.75	5.02
Gas	1.51	2.20	2.53	3.47
Coal	2.26	3.39	3.92	6.45
Nuclear	0.12	0.57	1.29	5.17
Hydroelectricity	0.50	0.73	0.83	1.46
Solar[b]	0	0[f]	0.09	0.30
Other[c]	0	0[f]	0.17	0.52
Total[d]	8.21	11.08	13.59	22.39

[a]Primary fuels production or primary fuels as inputs to conversion or refining processes.
[b]Includes mostly "soft" solar - individual rooftop collectors - also small amounts of centralized solar electricity.
[c]"Other" includes biogas, geothermal, commercial wood use.
[d]Columns may not sum to totals because of rounding.
[e]The data are given as reported by BP, without adjustments to IIASA aggregations
[f]No data reported.

The IIASA Low Scenario conceives a 22.30 TWyear/year level of primary energy supply for 2030 (see Table II) thus essentially reflecting a bit less than a 2 % growth rate, not an unreasonable figure. Reasonabless refers to growth rates in the individual Regions, a degree of energy conservation, and changes in the structure of the economy. It thus may provide a yardstick for the further consideration here. Table III gives the IIASA Low Scenario by primary energy sources. In 2030 nuclear energy is seen to contribute 5.17 TWyear/year of thermal power. It is composed of 1.89 TWyears/year coming from LWRs and 3.28 TWyears/year from FBRs [6] reflecting an installed capacity of 1.1 TWe for the LWRs and of 1.9 TWe for the FBRs, a total nuclear capacity of 3 TWe.

One may want to compare this figure with the OECD/IAEA high and low estimates for 2025, high is 2.16 TWe and low 0.875 TWe [7].

3. The Colombo and Goldemberg Energy Conservation Scenarios

The necessity to pursue generally the improvement of energy end use efficiencies and more generally the conservation of primary energy is recognized practically by all and is definitly not controversial. Instead, it is the degree of such energy conservation that is indeed controversial. A reduction of primary energy uses by 10 or 20 % is certainly feasible, although one has to realize that such observations are usually meant as a worldwide average, and then such stated feasibility is already questionable while for OECD countries that does not seem to be the case. But a degree of conservation of 50 % is already another matter. Usually it is the substitution of energy by capital or labor that is implicitly or explicitly implied. Thereby the issue of the feasibility of high degrees of energy conservation becomes a matter of economy and that includes competitivity among states and industrial firms. And further, it becomes a matter of innovation and eventually of public acceptance of radical changes of societal patterns. Thereby the issue becomes open ended.

TABLE IV. GROSS DOMESTIC PRODUCT, PRIMARY ENERGY CONSUMPTION AND ENERGY INTENSITIES 1988

Country	Area [10^3 km^2]	Population [10^6 cap]	GDP/cap [$ 1987/cap]	PEC/cap [toe/cap]	ElC/cap [MWh/cap]	PEC/GDP [toe/10^3 $ 1987]	PEC/GDP [Wyr/$ 1987]
FRG	249	61,20	18 264	4,35	6,88	0,24	0,32
France	544	55,63	15 817	3,53	6,45	0,22	0,30
India	3 288	786,00	270	0,29	0,25	1,07	1,43
Italy	301	57,33	13 224	2,58	3,50	0,20	0,26
Japan	372	122,09	18 876	3,09	5,78	0,16	0,22
PR China	9 597	1 077,00	330	0,66	0,44	2,00	2,66
Sweden	450	8,40	18 810	6,62	17,50	0,35	0,47
UK	244	56,93	11 765	3,60	5,32	0,31	0,41
USA	9 363	243,91	18 338	7,58	11,13	0,41	0,55
USSR	22 402	284,00	8 000	5,08	5,86	0,64	0,85
World	135 830	4 980,00	3 370	1,59	2.05	0,47	0,63

GDP: Gross Domestic Product

PEC: Primary Energy Consumption

ElC: Electricity Consumption

A way to address that issue is the consideration of energy E over Gross Domestic Product GDP ratios. In the seventies a typical figure for the OECD countries was 1 Watt year/US$. Nowadays a figure of 0.5 Watt year/US$ is more appropriate but only partially because of the Watt years, more so because of the inflated monetary units and their quickly varying exchange rates. Table IV lists recent data as compiled by EDF. One realizes the wide gap between OECD data and data for the USSR and China. This large gap illustrates the difficulty of worldwide averages.

Given these opaque circumstances one is prepared to consider the two energy conservation scenarios of Colombo-Bernardini and of Goldemberg-Johanson-Reddy-Williams. The Colombo scenario was conceived in 1978 to establish a contrast to the IIASA Low Scenario [8], and so the two scenarios were compared by the author [9]. Such comparison was eased by the fact that the Colombo scenario makes use of the IIASA World Regions. The Goldemberg scenario was conceived much later [10]. It is less disaggregated region wise but it does refer to the IIASA Low scenario and thus permits for a comparison too.

The conception of the Colombo scenario was certainly not much influenced by the CO_2 problem, it was too controversial still by 1978, and this it has in common with the IIASA Low Scenario. To what extent the CO_2 problem had influenced the conception of the Goldemberg scenario is not known by the author. But one should realize that the Goldemberg et al. study [10] of which the scenario is an important part had a determining influence on the widely recognized so called Brundtland Report [11]. This Brundtland Report is named after the Norwegian Prime Minister Gro Harlem Brundtland who served as the chairperson of the World Commission on Environment and Development, Our Common Future. The report of this Commission [12] in turn was of major influence during the Toronto CO_2 Conference mentioned above. In fact, the Norwegian Prime Minister was present when the Canadian Prime Minister Brian Mulroney opened the conference and especially greeted and cheered.

It is against such a background that the nuclear community should recognize the low posture that was given for nuclear power in the Brundtland report. It was given an ambigious if not negative place [13] compared with the case of renewable energy and particularly energy conservation whose opaque circumstances were not elaborated on. It is without doubt that the nuclear community is challenged to take position, make its case and respond with a view of the global long range issues and particularly the CO_2 issue. The statement of the Toronto Conference did ask for a "revisiting of nuclear power" and such revisiting of nuclear power should take into account the problems of reactor safety, final waste disposal and non proliferation of nuclear weapons. One should bear in mind that the Non Proliferation Treaty expires in 1995 and thus its extension or reshaping is an important task during the forthcoming years.

The essence of the Colombo scenario is to maintain the average per capita consumption of primary energy through the years to 2030 and possibly thereafter while the essence of the Goldemberg scenario is to maintain the present primary energy consumption as a whole. The difference comes from the population growth. Therefore Colombo admits a further increase to 16 TWyears/year while Goldemberg sticks to the present 11 TWyears/year. Table II compares the three scenarios for the seven IIASA world Regions including their expected populations. One should note the relatively small differences in the totals for the IIASA Regions IV - VII that more or less represent the Developing Countries (LDCs). IIASA has a total of there of 8.49, Colombo of 8.05 and Goldemberg of 6.9 TWyears/year. When the IIASA Low Scenario was conceived a number of analysts from the LDCs participated.

TABLE V. COMPARISON OF ENERGY SCENARIOS FOR 2030 (2020) (II)

	Per Capita Consumption of Primary Energy [kW/cap]					GDP Growth Rate [%/year]		
Region	1975 IIASA	1987 BP	2030 IIASA Low	2030 Colombo	2020 Goldemberg	1975 - 2030 IIASA Low	Colombo	Goldemberg
I(NA)+II(SU,EE)+ III(WE/JANZ)	5.82	6.48	8.90	5.09	3.5	2.09	2.00	n.r.[a]
IV(LA)+V(Af,SEA)+ VI(ME/NAf)	0.43	0.67	1.32	1.28				
VII(C/CPA)	0.5	0.86	1.30	1.20				
IV(LA)+V(Af,SEA)+ VI(ME/NAf)+VII(C/CPA)	0.45	0.73	1.32	1.25	1.26	3.24	3.84	n.r.[a]
World	2.08	2.22	2.80	2.0	1.6	2.37	2.50	n.r.[a]

[a] n.r.: not reported

TABLE VI. COMPARISON OF FINAL ENERGY SCENARIOS IN THE OECD FOR 1975, 1986 AND 2030 (GWyears/year)

	1975		1986	2030		
	IIASA	OECD[b]	OECD[b]	IIASA Low	Colombo[c]	% Reduction[a]
Region I(NA), Total	1871	1823	1896	2656	1819	-32
Industry	757	590	573	1327	818	-38
Transportation	541	590	662	688	410	-40
Household-service	573	-	-	641	591	-8
Other Sectors	-	643	661	-	-	-
Region III(WE/JANZ), Total	1589	1487	1637	3143	1723	-45
Industry	805	631	594	1588	725	-54
Transportation	313	307	415	716	394	-45
Household-service	417	-	-	839	604	-28
Other Sectors	-	549	628	-	-	-

[a]Percentage reduction from the Low Scenario for the Colombo Scenario, as a percentage of the Low Scenario
[b]OECD statistics of 1987
[c]Based on the evaluation of the "16TW" case in EIFW [4]

They insisted that a higher energy demand, while helpful as such, could not easily be seen because of a lack of corresponding feasible economical development. A higher economical growth rate was reflected in the IIASA High Scenario, not reported here. Its total for the IIASA Regions IV - VII is twice as high, 15.16 TWyears/year. If the totals for the LDCs are essentially the same for the three scenarios their difference comes from the industrialized World Regions I - III, that is the OECD and the Comecon countries.

Indeed, IIASA has there a total of 13.91, Colombo of 7.95 and Goldemberg of 4.3 TWyears/year. Table V exposes the same situation in terms of per capita values. IIASA Low permits a slight increase of the world's average from 2.08 kWyears/year in 1975 to 2.80 kWyears/year in 2030 while Colombo sticks to 2.0 kWyears/year and Goldemberg can allocate only 1.6 kWyears/year (2020) because the population increases while Goldemberg demands a constant over all primary energy consumption. Table V exposes also the expected GDP growth rates. Colombo expects higher growth rates than the IIASA Low Scenario. The reason is the expectation of sharply decreasing E/GDP ratios as discussed above. Such reductions of final energy (e.g. gasoline or electricity) are reflected in Table VI for Region I (North America) and Region III (the rest of OECD) as there are the data available. OECD data there cannot precisely be compared because of a somewhat different disaggregation. But one realizes the general fact that Colombo expects for 2030 values that are already obtained in 1986 while IIASA permits for modest increases.

TABLE VII. ESTIMATED GLOBAL AVERAGES OF CARBON CONTENT IN FOSSIL FUELS

	Gt C/TWa
Coal	0.751
Liquids	0.605
Gas	0.432

4. Technical elements for a reduction of CO_2 emissions

Having dealt with the element of energy conservation respectively efficiency improvements of energy end uses one also has to evaluate the other possible measures for the reduction of CO_2 emissions 1.) - 3.) as explained above before one addresses measure 4.), the case of nuclear power that is the interest here.

ad 1.)
A change of the fossil fuel use can possibly help significantly. Table VII gives the carbon content in fossil fuels as an estimated global average. For one unit of energy natural gas releases only 57 %, and oil 80 % of the CO_2 amounts that are released by coal. But one has to realize that methane is a Greenhouse gas itself and contributes to global warming 32 times as much as CO_2 when compared on a molecule by molecule basis. The effective carbon content equivalent therefore follows the relationship

$$\frac{GtC}{TWa} = 0.432 \quad (1 + l \times 32)$$

if l is the ratio of methane moles last per methane moles actually oxidized. If l equals 2.3 % the effective carbon content of methane equals that of coal. Actual losses of methane that remain in the atmosphere are in that range but not really known yet. For the purposes here we therefore assume that l can be kept small but attention must be paid to further related information.

C. Marchetti has proposed [14] to reform natural gas by the use of the High Temperature Reactor (HTR) according to the relation

$$CH_4 + 2\ H_2O \longrightarrow CO_2 + 4\ H_2$$

His idea is to pump the CO_2 so generated into the very some underground caves where the CH_4 was taken from. This would be a novel use of methane together with nuclear power that does not generate Greenhouse gases. The technology of applying exogeneous heat to the reformation of methane has been successfully proven at KFA Jülich in the 10 MW range. It is known as the EVA scheme [15].

ad 2.)
The use of biomass follows the idea of carbon recycling. Therefore if one unit of biomass is burned per unit of time one such unit of biomass must be replanted per unit of time. Goldemberg et al. envisage in principle a global potential of as much as 5 TWyears/year [16]. As such this is a sound idea. Nevertheless, one should be aware of its implications. Under natural circumstances the power production density of biomass is close to 0.2 W/m^2 [17]. Assuming an enhanced value of 0.3 W/m^2 a total of 5 TWyears/year would imply an area of about 17 mio km^2. The present global agricultural uses of land make up for about 13 mio km^2. Besides of the sheer size of such additional land uses such large scale uses of biomass imply large logistic problems of transport and management. One should bear in mind that the average power consumption density in urban areas is 5 W/m^2 [18]. A city like Vienna covers an area of about 600 km^2, for its supply on the basis of biomass it would therefore require 10 000 km^2. Given streets, villages and other uses of land this would come effectively close to an area of perhaps 150 km x 150 km. Indeed, prior to the first industrialized revolution when wood was the principal source of energy such land use patterns existed around Vienna and created severe problems. There will be other problems like ecological consequences or recycling of nutrients. The exact nature of these implications are certainly not fully understood yet. They vary also from region to region and are certainly different in Brasil and Austria. One therefore can only assume that a total of perhaps 1.5 TWyears/year or so is a more realistic guess. And such a value was indeed used in the Goldemberg scenario.

ad 3.)
Carbon free solar power refers to hydropower, to local uses of solar power and to large scale central uses of solar power. The global total of hydropower is somewhere at 1 TWe year/year and therefore of the same order as the above considered case of biomass. Much of such potential of hydropower is already used. This is notwithstanding the fact that locally additional uses of hydropower lend themselves very much. Places in South America and Africa provide examples for that. Large scale uses of solar power provide indeed the opportunity for significant supplies of power in the several TW range. In sunny arid areas, say the north African deserts, a value of 10 We/m^2 gives a reasonable over all average. At 1 mio km^2, in these desert areas not an unreasonable figure, this results in as much as 10 TWe. It is generally known that the over all costs are still inhibitive. Only partly this relates to the costs of photovoltaics, much goes to power conditioning and other infrastructures. It is not the purpose of this paper to elaborate on future uses of solar power and other alternative sources, it is nuclear power that is of interest here. Therefore the above remarks should suffice.

5. The 1989 Jülich CO_2 reduction scenario

It is now possible to conceive a CO_2 reduction scenario against the background of the considerations made above. This will in turn be instrumental for the assessment of the role of future uses of nuclear power in such a context. A number of explanations are in place:

a) The scenario assumes the reality of the CO_2 effect

b) The scenario is meant for 2030. By then an ultimatly satisfactory solution of the CO_2 problem can under no circumstances be expected. Therefore the scenario can only describe a transitional stage of world's energy systems.

c) Given the situation described under b) the scenario aims at a value of 4 GtC/year emission rate of CO_2. With 1 GtC/year coming from non energy sources this results in the 5 GtC/year mentioned above. Should they continue at that scale the CO_2 concentration would be accordingly less. Compared with the 1987 emissions of 6 GtC/year this would be a reduction of 33 % of that value.

d) The scenario is not the result of a mathematical model of any kind. But it does observe a number of constraints and follows certain reasons. Within the space so left it is judgemental and thus it asks for further work.

e) The scenario is not meant to be feasible in todays meaning of the word. Todays feasibilities do not allow for significant CO_2 reductions. Instead, the scenario exhibits a number of "impossible" features and essentially addresses the question: How impossible is impossible?

Given these explanations it is fundamental to assume the degree of energy conservation. In that respect the 1989 Jülich CO_2 reduction scenario follows the scenario of Colombo and Bernardini thus assuming a degree of energy conservation in the industrialized part of the world that is close to 43 % of the primary energy demand as foreseen by the IIASA Low scenario. This is felt to be on the high side of energy conservation. To what extent that is "possible" or "impossible" must remain open here.

The acception of features of the Colombo/Bernardini scenario goes further. This scenario makes use of the seven IIASA World Regions and when foreseeing 16 TWyears/year for the year 2030 it also allocates shares of that primary energy to the IIASA World Regions. Also these allocations are accepted. The question is then left how these shares of 16 TWyears/year can be provided by the uses of the various primary energy sources in such a way that a total of 4 GtC/year is not superceded. The answer to that question is in fact more difficult than it appears at a first glance.

Table VIII presents the 1989 Jülich CO_2 reduction scenario.

The allocation of oil is straight forwardly idealistic. Oil is the most precious form of primary energy requiring only a minimum of capital intensive infrastructure. Thus a major share of the over all figure of 3.5 TWyears/year is given the LDC's while the total of 1987 was 4.19 TWyears/year. For the OECD countries (Regions I + III) this would mean a halving of its present consumption, for China, Africa and South East Asia essentially a doubling.

The traditional uses of natural gas mostly continue. Certain reductions are expected for the Soviet Union while a doubling is expected for Latin America. 1987's total of 2.2 TWyears/year is reduced to 2.0 TWyears/year.

TABLE VIII. A 1989-CO_2-REDUCTION SCENARIO FOR THE ALLOCATION OF PRIMARY ENERGY (TWyears/year) TO THE SEVEN IIASA WORLD REGIONS FOR THE YEAR 2030

Region	Oil	Gas$_1$	Gas$_2$[c]	Coal$_1$	Nuclear$_1$[d]	Nuclear$_2$[c,d]	Solar[e]	Hydro[f]	Bio[g]	Total
I(NA)	0.6 (1.18)[a]	0.6 (0.67)	-	0.3 (0.69)	0.6 (0.20)	-	0.1	0.12	0.2	2.52[b] (2.95)
II(SU)	0.5 (0.82)	0.6 (0.88)	0.3	0.3 (1.01)	0.6 (0.08)	0.225	0.075	0.2	0.18	2.98[b] (2.89)
III(WE/JANZ)	0.6 (1.17)	0.4 (0.37)	0.2+0.2[h]	0.1 (0.53)	0.45 (0.26)	0.15+0.15[h]	0.05	0.07	0.08	2.45[b] (2.52)
IV(LA)	0.5 (0.31)	0.2 (0.10)	0.3[h]	- (0.03)	0.13	0.225[h]	0.2	0.17	0.505	2.23[b] (0.57)
V(Af/SEA)	0.7 (0.39)	- (0.09)	0.7[h]	0.2 (0.34)	- (0.03)	0.525[h]	0.2	0.07	0.105	2.50[b] (0.91)
VI(ME/NAf)	0.2 (0.17)	0.1 (0.07)	0.3	-	-	0.225	0.445			1.27[b] (0.23)
VII(C/CPA)	0.4 (0.15)	0.1 (0.02)	-	0.6 (0.79)	0.42	-	0.13	0.17	0.23	2.05[b] (0.99)
Total	3.5 (4.19)	2.0 (2.20)	2.0	1.5 (3.39)	2.2 (0.57)	1.5	1.2	0.8 (0.73)	1.3	Σ=16[b] (11.08)

[a]Values in brackets for comparison with 1987, from BP statistics
[b]Based on the Colombo scenario
[c]Assuming a shift from CH_4/H_2O to $CO_2/4H_2$
[d]Thermal equivalent
[e]Wind and photovoltaics, direct (electrical) output
[f]Direct (electrical) output
[g]Organic waste and plantations
[h]It may or may not be imported from other regions

But there are the new uses of natural gases (gas$_2$) together with nuclear power (nuclear$_2$) as described above, resulting in hydrogen. Such hydrogen may be transportable and such imports are assumed for Western Europe, Japan, Latin America and Africa (Regions III, IV and V) where natural gas sources are limited. But it is left open whether hydrogen or methane is transported. *One should realize that such novel uses double the uses of* natural gas, another 2 TWyears/year are engaged, but together with 1.5 TWyears/year of high temperature nuclear process heat. Otherwise it is not possible to meet the target of 4 GtC/year.

Coal in turn must be reduced by more than half, from 1987's 3.39 TWyears/year down to 1.5 TWyears/year. This is a serious cut for North America, more so for the Soviet Union and for Western Europe. But the most serious case is that of China which has to decrease somewhat its 1987 value instead of increasing it to 3 TWyears/year what is presently envisaged by state planners in that country.

Solar with a direct electrical output (wind, Photovoltaics) are given a total of 1.2 TWyears/year. That is more than twice the nuclear energy generation of 1987. It is purposely a high figure. The perception is that it could be less but not more. Most of these 1.2 TWyears/year are seen in the Middle East and Africa (Region V). All the allocations to the Regions as well as the over all figure are debatable, but resulting probably in lower values.

Hydro and Bio Sources are somewhat in line with estimates of the Goldemberg Scenario. This leaves 2.2 TW years (thermal)/year for nuclear electricity generation. It is on purpose that most of it is meant to come from the industrialized part of the world (Regions I-III). But China is given also a large share, otherwise it could not compensate for the waiver of additional coal uses.

TABLE IX. COMPARISON OF PRIMARY ENERGY (PE) IN TWyears/year AND CO_2 EMISSION (CO_2E) IN GtC/year IN VARIOUS SCENARIOS

	1987[a]		IIASA Low 2030		A-1989-Reduction Scenario 2030				Colombo 2030		Goldemberg 2020	
							reduced nuclear					
	PE	CO_2E	PE	CO_2E	PE	CO_2E	PE	CO_2E	PE	CO_2E	PE	CO_2E
Oil	4.19	2.53	5.02	3.04	3.5	2.12	3.5	2.12	1.72	1.04	3.21	1.94
Gas^b_1	2.20	0.95	3.47	1.50	2.0	0.86	2.0	0.86	0.99	0.42	3.21	1.39
Gas^b_2	-	-	-	-	2.0	-	-	-	-	-	-	-
$Coal^b_1$	3.39	2.55	6.45	4.84	1.5	1.13	1.5	1.13	4.95	3.72	1.94	1.46
$Nuclear_1$	0.57	-	5.17	-	2.2	-	0.75	-	1.74	-	0.75	-
$Nuclear_2$	-	-	-	-	1.5	-	-	-		-	-	-
Solar			}		1.2 }	-	1.2 }	-		-	0.09 }	-
$Hydro^c$	0.73	-	} 2.28	-	0.8 } 3.3	-	0.8 } 3.3	-	6.60	-	0.46 } 2.13	-
$Bio^{b,d}$			}		1.3 }	-	1.3 }	-		-	1.58 }	-
Total	11.08	6.03	22.39	9.38	16.00	4.11	11.05	4.11	16.00	5.18	11.24	4.79

[a] BP Statistics, 1989

[b] Not counting for any losses of methan to the atmosphere

[c] Direct (electrical) output

[d] Organic waste and plantations

The result of such a disaggregated approach is given in Table IX.

The 1989 Jülich CO_2 reduction scenario yields 4.11 GtC/year. By comparison, the Colombo/Bernardini scenario yields 5.18 GtC/year and Goldemberg 4.79 GtC/year.

The following helps to understand the so assessed role of nuclear power: For reasons of comparison one may want to reduce the role of nuclear power in the 1989 Jülich reduction scenario down to a value of 0.75 TWyears/year, the value that was considered by Goldemberg in his scenario. That relates to a capacity of about 400 GWe world wide, shlighly more than the above considered saturation type pessimistic after Chernobyl value of 360 GWe. This implies also the waiver of CO_2 free uses of natural gas (gas_2) though. One then arrives at 11.05 TWyears/year of primary energy use, and also otherwise numbers become comparable to those of the Goldemberg scenario. It was explained above that this means a reduction of primary energy uses in the industrial parts of the world, not of 43 % as it was the case in the Colombo Bernardini scenario but of 69 % of the IIASA Low Scenario value for 2030. The use of 3.7 TWyears/year of nuclear power instead of 0.75 TWyears/year avoids such a drastic and unreasonable decrease of primary energy uses and this is the core of the argument for nuclear power extended here.

6. 3.7 TWyears/year of nuclear energy

In the 1989 Jülich CO_2 reduction scenario 3.7 TWyears/year are given to nuclear power. This is less than in the case of the IIASA Low Scenario where the total is 5.17 TWyears/year. Out of these 3.7 TWyears/year a share of 2.2 TWyears/year is for electricity generation. Assuming a thermal efficiency of 0.4 (FBR and/or HTR) and a load factor of 0.7 this relates to a capacity of 1.25 TWe. As an orientation, one may further relate the 1.5 TWyears/year of high temperature nuclear process heat to an equivalent electrical power generation capacity of 0.75 TWe, if again a thermal efficiency of 0.4 but a load factor of 0.8 is assumed ad hoc. Therefore the total capacity would be 1.25 + 0.75 = 2 TWe and this is practically the OECD/IAEA high estimate for 2025. The advantage of this observation is the fact that all the fuel cycle implications like the ratio between breeders and burners, the capacities of reprocessing, the consumption of natural uranium can all be taken from the related OECD/IAEA study [7]. Therefore these fuel cycle considerations are not repeated here.

Instead, a reflection on the total number of nuclear reactors is in order. A capacity of 2 TWe means 2000 reactors at 1 GWe each. The capacity of 1988 which was 331 GWe would relate to 331 such units. Thus an increase by a factor of 6 is under consideration. It is observed that the safety features of the 2000 reactors here envisaged for 2030 must be improved by at least a factor of 6, better more, a factor between ten and one hundred, one or two orders of magnitude.

Then nuclear power can make this contribution to the decrease of CO_2 emissions considered here. Should all the optimistic assumptions about non nuclear non carbon primary energy sources not materialize the nuclear contributions had to be even larger.

Acknowledgement

The author wishes to thank Dr. E. Geissler for valuable help in the preparation of this paper

References

[1] Nuclear Energy and its Fuel Cycle, Prospects to 2025, Report by an Expert Group, OECD Nuclear Energy Agency and International Atomic Energy Agency, Paris (1987), Table 5.1, page 12.

[2] HAEFELE, W., "Energy Systems in the 21st century and the significant role of energy", (21st Japan Atomic Industrial Forum, JAIF-Conference, April 13-15, 1988, Tokyo), Genshiryoku Shiryo (Atomic Information), No. 210, 7, pp. 1-23, (1988).

[3] Toronto Conference Committee, Statement of the Conference: The Changing Atmosphere, Implications for Global Security, World Conference Toronto, Ontario, Canada, June 27-30, 1988.

[4] HAEFELE, W., (Program Leader), Energy in a Finite World (EIFW), Report by the Energy Systems Program Group of the International Institute for Applied Systems Analysis, Vol 2: A Global Systems Analysis, Ballinger Publishing Company, Cambridge, Massachusetts, (1981), chapters 14-20.

[5] Energy in a Finite World, [4], chapter 10.

[6] Energy in a Finite World, [4], Table 17-2, p. 522.

[7] Nuclear Energy and its Fuel Cycle, [1], Table 8, p. 33.

[8] COLOMBO, U., BERNARDINI, O., A low Growth 2030 Scenario and the Prospects for Western Europe, Report prepared for the Commission of the European Communities, Panel on Low Energy Growth, Brussels, (July 1979).

[9] Energy in a Finite World, [4], Chapter 18, p. 601.

[10] GOLDEMBERG, J., JOHANSSON, T.B., REDDY, A.K.N., WILLIAMS, R.H., Energy for a Sustainable World, Wiley Eastern Limited, New Delhi Bangalore Bombay Calcutta Madras Hyderabad, (1989).

[11] Energy 2000 - A Global Strategy for sustainable Development, A Report for the World Commission on Environment and Development, Led Books Ltd, London and New Jersey (1987).

[12] The World Commission on Environment and Development, Our Common Future, Oxford University Press, Oxford New York 1987.

[13] See Our Common Future, [12], pp. 181/189.

[14] MARCHETTI, C., "How to solve the CO_2-Problem without Tears?", Paper 7th World Hydrogen Conference, (Moscow, U.S.S.R., Sept. 25-29,1988).

[15] NIESSEN, H.F., BHATTACHARYA, A.T., BUSCH, M., HESSE, K., ZENTIS, A., Erprobung und Versuchsergebnisse des PNP-Röhrenspaltofens in der EVA II-Anlage, Rep. Jül-2231, Kernforschungsanlage Jülich, (Aug. 1981).

[16] Energy for a Sustainable World [10], Appendix A.4, pp.380-384.

[17] Energy in a Finite World [4], Fig. 6-3, p. 203.

[18] Energy in a Finite World [4], Chapter 23.

MAIN ISSUES REQUIRING RESOLUTION FOR LARGE SCALE DEPLOYMENT OF NUCLEAR ENERGY

A. GIRAUD, G. VENDRYES
Commissariat à l'énergie atomique,
Rocquencourt, France

Abstract

A new development of the nuclear energy in the world would certainly start in the United States : this paper is centered on this hypothesis.

The fast development of nuclear energy in France is interesting to observe in order to use elsewhere some of its characteristics : the care for being reasonably independent in the energy field plaid an important role in the decisions taken around 1973, at the time of the oil crisis. The safety organization remains narrowly linked to the technicians thanks to its Institute which is an autonomous part of the Atomic Energy Commissariat. The responsible organizations, being very few (including the only utility, EDF) can have a very fruitful dialogue between them and with the safety authorities.

Building standardized stations has lowered the construction time and the price.

The public acceptance has been helped by some financial measures and by an important information effort : visits in the stations have been a big success. Much remains to be done, in particular in the waste field.

Do we have to launch new, revolutionary reactor types ? We are personally in favor of evoluting existing types without any deep changes.

Our paper will be focused on the case of the United States, as we are convinced that a revival of nuclear energy in this country is a necessary condition -and we are not far to think that it is a sufficient one as well- for its revival worldwide.

The use of nuclear energy by countries which are still lagging behind in the process of economic development faces tremendous difficulties, among which insufficient or inadequate infrastructures, shortage of financial resources and lack of a large enough number of well trained people. In spite of the extremely valuable assistance of the IAEA, much effort and a long time will be needed before those countries will be able to turn nuclear energy to account at any significant scale. One cannot imagine them doing so as long as the industrialized nations do not again move forward aggressively along that way. Concerning the latter, it should be remembered that those which have reduced or even stopped their nuclear energy programs did so in the wake of the grassroot opposition which started in the United States about

20 years ago and which spread out as a forest fire elsewhere. We are convinced that the pendulum will swing back in some future, and that, as before, signals coming from the United States will prove decisive for the rest of the world. This will be a fair return.

Before considering the American scene, it could be helpful to summarize the experience gained with the French nuclear energy program, and to stress the saliant features which made it on the whole successful. Indeed, it was not devoid of shortcomings, but from those too, lessons can be drawn. Resolve and determination at the highest levels of the Government have provided the impetus for the French nuclear energy program, which became a national challenge. Aiming at the security of energy supply of France, a strong commitment to nuclear energy was endorsed by all successive Government leaders and by all political parties. The Constitution of the Fifth Republic approved in 1958 gives to the Executive Branch broad powers in the areas of economy, industry and research. It is highly suited to the conduct of vast and expensive programs, whose payoff lies in the distant future.

The Ministry of Industry which is in charge of the civilian nuclear program, and which supervises both EDF and the CEA, includes the SCSIN (Central Service for Safety of Nuclear Installations), whose responsibilities are to implement procedures concerning the safety of nuclear power plants and facilities, to write applications for their construction and start-up approval by the Government and to monitor proper operation, among other things. This ensures the separation, which is necessary as a matter of principle, between those in charge of promoting and implementing nuclear technology and those responsible for authorizing its use.

However, the research and development on nuclear safety and the safety analyses, which are essential for the authorization procedures, are carried on for SCSIN by IPSN (the CEA's Institute for Nuclear Protection and Safety), which has the necessary technical skills. The normal and permanent exchange of personnel between the IPSN and the other departments of CEA is a key practice to insure a level of excellence at IPSN through the continuous introduction of scientists and engineers who have acquired their expertise by daily contact with specialized technical matters.

The administrative steps in an authorization procedure include among others a public inquiry, the approvals of various ministries and consultations with the "Groupe Permanent", an advisory commission which plays a role similar to the ACRS. They are no fewer in France than in the U.S. For a nuclear reactor for instance, EDF must submit a preliminary safety report, a provisional safety report and a final safety report to obtain successively the construction permit, the start-up permit and the operating licence. It must be emphasized that the procedures are implemented by specialists and not by bureaucrats. Rules and standards, which are continuously kept up to date through the feedback of experience gained with the operation of existing plants, are as pragmatic as possible. Generally speaking, one prefers to draw up guidelines for the specified objectives rather than to impose the means to reach these goals. It is believed that it would be totally unhealthy, counterproductive and damaging for technical issues to be dealt with in public and constantly exposed to criticism and statements by just everyone. The procedures assure a rigid protocol and process for any intervention by private individuals and organizations.

The safety procedures in France are long and stringent. Every aspect of design, manufacture and assembly of components, commissioning and operation of any nuclear installation is looked after in depth and with great care by the Safety Authorities. But, at the same time, the rules of the game are well known and well tested for everybody and they are not likely to change for a given plant, except in the rare occurence when a major new problem is discovered in the course of its construction or operation. That means that under normal conditions, the overall duration of the procedures till the issuance of the start-up permit can be reasonably well foreseen.

This system has operated very satisfactorily, producing the sought-after dialogue and flexibility. It is our feeling that the level of safety achieved in this manner is at least equivalent to that found in other countries.

EDF has a monopoly on the distribution and sale of electricity in France and accounts for 90 % of the nation's electricity production. It is the biggest utility of the Western World, and it is well equipped to master very large construction projects and to manage all operational aspects. It draws its outstanding expertise on a long tradition developed through the successive construction of a large number of hydroelectric dams, conventional stations burning fossil fuels and nuclear power plants of various kinds.

The greatest care is taken by EDF to the training of its personnel. As an example, the commissionning of 9 reactors in 1980 meant training some 40 highly qualified teams of operators.

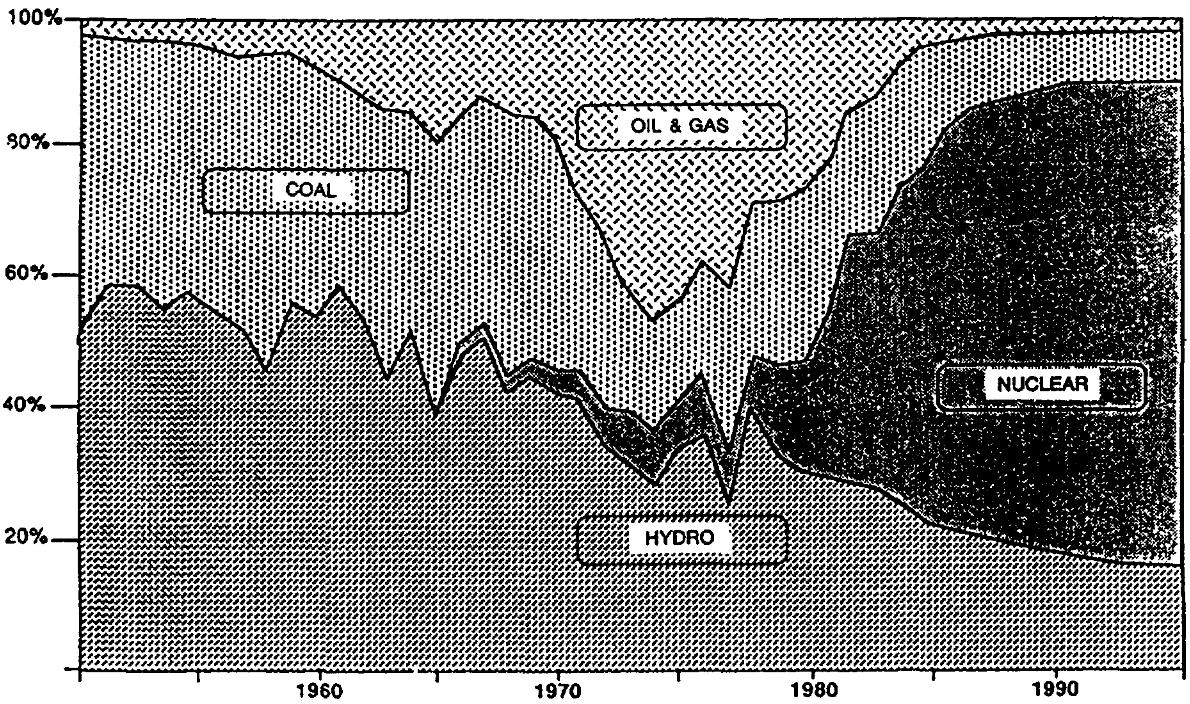


FIG. 1. Evolution of French electricity generation per energy source.

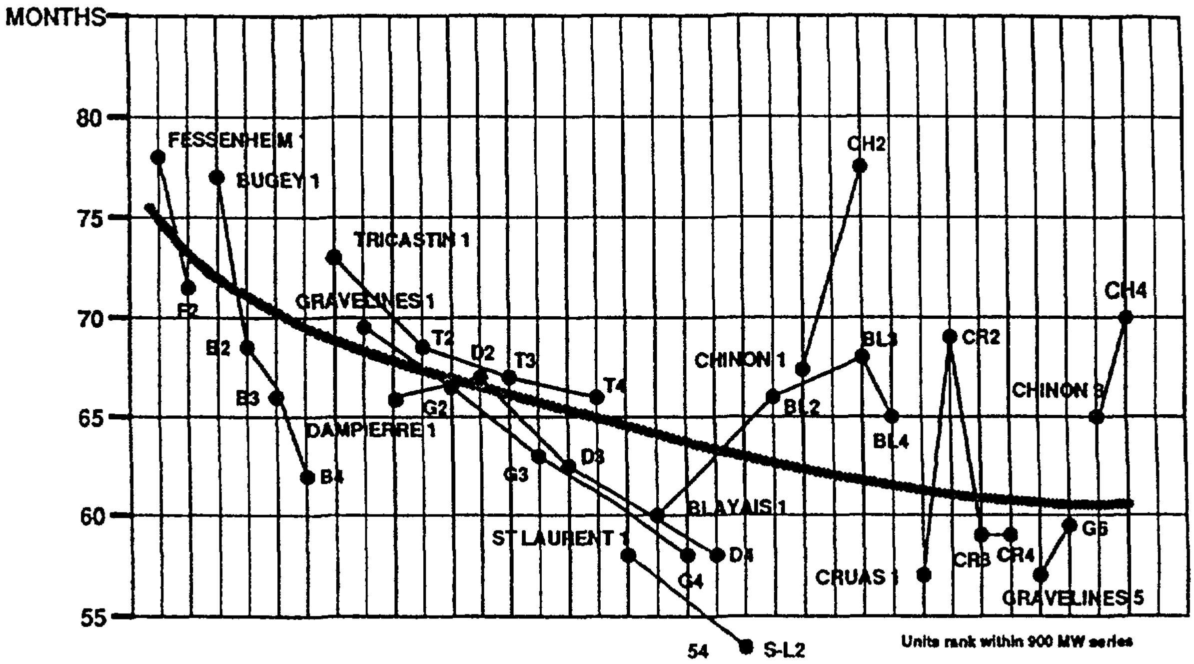


FIG. 2. Actual construction times of 900 MW PWR units (construction time from boiler commitment to first connection to the grid).

Obviously the intensive use of various types of operation simulators is vital.

A few figures illustrate what has been achieved by EDF.

Fig. 1 shows how the share of various energy sources to produce electricity in France evolved over the last 40 years. In 1988, roughly 75 % of the electricity generated by EDF came from nuclear power plants.

Fig. 2 gives some data concerning the time which was needed for the construction of the successive 900 MWe PWR's built in France.

Concerning the operational record of the French PWR's over the years, fig. 3 shows the average energy availability of the 900 and 1300 MWe units, fig.4 the average exposure of personnel (roughly 2 man.sievert per unit and per year), fig. 5 the average number of unplanned scrams, which is expected to go down further in the years to come, and fig. 6 the dramatic reduction in the release of SO_2 and of nitrogen oxydes in the atmosphere, as a result of the replacement of fossil fuel burning plants by nuclear ones.

The CEA is a unique organization, which has no exact equivalent outside France. It is a Government agency whose main responsibilities concerning the peaceful uses of nuclear energy, are the following :

. The CEA advises the Government on the nation's nuclear program, and on international nuclear policy, exports and non proliferation ;

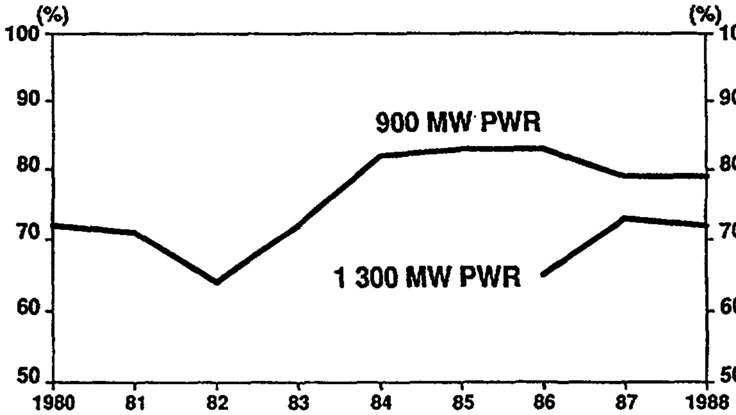


FIG. 3. Energy availability (PWR units in commercial operation).

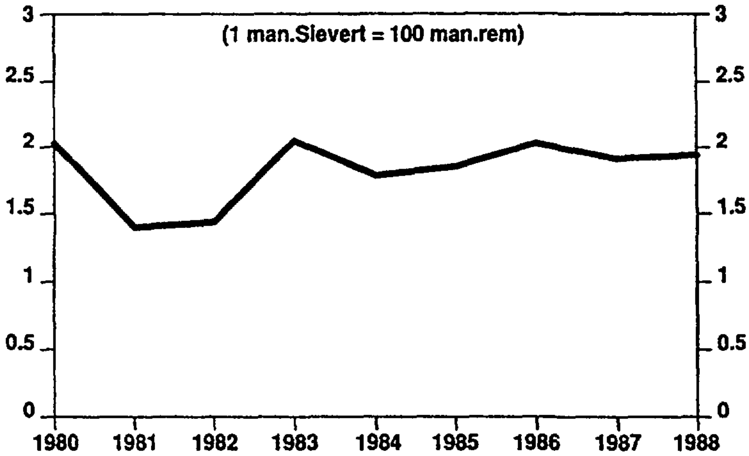


FIG. 4. Annual collective dose per PWR unit in commercial operation (man·sievert).

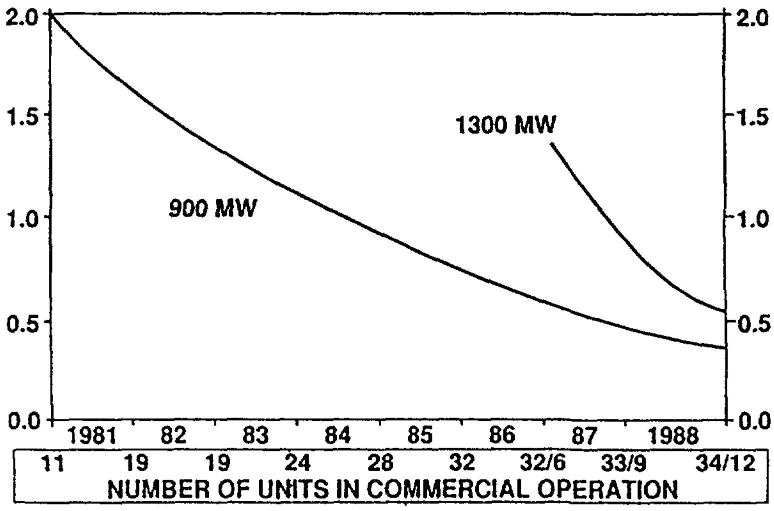


FIG. 5. 900 and 1300 MW PWR units unplanned automatic scrams (per 1000 hours of operation).

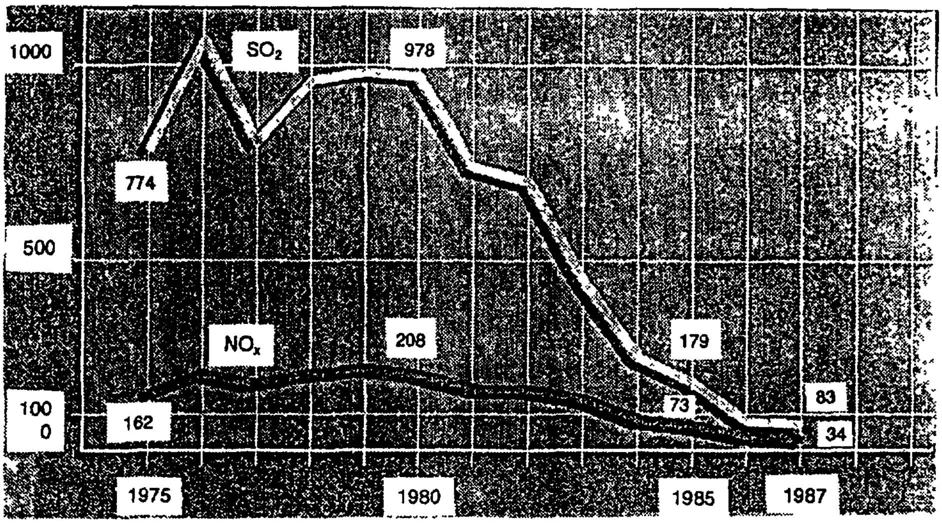


FIG. 6. Releases of SO_2 (thousands of tons) and NO_x (thousands of tons NO_2) from French power plants.

. It is in charge of most R & D programs on nuclear reactors and their fuel cycle ;

. As a shareholder of Framatome- Novatome it is directly involved in the activities of the French builder of nuclear plants and in particular in its industrial and commercial strategy ;

. Through its various affiliates, including Cogema, Eurodif, and others, the CEA has become an industrial and commercial leader in all phases of the fuel cycle, including prospection and mining of uranium deposits, enrichment, fuel fabrication, reprocessing, packaging and storage of radwastes.

Industrial activities in the nuclear field are highly concentrated in France. Framatome, which initially acquired a large part of its technical experience through a license agreement with Westinghouse, is the sole company which designs nuclear islands for EDF plants, provides their engineering and manufactures the essential components, such as reactor vessels and steam generators. Through its subsidiary Novatome it plays a similar role for FBR's. Fragema, a joint affiliate of Framatome and Cogema, has a de facto monopoly on the design and sale of LWR fuel. In addition Alsthom Atlantique is the only company in France which designs, fabricates and sells high power turbogenerators, in particular all those used in EDF power plants. All these industrial firms have an excellent technical expertise. It is expected that the international agreements which are now being implemented will further extend, not only the scope of the activities, but also the strength and the competence of these companies. As you may know, Alsthom and the Power Systems Division of the British General Electric Company will be merged, and the links between Siemens-KWU and Framatome will become closer and closer.

This summary of the French situation shows that in the nuclear area, the major actors are very few. Even if their interests may differ, they maintain close and trustworthy relations with each other, and they elaborate jointly a coherent nuclear strategy. Of course the final decisions are made by the Government but only after they have been discussed and prepared by the interested parties.

A particularly important decision, was to construct the power plants in series made of identical units. It raised some basic questions. For instance, what would happen if, after many plants are in operation, a major generic defect would appear on one unit, serious enough to oblige shutting down all the others for repair and modification works ? It would undoubtedly have been a rash decision to adopt such a policy for series of reactors based on a still insufficiently demonstrated technology. But this was no more the case in 1973, as the LWR technique could draw on extensive experience, especially in the U.S. The few generic problems which were encountered later on could always be cured in turn on the various plants involved, so that they had not to be shutdown all at a time. The French experience with standardization revealed many advantages. Construction times were shortened, and successive plants in a series were built more efficiently. Procurement of components for a series led to cost reduction in manufacture and in some cases components were shifted from one plant to another when the need arose during construction. The safety analysis for the lead plant in a series was generally applicable to the subsequent ones, thus streamlining regulatory approval. Training of personnel was efficiently concentrated at training facilities for each series and operators were to a high degree qualified for duty at any plant of the series.

Let us turn now to the situation of nuclear energy in the United States. At present, it is a rather depressed one.

The main obstacle to revival of nuclear energy in the U.S. is that public acceptance is still inadequate. We even dare say that this is the only real problem, the only one of substance.

The misgivings of many citizens are fostered by a series of negative mental pictures, conscious or unconscious. Nuclear technology is associated with nuclear weapons. Nuclear radiation is considered as mysterious and insidious. The exposure to these invisible rays can cause cancer, the most feared disease, the bare name of which is frightening like the plague in the Middle Ages or more recently AIDS. Besides, irradiation may not only hurt people directly exposed to it, but give rise to a legacy of birth defects in future generations. Last but not least, some of the nuclear wastes produced to day will remain radioactive for thousands of years, which raises the issue of our responsibility towards our descendants in a very remote future.

Most of those symbols are perceived in a purely emotional way by the public, which does not analyse them in rational terms, so that they are particularly difficult to counter.

Any time an important issue concerning nuclear energy is raised, those latent fears are easily revived by well organized antinuclear movements or by lobbies whose interests are opposed to nuclear energy.

In some countries, the media, always eager for a scoop of thrilling news, may be inclined to dramatize even minor incidents. It could also happen that politicians be tempted to adopt an antinuclear stand in the hope to collect more votes.

The main objective is to recover the trust and confidence of a clear majority of American citizens in nuclear energy and its promoters. It will be a difficult and long lasting undertaking but we do not at all consider it as insuperable, because we strongly believe in common sense. We are sure that people will be prone to quiet their apprehensions about, say, the erection of a new nuclear power plant, once they perceive a personal advantage if it is built, in the first place if it means a financial bonus for them, or if they have a strong feeling that it will contribute to relieve them of impending problems.

On the, so to say, negative side of motivations, occasional interruptions in the import of foreign oil or gas, or more frequent occurences of electricity brownouts in some future will make them more conscious of their personal vulnerability, as far as energy supply is concerned. Likewise, a growing awareness that electricity rates would increase for lack of nuclear power plants should do a great deal to mitigate their concerns about hypothetical accidents or long term reliability of radwastes repositories.

On the positive side, there are -we think- measures, in particular financial incentives, which Federal or State Authorities could take, would they choose to do so, to make nuclar energy attractive again to a growing fraction of the public. In France for instance a large scale industrial facility provides significant advantages to local communities, thanks to a system of taxes directly paid to them. EDF has also done its utmost to use local contractors and workers. It should be noted that a special procedure, known as "grand chantier - major construction site", was established in 1975 to streamline integration of large projects within the local social and economic fabric, in terms of employment, development of infrastructures like roads or railways, housing programs, facilities of various kinds, etc ...

An obvious prerequisite to alleviate the fears of the people is a reliable operation of the current generation of nuclear power plants, without any serious accident. Good progress has been made during the last years concerning the average availability of the nuclear power plants in the U.S., but there is still room for further improvements. The electric utility industry must establish a reputation with the public for safe, efficient and economical operation of those units now operating. The utilities are of course the prime actors in that respect but they are not the only ones. Could it be that the Federal Government focuses greater resources to help the utility industry on attaining an even better record of operation of current nuclear power plants ?

In democratic societies like ours, the public must be continuously informed. No matter what efforts are made to inform people, they invariably say that they are not well informed. Does it mean that information is just wasted time and money ? We do not think so, as experience shows that people in general respond more favorably to nuclear projects if they have been informed, even if at the same time they claim that they have not been. Thus a wide scale ongoing effort is valuable. The information to be provided, no matter what it contents, must be continuously available. People should know where they can get it easily, if and when they want it.

It is out of question that but a tiny proportion of people could and would acquire even a superficial knowledge of what nuclear technology is. They do not ask for overly scientific details. Basically they want to be reassured. What matters is to provide them with true and simple data, in terms they are used to and they can easily understand.

Much value should be given to information which can be transmitted in a direct and visual way. For instance well organized sytematic visits of nuclear stations and installations can include on the whole a large number of people. In France, some four hundred thousand persons on an average visit the EDF nuclear plants every year. Visitors are thus able to see equipment similar to what can be seen in other conventional plants or industrial facilities more familiar to them, and to notice that operators of nuclear power plants do work in a day to day framework which is by no means frightening or unusual, but commonplace.

As it is impossible to reach directly everybody, information has in many cases to be distributed in steps. French rural inhabitants usually place much confidence in the opinions of local persons of influence, like mayors, doctors, teachers, etc ... who can play an important role in relaying the information.

Local Information Committees exist for every nuclear power plant in France. They comprise elected officials and representatives of the media, trade unions and local associations like environment protection groups. Experience has shown that these Committees play a strongly positive role. Their very existence reassures the public by demonstrating that a means is available for supplying regular information on operation of the plant, in particular to organizations which are openly hostile to nuclear power and that an alarm would be sounded in the event serious problems arise. At the same time, providing information openly prevents antinuclear groups from distorting it for their own purposes, out of fear of being exposed.

In April 1988, the French Government issued an Incident and Accident Severity Scale which is in systematic use by EDF and by the Safety Authorities since then. The Committee which drafted this scale included two representatives from the media and one from the antinuclear groups. Any time an incident occurs -even a minor one involving no risks at all, but from which lessons can be drawn to improve the design or the operation of any component from a safety standpoint- it is reported immediately to the media with an indication of the level (1 to 6) at which it has been graded. An essential complement of this severity scale is the video communication system called Magnuc through which millions of French families have a direct and permanent access from their home to a large data bank concerning nuclear safety and radiation protection, which is kept up to date every day.

All these systems proved useful to communicate with the media and the public but more efforts are still required. For instance we were consistently unable so far to make the French media understand that the purpose of the La Hague plant is to reprocess irradiated fuel and not to reprocess wastes.

Public debates do rarely succeed in improving the case for nuclear energy because they are difficult to run in a fair way. The dialogue between supporters and opponents of nuclear energy is not balanced for several reasons. First it is much easier to frighten than to reassure listeners. Second, experts from the nuclear establishment must take extreme care to quote exact figures and data, while nuclear opponents did not always make a point of accuracy ; if it was shown later on that they did say untruths, they could always pretend that the real facts were hidden from them. One should also be careful not to let a public debate be diverted towards false arguments, like discussing if the nuclear risk is null, since it is not and cannot be, or if it is ten to the minus 7 or ten to the minus 9, which is meaningless and completely confusing for the public. As any human activity, nuclear energy involves a certain amount of risk, which should be compared in simple terms with other hazards well known and accepted by everybody.

We already mentioned how sensitive people are about the problem of nuclear wastes. This is a field where information campaigns are particularly needed. Ten years ago the selection of a second site for the storage of low and medium activity radwastes was started in France. One of the planned sites was rejected by the local population in 1981. An alternative one, at Soulaines, was accepted two years ago, although the discussions with the public and the meetings of the enquiry commission took place not long after the Chernobyl accident. The works on site are now progressing smoothly. This is a good example of how information actions, when they are properly conducted, can be effective. The Andra Government Agency , in charge of nuclear waste management in France, spends a great deal of time and does an excellent job in that respect.

It will take presumably several years before public acceptance of nuclear energy has enough recovered in the U.S. to make possible launching a few new nuclear power plants, at least in some locations where the need is particularly acute. Use should be made of this incubation phase to solve the somewhat artificial institutional problems which contributed to block the deployment of nuclear energy during the last fifteen years and to pave the way for a restart on a better foundation than in the past.

At present no utility in the US is willing to order a nuclear power plant because the business is just too hazardous. The risks that events beyond the control of the company will delay by several years the date on which the plant comes on line, or multiply its cost by a large factor, or block its operation, are so great that the financial balance of the utility might be fully jeopardized. In addition to being safe and acceptable to the public, commercial nuclear power must be economic, which is entirely feasible as this has been conspicuously demonstrated elsewhere.

The remedies to the present unsatisfactory situation of nuclear energy in the United States have been identified many times and they are not so many. The brief remarks which follow are not ours, as it would be fully inappropriate for us to pretend to gives advices concerning the U.S. scene. They just express the common views of most our American friends and colleagues.

The implementation of solutions depends on the real willingness, the courage and the cooperation of the major actors.

A prerequisite is of course a strong resolve from both the Government and the Congress. They both share the responsibility towards the nation to care about long term goals, like the security of energy supply for the country and the protection of the environment. If they are really aware of the crucial importance of these issues, and of the contribution which nuclear energy can offer to solve them, it is their duty to take the required measures.

The major part assigned to the Government does not arise only from its investment in underlying research, development and demonstration, but also from its regulatory role. A pressing objective is to create a stable regulatory climate by providing orderly and timely licensing actions which are essentially final once made. Finding clear solutions to planning for emergencies and to nuclear wastes management are equally important and urgent tasks.

Another essential issues is how the electricity rates are regulated by the public Utility Commissions of the various States. It seems that significant modifications should be introduced in the rules of the game during prudency reviews towards a fairer balance between rewards and risks for utilities.

Changes seem also to be desirable towards a greater concentration on the industry side. Would a larger pooling of resources by utilities be possible through the formation of joint ventures, consortia, etc ... ? We hear much about generating companies which would be deregulated, or regulated under federal laws, about IPP's, QF's and other kinds of entities. We would not be surprised if new schemes for producing and selling electricity would emerge in the next years to come.

One important point is that the actual supplier of the reactor concept, including the systems design, the hardware, the licensing support, fuel and services, be able and ready to make commitments for continued service over the life of the plant. Will turnkey contracts become again common practice ?

Last but not least, there is an obvious incentive towards the systematic use of standardized reactor designs.

Though the institutional issues we have just mentioned seem to us of prime importance, it does not mean that no technological progress must be pursued in parallel. But our point is that it would be foolish to cope with institutional facts or artefacts by trying to respond with technological answers.

Much work is carried on at present in the United States on various new reactor designs. The intense brain storming which is in progress is a clear testimony of the vitality of nuclear engineering in this country. All current designs aim at enhancing safety, reliability and economics. We will not review them now, as they will be discussed during the next days at this Workshop, but we will only make a few comments.

There are, roughly speaking, two different approaches, the one we will call evolutionary and the other revolutionary. In that case, we stand firmly on the evolutionary side. We consider that the safety of nuclear power plants like the PWR's presently operating in France is perfectly adequate. It does not mean that no progress can be made.

On the contrary, improving the safety is a permanent process, which will continue for ever, as it is the case with the safety of cars, railways or planes. We feel that the best way to improve further the reliability and safety of nuclear power plants is to start from what exists now and to build up on the operational experience which is accumulating day after day.

We have good American friends who do not share the same opinion and who favor the revolutionnary approach. Some are saying : "Nuclear energy in the US is dead. The only way to revive it is to offer people brand new systems which can be presented as basically safer than the old ones". In our opinion such an attitude is at least very ambiguous. Either it is thought that present day reactors (like say French PWR's) are not safe enough, and we disagree. Or it is thought that they are in fact safe, but that, in order to regain public acceptance, there is no other way than to admit that they are not and that they must be replaced by safer systems, and we disapprove this approach.

It does not mean that we see no value in studying a variety of new designs. Generally speaking, progress comes from diversity and competition, but one must be very cautious on how to proceed.

We are extremely skeptical in the ability of a magic potion to ressuscitate a dead, but we see a great risk that it would kill healthy people.

For similar reasons, we are extremely opposed to the slogan of "inherently safe reactors" which carries the idea that there would be reactors presenting no risk at all, which is just not true.

There is a current trend in the United States towards smaller unit sizes, say 600 MWe. We understand at least some of the reasons for a renewed interest in such intermediate power levels, in the American context. But we think that the size of a particular plant depends on many considerations related to the site, the size of the grid, the growth rate of consumption, the financing, the time at which the decision has to be made, etc ... we are convinced that there still is (or that there will again be) a market for large nuclear power plants, of 1000 or 1500 MWe. Anyhow we do not see at present anything like an optimum size for which the safety of the plant would be maximum.

All these questions will be discussed in detail during the next days. Let us express our strong belief that the public will progressively become aware that nuclear energy, when compared to other ways to produce electricity, is environmentally benign and that it will be more and more ready to accept it.

SAFETY APPROACH EVALUATION FOR FUTURE LIGHT WATER POWER PLANTS

L. NOVIELLO
Ente Nazionale per l'Energia Elettrica (DSR),
Italy

In my country in the last two years, first owing to the referendum and then to the effort of converting into technical directives the new policy adopted by the Government, a wide debate developed on the design basis for the new nuclear power plants.

In this context we are co-operating with many international organizations such as IAEA, OECD, EEC; and ENEL, as a utility, has become an active member of EPRI's program for the requirements of the future light water power plants.

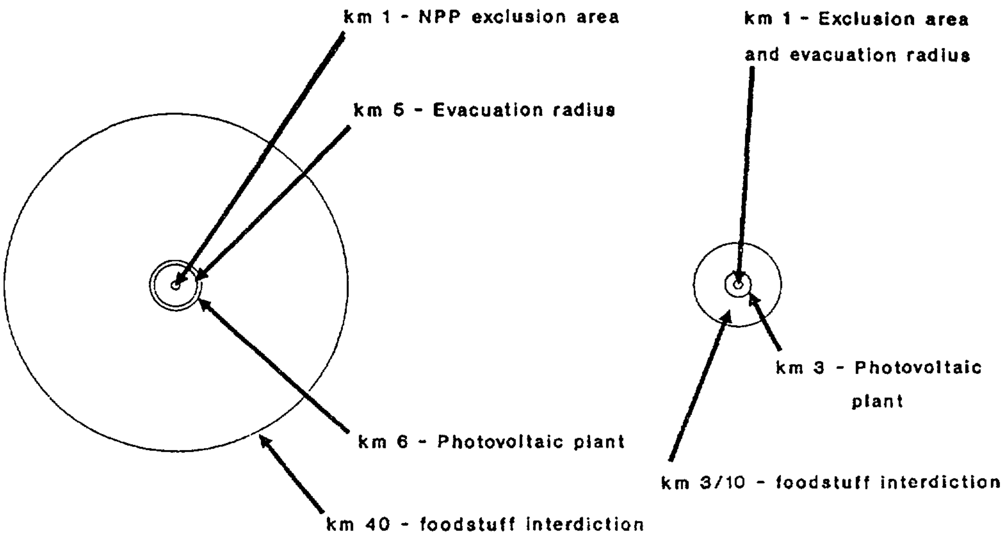
In my opinion the design basis of the new nuclear power plants have to be founded on the three following fundamental guide-lines:

1) a stressed engineering approach;
2) a wider account of the general trends of the society;
3) wherever applicable adoption of the same safety criteria in the various countries.

A stressed engineering approach means a stronger overall return to the traditional use of one of the most important technical basis of the engineering: the experience. The traditional use of the experience entails an effort to eliminate any problem shown by a machine from the standpoint of quality, safety and acceptance. If there is a limit to the modifications introduced, generally it is due only to the technical and economical inconvenience to do more. A stronger engineering approach also means to accept as a natural event the continuous evolution in the field of quality and therefore also of safety without taking for granted the fact that the more advanced characteristics of the new products automatically are detrimental to the older products. The industrial societies offer numberless examples of the use of equipment having different characteristics.

What I have told may seem obvious, but it is not so.

As matter of fact after TMI and even more after Chernobyl as an international community we are not yet adequately searching into the possibility of deterministically introducing the core melt (which has happened) in the design basis of the mitigation



Current situation in Europe Design objective

SEVERE ACCIDENT ENVIRONMENTAL IMPACT

systems of the new plant designs. After having experienced a serious problem of environmental pollution (Chernobyl) and the refusal of the population to emergency plannings which involve a remarkable number of persons and a significant portion of the territory (Italy, Shoreham) a co-ordinated international effort is still lacking in order to define a new philosophy of environmental impact. Even worse, there is a trend to different approaches on the both sides of the Atlantic Ocean as regards the backfittings on the power plants in operation.

This inertia and this tendency to diversification are extremely harmful in an international society which is more and more interconnected and which shows a greater and greater sensitivity about environmental problems. I do not think to be far from the truth when I say that the Western world trends to zero-release factories because of the lower and lower acceptance of the environmental pollution. For instance, in this framework mention is to be made of the latest initiatives taken in Paris by the Western leaders, of the cuts in toxics release decided by some chemical industries (even prior to any legal action), of the reduction of NO_x and SO_2 in coal-fuelled power plants and of the development of new combustion methods. In this scenario also the nuclear industry must show dynamic and responsive to the societal trends.

Nuclear power plants have already high environmental standards as regards the day-by-day operation, but this quality can not be appreciated by the public in the light of the present regulations on accidents. Since today the public and its representatives play a significant role in the decisions on the use of nuclear power, we have to accept the fact that the need of planning an evacuation and, even worse, of testing it is felt much more strongly than the low probability of its occurrence. The planning and the drilling of an evacuation are a physical reality, may be personally experienced; the probabilities are only numbers. As a result, I deem that it is necessary to introduce new designs technologically feasible to meet all the credible accidental scenarios thus reducing the objective need of an emergency planning and of a radiological control of the territory in the long term. Of course, any technological improvement is meaningful only if there is the availability to revise the present regulations and especially the many conservative assumptions that were set when we knew less. On the other hand, the probablistic instrument must come back to be only a design tool to select the accidental scenarios to be included in the design basis. Its use for sophisticated estimates of potential health hazards should be limited as much as possible at the least, again, simply because that lay-men and decision-makers do not understand it.

To complete this concept, let me hint at the homogeneity of the regulations. If in the plant design criteria, because of different siting conditions some differences exist (for instance aircraft impact), no macroscopic differences can be assumed among the various countries as concerns the modes development of particular phisical processes under the same phisical conditions. On the other hand, in the fields where experimental tests and the accidents have provided new data, neither is possible to defend only as "legalistic problems" regulations issued 20 or 30 years ago: in any technical matter rules "curved in the stone" can exist.

At least as regards Europe the integration process in view of the year 1993 is very likely to accelerate a common rethinking process.

To give this meeting a practical contribution let me show you a slide. Based on my understanding of the technologies available today, the upper part of the slide identifies, as a reference, what can be reasonably obtained with the backfitting of the existing plants. The lower part indicates the minimum overall design targets that should be met by the new projects. As you can see, I am not necessarily proposing a zero-release plant for severe accidental conditions. In my opinion a nuclear station with a limited impact area of the same dimension as that of an equivalent photovoltaic solar plant can be accepted by the general public and can be designed with the available technologies.

SOME COMMENTS ON FUTURE NEEDS FOR NUCLEAR POWER

G. YAGAWA
University of Tokyo,
Tokyo, Japan

Global environment and world economy related with nuclear energy

The use of nuclear energy is essential if we are to preserve our global environment, as the International Energy Agency Paris meeting and the Summit Paris meeting adopted a communique endorsing the promotion of nuclear energy as an alternative to energies that may lead to global warming. The burning of oil, coal, natural gas and firewood emits carbon dioxide,which in excessive amounts can lead to major climatic changes, including heavy rains and drought. With the last year's heavy drought in the United States, world grain stocks have dipped to an alarming level. If another drought of that magnitude occurred this year, it could send the world's grain markets into a tailspin. And a shortage of rainfall in Africa would make international disputes over water even harsher.

In United States, the advance of nuclear power appears to be in the doldrums because of strong public objections. This has led to an increase in crude oil imports, and a gradual rise in oil prices. Moreover, increasing oil imports hinders the United States from reducing its trade deficit. Thus the nuclear energy issue is connected not only with pollution of the Earth's atmosphere with carbon dioxide, but also with financial issues.

Have vs have-not nations

The concerns about global climate changes are understandable, but only to a limited extent. The industrialized nations have benefited in the past at cost of the environment.The have-not nations, however, tend to see the concerns as selfish and self-righteous. Developing nations feel they are paying the price for damage already done by industrial nations to the environment. If strict regulations to protect the environment go into effect, the advanced country will be able to comply much more easily than the developing nations.

Coal is the most important source of fuel in China, but China's technology to prevent air pollution is far beyond that of the advanced nations. Many of China's coal burning factories were made before World War II, and the air in major industrial cities such as Shanghai is heavily polluted. Pollution prevention controls must be installed in these plants, but the capital investment needed to do so will be enormous for this country.

Means other than nuclear energy

Energy conservation has its limits. Currently no energy source other than nuclear energy appears appropriate to replace petronium and coal. Since the first oil crisis, strenuous efforts have been made to search for substitute of energy sources, without producing any feasible solution. Solar energy is still 30 to 40 times expensive compared with nuclear energy.

Nuclear energy for developing countries

Nuclear energy will be necessary in developing countries as well in the beginning of 21st century. Indonesian Mines and Energy Minister announced recently that a lack of primary energy resources will make the use of nuclear power unavoidable by the year 2010 in his country. Indonesian Research and Technology Minister Habibie said in another occasion that in 2015, primary energy sources alone will not suffice to meet the some 27,000 megawatts of additional electricity needed just for the densely populated island of Java. This situation is more or less the same in other developing countries.

Recent trends of public opinion for nuclear energy

A U. S. opinion survey last November showed that 79 percent of Americans considered nuclear power necessary to meet the nations electricity needs and that 78 percent thought new nuclear power stations should be built. Similar survey was performed in Japan last October which showed that 60 percent thought that new nuclear power stations should be built.

These surveys imply that majority of people gradually tends to think nuclear energy to be important as a future energy source.

Conclusions

(1) Nuclear energy is unavoidable from the viewpoint of global environment, world economy and energy security in industrialized as well as developing nations.

(2) Assuring safe operation of nuclear plant is the only way to ensure public support for nuclear energy. Especially the aging problems will be the main issue for the older plants. More efforts should be made to minimize troubles relating to aging of plants .

(3) It is urgent to develop more safe plants with passive safety, especially for developing countries.

FUTURE NEEDS FOR NUCLEAR POWER

A.T. CALLEJA
Iberduero, SA,
Bilbao, Spain

1. DEMAND

Looking at the current forecastings of future energetic and electrical demands in different countries leads to conclusions on rather commonly agreed prospects concerning certain trends which shape the present-time energetic policies.

First, the expected continuous growth of energetic needs in practically all the countries in the world, in percentages fluctuating between 1% per year (USA, years 2000 to 2015) and 4% per year (countries with high growth potentials from current medium and low levels of development and consumption).

Secondly, the expected continuous growth of electric energy needs in practically all the countries in the world, in percentages fluctuating between 1.5% per year (USA, years 2000 to 2015) and 5.5% per year (countries like the ones mentioned above).

It is important to realize that electric energy needs grow proportionally faster than total energy needs, this phenomenon being the more outstanding as the growth of educational level foreseen for the labor population is faster, as a consequence or need of its economic development. In other words, the ratio between electric energy and total energy is growing, and its growth is larger in developed countries.

2. REPLACEMENT OF GENERATING EQUIPMENT

Within a different field, the composition of current electrical generating systems shifts towards age distributions where the amount of stations with an active life over 25 years starts being worthy of consideration.

Some nuclear power stations have already surpassed such a life, and many conventional thermic stations also have it. The accumulated power of those which still surpass twenty five years old in the nineties is very important.

The expected activity to be originated by the replacement of obsolete generating units will be really important in times already close to us.

3. ALTERNATIVES

The role played in these last fifteen years by energetic savings oriented policies and technologies has amounted to the most spectacular source of energy, and it is mandatory not to slack in this effort, where the achievement prospects are still important.

Renewable energies should also be developed as much as possible, and be used profitably; hydroelectric energy is still a non-exhausted source, with interesting prospects.

Anyway, the base electric energy needs to an important extent and forever the basic alternatives of fossil fuels and nuclear power. These alternatives will keep being such for many more years ahead.

4. THERE IS NO MAGIC SOLUTION

The knowledge of greatness and servitudes, of advantages and drawbacks of every alternative if now fuller, deeper and more developed than ever.

The greenhouse effect, the acid rain, the ozone layer damage, the obligations in radioactive waste managing, the flooding of large areas, the modification of natural hydraulic systems, and a long, hypothetical, etc. are just effective and experience based verifications that each option implies important servitudes, whose consequences should be palliated as far as possible, and that there is no magic, brilliant, harmless, inoffensive and cheap solution.

There is a well-known, manageable reality. There is a reality needing be to rationalized, now more than ever.

5. A WORLD OF FEELINGS. A WORLD OF REALITIES

Discussion on energetic subjects has been emphasized starting from the conviction about its strategic importance, and the growth of the presence and acting levels of all kind of institutions more or less involved.

Somehow, the rationalization of this subject has been hindered by the complexity of dealing, within a feeling field as the political and social world of groups and institutions, with such a complex and important topic as the one we are considering; the dialogue on energetic subjects has proven difficult on sincere basis, and still more difficult, of course, on the grounds of many clashes of interests based on different intentions and various justifications.

The knowledge of benefits and drawbacks of each option, as mentioned before, leads to the mentalization of different agents about the necessity of building a world based in realities, which implies a call for professionalism and a will of rationalizing decisions.

The feeling of risk does not lead rationally to decisions. It is the reality of risk which must lead us to them.

6. QUOTAS

This world of realities must lead us to the rationality and, all things considered, to choosing the different participation quotas of every existing alternative, determined according to the part played and implied by each of them in every specific country.

Nuclear power, as a possible alternative and as a result of rationality coming from a deeper knowledge of benefits and drawbacks of each option, will have a participation share in each country because as lacking of a magic solution, the rational solution must be opted for.

The nuclear share of participation is suggested bigger than the present one in many cases, due to different reasons that are rising very strongly lately.

7. THE NUCLEAR POWER QUOTA

The nuclear power quota will depend in each case and country and as a whole, on the treatment given to specific differential subjects as regards other alternatives which have meant the root of differences in the social positioning and treatment of this kind of energy, till now.

I shall limit myself to mentioning these differential subjects:

a) It is a newer and more complex energy than others. These circumstances have determined general mistrust above its controlability as a result of a supposed and not existing inadequate technological development.

b) The knowledge of its characteristics by the public and the involved agents is difficult to acquire, and therefore it is frequently inadequate.

c) The participation and activity of social agents and groups have made the rationalization possibilities of decisitions to depend upon the Governments and Administrations strength.

d) The economic and financial problems appeared in stations under construction as a result of the protracted construction periods have shifted the options as regards to the opinion of managers who are not deeply involved in this topic.

8. NEEDS OF THE NUCLEAR ALTERNATIVE

If we centre on the nuclear option and try to identify actions and needs required by this option in order to hold the place it deserves in each rational decision, three fields of treatment should be differenciated:

a) Safety.
b) Public opinion.
c) Economy.

As far as the first item, that is Safety, is concerned, I consider that the following sessions will be centered on it, therefore I am not going to spend time in this respect. I will limit myself to emphasizing significant needs in the other two fields.

b) Public Opinion.

Reinforce the actions in order to increase the credibility of the institutions which issue messages and informations on this subject.

Explaining simply the benefits of nuclear power as regards protection and respect of the environment. The rationalization and clearing of this side is vital.

Persuading that the waste disposal topic is sufficiently solved, and will not jeopardize future generations. The criterion on protection policy is changing. It seems more adequate to concentrate and control other than to dilute.

Stimulate considerations about an oil or gas lacking future, these raw materials being necessary for many industries.

Emphasizing the advantages of a rational balance in the use of different sources of energy, as regards supply reliability and the treatment of world reserves.

Explaining the benefits of using nuclear power as regards energetic independence, and the price stability of electric power.

Optimizing the **mechanisms** of national and international cooperation, in order to reduce the number of incidents due to the use and benefit of different operational experiences.

c) Economy.

Shortening of the construction terms, by simplifying designs and modularization.

Standardization, in order to cut the equipment prices and make interchanges between stations easier.

Enlargement and prolongation of the stations useful life.

Simplification and shortening of the authorization processes.

WHO NEEDS NUCLEAR POWER?

P.M.S. JONES
United Kingdom Atomic Energy Authority,
London, United Kingdom

1. INTRODUCTION

In a session on the future *need* for energy it is as well to start by defining terms. Is need synonymous with potential use in the absence of constraints or is it income constrained demand? Does it imply a distinction between what might be desired and what might be considered essential?

Whichever concept is adopted it is readily apparent that needs will differ between geographical regions; between cultures and over time. That which is desired, which would be purchased or which is considered essential in terms of energy use is very different in the Europe of 1989 from what it was in 1939 and from what it is today in the poorer developing nations.

2. CHANGING PERCEPTIONS

Most energy demand studies (1) of the 1960s and earlier were concerned with the questions of provision of energy supplies that matched demands that were implicitly income constrained, although some economists subscribed to the view that a driving force behind economic growth was access to abundant cheap energy (2). In their view the unprecedentedly rapid growth of the 1950s and 1960s was due to the exploitation of cheap oil. The majority of 'establishment' energy analysts still adhere to income constrained demand projections but make allowance for technological development and public attitudes to the extent that these affect demand (3).

Rachel Carson's 'Silent Spring' (4) heralded the emergence of the environmental movement, initially confined to the USA, which attracted adherents who were concerned that insufficient attention was being given to the side effects of technological developments. Amongst these were some whose concerns focused on energy and resource use, reflecting in a modern form the worries of Malthus (5). Computer based world models predicting the demise of industrial society (6) were strongly contested (7) but the concept of sustainability emerged. This called for moves to end dependence on finite resources and to switch to renewables, recycling and conservation.

The oil crises following the Yom Kippur war (1973-74) and the outbreak of Iran-Iraq hostilities (1979-80) led to further pressures to save energy, almost regardless of cost, because it was 'a scarce and valuable commodity'. Advocates of conservation, combined heat and power and renewable energy sources exploited public concern despite the fact that there was no inherent or impending *energy* shortage but merely a temporary disruption of one important fuel which was difficult to replace in the short term. One obvious available complement to energy supplies was nuclear power, but those committed to energy saving and renewables were for the most part opposed to nuclear power, and many also regarded electricity as a wasteful form of energy to be used only where it was essential.

Resource development, fuel gluts and declining market prices have effectively destroyed the myth of short term scarcity, and time is available to reduce dependence on those resources (oil and gas) depleting most rapidly and to avoid longer term problems. However, the re-emergence of environmental concerns about fossil fuel use and coal in particular have brought the old arguments back into the limelight (25); their advocates still opposed to nuclear power and wider electricity use.

3. ARGUMENTS AGAINST NUCLEAR POWER

To support their position a number of studies have been published pointing to technical opportunities for improved energy efficiency and claiming that these offer highly cost effective means of reducing fossil fuel consumption (8). At the same time nuclear power has been attacked on grounds of relative cost, absolute investment costs and its infrastructural requirements (9). Energy demand scenarios have been put forward based on the assumption that the industrial nations adopt the most efficient technologies whilst developing countries remodel their energy infrastructure and meet their basic needs. By these means a 'sustainable' world order is established (10).

Most efficiency orientated scenarios adopt a bottom-up approach. This provides a normative or goal-orientated scenario, illustrating how an objective favoured by its authors can be achieved with, in their view, benefits to all (10, 11). There are good grounds for believing that bottom-up approaches will systematically understate demand (12).

4. WHY EFFICIENCY IS NOT ENOUGH

Sustainable living standards are critically dependent on the level of technological and social advance. Mankind's development from hunter gatherers, through farmers and herders to modern industrial society has been marked by the introduction of new materials and techniques and by the progressive substitution of more efficient means of production for man's own very limited capacities. This trend, which has relied heavily on progressive development and exploitation of energy sources (animal, biomass, renewables then fossil), has created the surpluses that have enabled the growth of civilisation through the release of human and other resources which could be devoted to infrastructure, education, the arts and social welfare (13). Nevertheless communities in many parts of the world still exist on a day to day subsistence basis without access to the capital that could provide security and the means of improving their lot.

One study (10) argues that the existing energy inefficiencies in the developing countries are such that their elimination through use of appropriate technology could provide adequate supplies to meet all basic needs and allow an improvement in living standards for their growing populations to equal those at present enjoyed in the less affluent industrial nations. Their advocated means of achieving this would be primarily through cultivation and better use of biomass. The enormous educational barriers and the dichotomy between the basic needs of the mass poor and the requirements of the small wealth-owning class would call for radical measures, and the authors (10) are strongly opposed to the view that wealth should 'trickle down' from the affluent to the rural or urban poor; although this was the process which, over time, created the social structure and wealth distribution in most of the industrial nations.

One of the most important objections to the laudable but over-optimistic low energy growth scenarios is their failure to recognise the fact that energy is used widely to increase convenience and consumer satisfaction. To those that can afford it, its efficient use is a secondary consideration. In Britain, for example, people heat their homes in preference to wearing more clothing; the majority prefer to have larger cars with good acceleration even if this uses more fuel; lighting in homes and offices is not kept to a minimum standard. Human nature and nations being what they are, as wealth increases growing affluence results in the less well off seeking to adopt practices and lifestyles they could not previously afford. The spread of ownership of houses, cars and consumer durables, and the growth in air travel and overseas holidays over the past 30 years bear witness to the importance and scale of the phenomenon.

The counter to this is to point to saturation effects. People cannot drive two cars at once or watch two television sets. Nevertheless the extent of multiple ownership of vehicles, radios, TVs, computers, etc by households is considerable and growing. Even in the wealthiest nations many have living standards well below those to which they aspire and lack the domestic aids considered essential to modern living. Second holiday homes which have to be maintained, furnished and in some cases heated, are still only owned by a minority. There is no sign yet that the populations of the industrial nations are satisfied that they have the standard of life they want (13).

Of course, technological change will continue to have an impact and the steady improvements witnessed over the past 80 years in the energy efficiency of plant, equipment and buildings for domestic, commercial and industrial use will not cease. However it is not in general energy-effective to retire equipment prematurely (14) and the pace of technical change is for the most part limited to the natural cycle of obsolescence and replacement.

New technology may enable substitution of less intensive in place of more energy intensive practices. For example, information technology may liberate some from the necessity to travel to their work, but it is not clear that such practices will in fact reduce energy consumption. The extra heating, lighting and equipment of home offices may significantly exceed in energy costs the provision of specialised central facilities.

Other technological changes may increase the variety of uses to which we apply energy. As already stated, much of our improvement in living standards derives directly from the substitution of energy for physical labour. In richer countries the housemaid has been replaced by the washing machine, vacuum cleaner and dishwasher and, in her new guise, is now in the service of most families. Power equipment replaces the gardener; the car replaces the horse and donkey. Automatic doors, elevators, escalators and moving pavements serve in some limited locations to remove almost all need for physical exertion. Labour-free electricity, oil or gas-fired central heating has displaced the labour intensive use of solid fuels in a majority of homes in Britain. Similar changes have occurred in industry, agriculture and commerce.

Again saturation arguments can be deployed but these are blinkered by the present. There is still great scope for automation in the home, office and factory. Control of the micro-climate within buildings in terms of temperature, air quality and humidity is still very imperfect. As mineral resources are depleted more energy intensive extraction and refining processes will be needed. Man's energies will increasingly in the future be devoted to conquering space and the continental shelf or exploiting the less hospitable parts of the land mass; none of which can be accomplished without a plentiful supply of energy.

In addition the whole urban and transport infrastructure built up during and after the industrial revolution will need to be replaced in many nations. It is highly likely that the balance of labour, materials and energy costs will favour more energy intensive solutions than those adopted by our forebears. Smaller bore pumped sewage schemes will replace gravity based systems; steel and concrete for roads and bridges are already replacing bitumen and stone. Road safety is enhanced by use of steel crash barriers and extensive lighting. Further improvements could entail greater automatic monitoring and warning, still more lighting and even fog dispersal and road heating.

5. FUTURE DEMAND GROWTH

Both in terms of capital stock and operational energy requirements there is considerable scope for growth in energy demand in affluent industrial societies. The potential in the developing world is even greater, though the pace at which changes can occur is a matter of conjecture. Certainly it seems highly unlikely that world energy demand could be constrained to Goldemberg's (10) 10TW in 2020, and figures of 15TW seem a likely minimum with demands above 20TW not improbable. Within this most observers including Goldemberg et al agree that electricity demand will continue to grow, and a doubling to 20,000TWh/yr seems likely (10, 14, 21).

This leads me to conclude that if we have plentiful supplies of cheap, environmentally benign energy available they should and will be used. There is no doubt about ultimate availability. The world's known low cost uranium resources are sufficient to meet all the world's current energy demands for 1,000 years if used in fast reactors, and this will be extended many fold as additional resources are found and other non-conventional sources exploited (15). Nuclear power could not meet all technical needs directly but the wider penetration of electricity, the direct use of nuclear heat and the exploitation of electrolytically produced hydrogen as a transportable fuel could do most things and greatly reduce demands on fossil resources in the long term.

Nuclear power is also an inexpensive source of electricity that promises to hold its price stable into the future. Recent studies confirm its economic advantage over coal and gas in most OECD countries (16) and there are clear prospects for further improvements in overall performance which should reduce costs further (17). Studies on fast reactor economics show that this plant should operate at costs closely similar to today's thermal plants when they are deployed on a commercial scale (18).

Environmentally there is no doubt about nuclear power's advantage. It produces no acid gases and no carbon dioxide except for the small amounts associated with material and fuel manufacture and transport. Its radioactive wastes can be contained and isolated permanently from the biosphere (19). Overall nuclear energy, used under proper safeguards and with due attention to safety, offers the world a vast, economically attractive resource of environmentally benign power. Even the limited detrimental effects associated with uranium mining can be reduced 60-fold in the longer term through the use of fast reactors.

On this basis one might hope to see nuclear power being deployed as rapidly as possible to replace the older polluting technologies. However, premature retirement of the existing plant stock is expensive, and the rate of change justified by our present state of knowledge about carbon dioxide effects on climate is far from clear (20).

On a present trends continued basis and OECD Nuclear Energy Agency projections, nuclear power could not expect to do much better than reduce anthropogenic greenhouse emissions by some 6-7% in 2020 (20). This is far from trivial but is certainly insufficient to stop the growth of CO_2 in the atmosphere. A vigorous programme might achieve more, perhaps as much as 15% reduction (14) by 2020, and if efforts were made to penetrate heat and transport markets a lot more could be done over the next 50 years.

Opponents claim that the pace of nuclear construction required would be excessive '... one new plant every 3 days', and prohibitively costly (8, 9). However, the 20 years old nuclear industry had a construction capability of 60GWe pa in the 1970s and was constructing at a rate of 35GWe pa (22); figures not ridiculously short of the high nuclear share scenarios. Equally, nuclear plants do not differ greatly in total generation cost from fossil plants and have lower capital and overall costs than many renewables (16, 23). The objections on grounds of cost, if valid at all, would be just as true of replacement fossil stations or the use of renewables. In fact, as indicated above, the necessary rate of fixed capital formation, which is not excessive in relation to domestic product (24), has been achieved in the past.

It would seem therefore that in a rational world new nuclear capacity would be targeted for construction post-2000 at a rate of some 40GWe pa, mainly in the industrial nations, to make installed capacity some 1,600GWe by 2020. This would not be sufficient of itself to prevent continuing increases in greenhouse gases (20, 26), and *economic* energy efficiency measures plus shifts in fuel use away from coal to hydrocarbons would be essential complements if global warming had to be constrained close to present levels.

No single approach could succeed on its own, and the adverse price effects and relatively short term availability of hydrocarbon substitutes for coal makes nuclear power's contribution one of the utmost importance, although necessarily secondary to efficiency measures in its potential near term impacts.

References

1. See for example JEVONS, W. S., (1863), The coal question, Environment and Change (1973) 373; Report of the Committee on National Policy for the Use of Fuel and Power Resources, Cmnd 8647, HMSO, London (1952).
2. SCHURR, S. H., "Energy, economic growth and human welfare", The Economics of Nuclear Energy, (BROOKES, L. G. and MOTAMEN, H., Eds), Chapman and Hall, (1984) 362-370.
3. See for example HÄFELE, W., McDONALD, A., ANDERER, J. and NAKICENOVIC, N., Energy in a Finite World, Ballinger, Cambridge, Mass (1981); Electricity in IEA Countries, IEA/OECD, Paris (1985).
4. CARSON, R., Silent Spring.
5. MALTHUS, T. R., An Essay on the Principle of Population, Johnson, London (1798).
6. MEADOWS, D. W., MEADOWS, D. L., RANDERS, J., BEHRENS, W. W., The Limits to Growth, Earth Island Ltd, London (1972); CLARK, J. and COLE, S., Global Simulation Modelling, Wiley Interscience, Chichester (1975).
7. KAHN, H., BROWN, W., MARTEL, L., The Next 200 Years, Morrow, New York (1976).
8. See for example Memorandum to the House of Commons Energy Committee Inquiry on Energy Policy Implications of the Greenhouse Effect, HMSO (1989), 192-i, 43-53.
9. KEEPIN, B. and KATS, G., Greenhouse warming, Energy Policy (1989), 538-561.
10. GOLDEMBERG, J., JOHANSSON, T. B., REDDY, A. K. N., WILLIAMS, R. H., Energy for a Sustainable World, John Wiley and Sons, Chichester (1988).
11. See for example LOVINS, A. B., World Energy Strategies, Ballinger, London (1975); LEACH, G., A Low Energy Strategy for the United Kingdom, International Institute for Energy Development, London (1979).
12. JONES, P. M. S., Nuclear Power: Policy and Prospects, Wiley Interscience, Chichester (1987), 320, 321.

13. *Idem, ibid*, 339-402; also reference 2.

14. *Idem*, Minutes of Evidence to House of Commons Energy Committee Inquiry into Energy Policy Implications of the Greenhouse Effect, 192vi, HMSO, London (1989), 85, 86, 87 and 99-101; *Idem*, Internalising Externalities, Surrey University Energy Centre Discussion Paper (1989).

15. *Idem*, ref 12, 327-341.

16. The Projected Costs of Electricity Generation, Nuclear Energy Agency/OECD, Paris (1989).

17. Good Performance in Nuclear Projects, Nuclear Energy Agency/OECD, Paris (1989).

18. HALL, R. S. et al, Towards an economic fast reactor, Nuclear Engineering International, 34 (1989), 17-21.

19. Spent Fuel Management, NEA/OECD, Paris (1986); Decommissioning of Nuclear Facilities, NEA/OECD, Paris (1986).

20. Memorandum 15 in reference 8.

21. Report of the Working Group on Long Term Forecasts, NEA/OECD, Paris (1989).

22. WALKER, W. and LONNROTH, M., Nuclear Power Struggles, Allen and Unwin, London (1983), 47.

23. Background papers relevant to the 1986 Appraisal of UK Energy R, D and D, ETSU-R43, HMSO, 1987.

24. For the UK see ref. 12, 233.

25. GRIBBEN, J., CO_2 and climate, Energy Policy, 6 (1978), 312-320.

26. GILLAND, B., Population, economic growth and energy demand 1985-2020, Population and Development Review, 14 (1988), 233-244.

FUTURE NEEDS FOR NUCLEAR POWER

C. STARR
Electric Power Research Institute,
Palo Alto, California,
United States of America

GLOBAL ENERGY DEMAND

The global energy demand to the year 2060 was estimated in my study, "Global Projections of Energy and Electricity," presented to the American Power Conference in Chicago on April 24, 1989 and recently expanded.

This study emphasizes that the two major driving forces are global population growth and economic growth (GNP/capita), as would be expected. The modest annual increases assumed in this study[1] result in a year 2060 annual energy use of more than 4 times the total global current use (year 1986) if present trends continue, and more than 2 times with extreme efficiency improvements in energy use[2] (i.e., full conservation). Even assuming a zero per capita growth for energy and economics, the population increase by the year 2060 results in a 1.5 times increase in total annual energy use.

---

[1]Population growth averaging less than 1% per year, and economic growth averaging about 2.3% in world product.

[2]Full conservation assumes direct energy use reduced to one-half of present trend, and electricity use reduced to two-thirds of present trend values.

Recognizing the uncertainties in demographic and economic projections, this study suggests that a long-term reduction in the present level of global energy use is realistically unlikely. The implications for global planning are clear, but the detailed strategies require careful consideration. Obviously, efficient energy use is a desirable objective for many reasons. A shift to nonfossil sources (hydro, solar, nuclear, geothermal) is inevitable, in my opinion, but raises many social trade-offs. Less clear is the value of depleting our high-hydrogen fossil resource (natural gas) to slightly reduce CO_2 emissions for a few decades. All this must be perceived in the context of the increasing role of other greenhouse gases which are population dependent--methane principally.

The principal implication of this projection is that only a massive expansion of nonfossil sources could prevent a continuing increase in annual CO_2 emissions globally. In 1986, global energy use was 321 quads, of which the electricity input was 105 quads (32.7%). Assuming an optimistic full conservation projection, by year 2060, the total energy will be 810 quads of which 423 quads go into electricity (52%)[3]. Thus, direct fossil source use (nonelectric) will increase from 216 quads in 1986 to 387 quads in 2060, roughly 1.8 times as much. Such an increase implies a steady growth in annual use of coal, oil, and gas, with a mix determined by resource economics and scarcity.

ELECTRICITY DEMAND AND NUCLEAR POWER

The electric component is estimated to increase by 4.7 times during this 1986-2060 period, with a full conservation effort. In 1986, nuclear electricity represented about 16% of total generation. As an upper bounding case, assume that the present fossil fuel and hydro remain fixed for environmental reasons, and assume an optimistic year 2060 contribution from solar electricity, then nuclear power would need to expand to fill the gap. This scenario is quantified in Table V and Figure 11 of the referenced study as an upper nuclear case.

The year 2060 potential contribution from future solar electric plants is an estimate based on a fully matured solar photoelectric capability, without energy storage. This assumes that solar sources can supply the daytime peak power demand of a typical diurnal load. For this bounding case assume that, as a maximum, solar represents 50% of the total global generating capacity (about three times the most that present networks can accept), and that this has a global average capacity factor of 30% as determined by the daily sunlight cycle. The resulting 15% of total kWhr output (50% x 30%) is a very optimistic estimate of solar's future role. Nevertheless, it may be a good surrogate for a mix of small-scale alternative nonfossil sources such as geothermal, wind, and waves. Table V shows the calculation for this bounding case.

The calculated nuclear capacity expansion of 20 times in 74 years represents a growth rate of about 4.1% per year, or an average addition of 77 GWe per year. Although this is much greater than present manufacturing capabilities, it could be achieved by the industrial countries if the market developed.

---

[3]Energy equivalent: 30 quads = 1 Terawatt year (TWyr).

Figure 11
ELECTRICITY AND TOTAL ENERGY INPUT

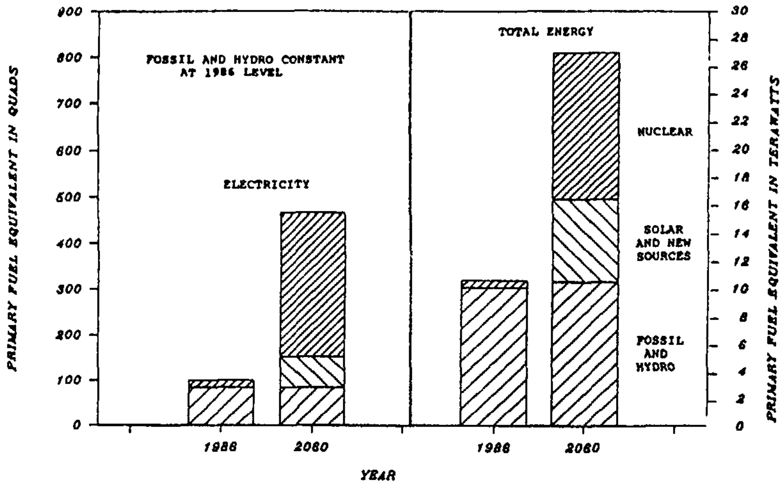


Figure 13
CONSERVATION CASE - ENERGY TYPE DETAIL
1980 - 2060

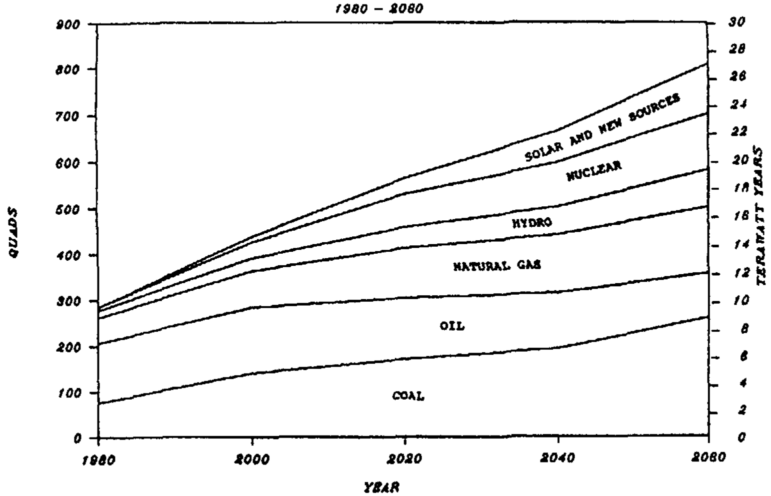


Figure 12
ELECTRICITY AND TOTAL ENERGY INPUT

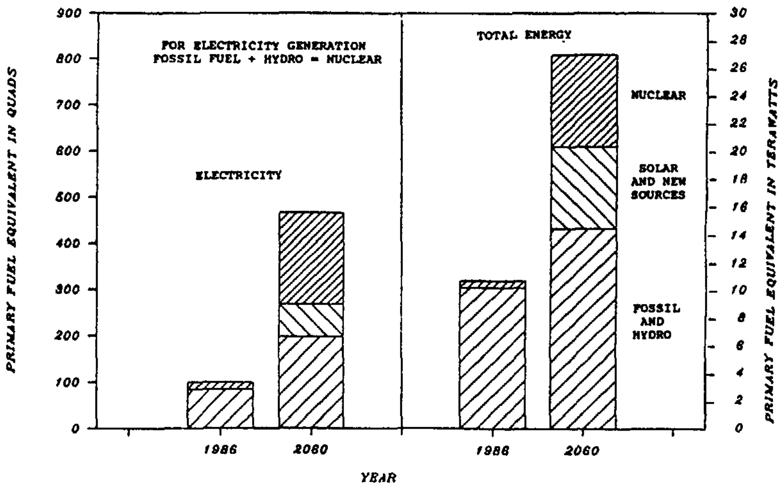


Figure 14
CONSERVATION CASE
CONSERVATION AND MAIN ENERGY TYPES

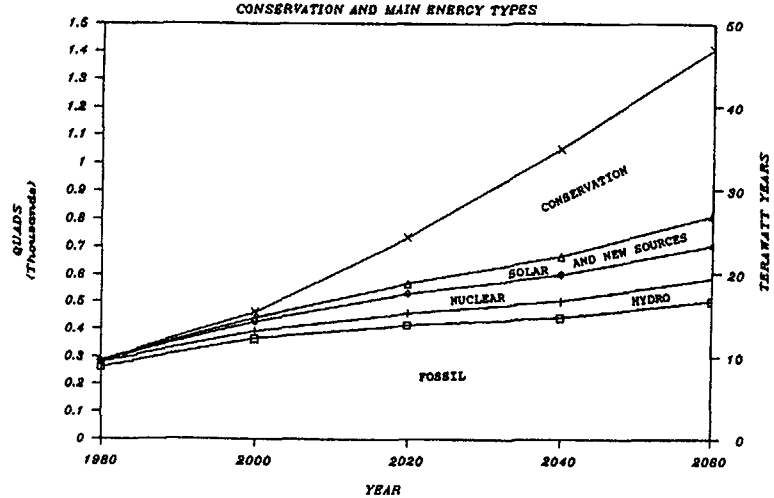


Table V

YEAR 2060 WORLD NUCLEAR POWER DEMAND:
FULL CONSERVATION CASE

Upper nuclear case	Fossil and hydro output fixed at 1986 level				
	10^{12} kWhr = 1,000 TWhr				
	Total electricity	Fossil and hydro	Solar	Nuclear	Nuclear capacity (GWE)
1986	9.97	8.41	--	1.56	301
2060	46.75	8.41	7.01	31.33	6,036
					Ratio 2060/1986: 20.1
Median nuclear case	**Nuclear output = fossil and hydro**				
2060	46.75	19.87	7.01	19.87	3,832
		Ratio 2060/1986: 2.36			Ratio 2060/1986: 12.7

It is much more realistic to assume that both hydro and fossil fuel capacity will increase to share the year 2060 load equally with nuclear, rather than be held constant. There are many regions where even small nuclear plants may be inappropriate for a variety of reasons. Thus, a continuous growth of each regionally competitive type of generating plant is likely to provide our future global mix. This scenario is shown as the median nuclear case in Table V and Figure 12.

The key implication of this study is that even with a full conservation program, both an increase in fossil fuel and nuclear generating plants is inevitable. Nuclear eventually must carry the major expansion if fossil fuel use is constrained by environmental or economic factors. Hydro may grow somewhat if ecological conditions permit. Solar, of course, can materially contribute to peak power needs, but contributes only modestly to total kilowatthour demand. The main future dependence will be on fossil fuels, primarily coal, and nuclear power. Such a projected mix for the full conservation case is illustrated in Figures 13 and 14. This projection is based on the current professional judgments on resource availability and resource costs. While it serves a useful means for providing a perspective of the future, the mix of energy types is pragmatically dependent on the economics of resource scarcity and the changing capital costs of energy equipment arising from technical developments and environmental constraints.

SAFETY OBJECTIVES

(Session III)

Chairmen

R. CARLE
France

V.A. SIDORENKO
Union of Soviet Socialist Republics

SAFETY OBJECTIVES FOR AN UNSURE PUBLIC

M. ROSEN
Division of Nuclear Safety,
International Atomic Energy Agency,
Vienna

Abstract

Despite an operating record marred by only one accident with consequences for public health, there remains widespread public concern that nuclear power and nuclear activities in general are too risky. This must be due in part to the nuclear community's collective inability to convincingly explain the realities of our radiation environment and the trivial changes introduced by nuclear power. Somehow an unsure public must regain confidence in nuclear power.

The real challenge of the 1990s will be to gain broadscale acceptance of nuclear technologies as a safe, well-regulated and non-detrimental to human health and environmental well being. A proposal is made for accelerating the communication process about the realities of the radiation environment through a concerted international effort. Four complementary objectives are advanced that would provide an informed basis for individual and collective decision-making.

INTRODUCTION

We have this first day emphasized the global environmental threat from fossil fuels and sought plausible energy mixes to reduce their growing negative effects on our planet. It has not been difficult to show this audience that a continued and expanded use of nuclear power will reduce destructive emissions which are changing the chemical climate of both the earth and its atmosphere. This might satisfy ageing nuclear engineers and some forward looking politicians, but most likely not today's public or the politician seeking re-election. In reality, almost universally, it is a minority of the public and far fewer in the political arena that would actively support increased electricity production through nuclear power. Thus, the curve of operating facilities levels at about 500 and construction activity trends towards zero.

The general public does not completely appreciate the complexities governing global environmental decisions. They view environmental effects of all industrialization as negative, and neither nuclear nor fossil electricity escape that verdict. But for nuclear, many are currently irrevocably convinced of the unrelenting health impacts of day to day operation and the nightmarish image of a severe accident. It is unfortunate that both extreme negative impressions, one for daily performance and the other for severe accidents, are reserved almost solely for nuclear activities. In comparison, the effects of other energy sources are perceived as somewhat bearable if not totally acceptable, at least in a practical sense. This must be due in part to the nuclear community's collective inability to convincingly explain the realities of our radiation environment and the relatively trivial changes introduced by nuclear power.

But, despite the needs of a concerned public, we now focus this meeting's attention on traditional safety objectives. Later, we will continue with future technological requirements for even better designed plants, which with some good likelihood may never be built. Before entering into this process, we should see if we can do better. To begin with, if we look at the current goals for nuclear safety as spelled out by INSAG, the Agency's 13 member International Nuclear Safety Advisory Group, we see three basic objectives very much in the traditional pattern; once more, none of which address the public concerns, but all of which unfortunately reinforce them.

First, there is an encompassing **General Nuclear Safety Objective** speaking to

> **"(the need) to protect individuals...by...maintaining in nuclear power plants an effective DEFENCE AGAINST RADIOLOGICAL HAZARD."**

The effective defence, we are then told, is fulfilled when the risk, as defined by the product of the probability of an accident and its adverse effect, is maintained lower than that from competing energy sources. Once the public grasps the need for a defence against radiological hazard, it needs no assistance in comprehending this goal. However, the concerned scientist has the unenviable task of becoming convinced that, with several hundred current and several thousand future reactors, which surely include the prospect of a number of problem plants, the accident likelihood is so low as to balance the potentially severe adverse radiological effects.

Second, we have the complementary **Radiation Protection Objective**, containing similar ominous warnings, which

> **"(requires) any release of radioactive material...(be) kept as low as reasonably achievable...and (requires the) MITIGATION OF...RADIATION EXPOSURES DUE TO ACCIDENTS."**

Third, and continuing the theme, there is the **Technical Safety Objective** to

> **"... (prevent) with high confidence...accidents in nuclear plants...(and) for all accidents..., even those of very low probability, radiological consequences, if any, would be minor; and...that the LIKELIHOOD OF SEVERE ACCIDENTS WITH SERIOUS RADIOLOGICAL CONSEQUENCES (BE) SMALL."**

This radiological consequence reasoning endures throughout many of the 62 additional supporting principles as spelled out by INSAG in their Basic Safety Principles for Nuclear Power Plants.

The INSAG document containing the three overlapping safety objectives has been well received by the nuclear community. It embodies a modern and technically understandable approach to ensuring nuclear safety. It appropriately and most certainly is directed towards the technical audience. However, the public, whose confidence we seek, can only be more convinced that in reality we have a dangerous technology likely to expose them to deadly radiation, and additionally possessing a potential for calamities. But I do not wish to detract from INSAG's accomplishment; we have all been driven by the need to ensure safety, not to explain it. For the technical challenge of the 1960s that approach was sufficient.

OBJECTIVES FOR AN UNSURE PUBLIC

What must characterize effective objectives for the global challenge of the 90s where the societal rejection of an energy source is the issue? They must speak to the unsure public and not just to the believing and still hopeful but ageing scientists. They must tackle the issues which concern the public, above all the need to somewhat understand and to believe that nuclear activities are not fundamentally harmful. Only in this way can we regain their confidence.

A First Objective must concern itself with convincingly communicating a non-controversial reality; **Low Level Radiation As A Fact of Life.** It must be directed to the public whose radiation literacy is low, but disturbingly also to many scientists whose fear is real. It should involve not only explaining the extensive variations in natural background radiation levels, but also, as a useful frame of reference, vigilantly relating each potential additional radiation exposure to that received from the natural environment. It must emphasize that we live in a radiation environment. It must show that the contribution of man-made exposures are principally from medical sources, and that nuclear power's portion is exceedingly trivial. Somehow the various radiation sources must be put into perspective with each other!

The Second Objective must speak to the real consequences or the **Impact of Low Level Radiation.** It requires demonstrating that for exposures of concern to most people, like those received each year from the natural background, or the much smaller one from the nuclear industry, the health and environmental effects can be considered not only just low, but of little relevance for both the individual and for society. Most importantly, it may require acknowledging that the current costly philosophy governing radiation safety decisions, in view of the low impact, proven or unproven, is not necessarily the best for the public interest. It may require formulating a more practical and simpler approach to ensure that measures to protect society are concentrated on real priorities. Somehow the true impact of low level radiation must be clarified!

The Third Objective, the most encompassing, must then address the **Comparative Health and Environmental Effects** of nuclear power along with those of its viable alternatives. It must speak to what matters, the net overall impact of the production of a given amount of energy. It must require demonstrating that while nuclear power in its day to day operation in a real sense is benign, this is not so for the alternatives' day to day health effects with their long term global environmental implications. It must require addressing the public's built up fear of a nuclear accident's devastating potential, and not only show that the probability is very low, but more so that the real consequences of a severe accident are tolerable both in terms of health effects, and in terms of contamination and the resultant need for evacuation and relocation; all of these aspects in comparison to the alternatives not so insignificant accident potential and consequences. It must require showing that among the principal fuels for electricity generation, when the entire production cycle from mining to waste disposal is considered, nuclear is cleaner, safer, and far less damaging to the environment. Somehow the effects of nuclear power must be put into perspective with other effects!

If we had in the past successfully addressed this third objective, a fourth would not be necessary. The Fourth Objective, essential to assuring a next generation of reactors, must address tomorrow's need for **Greater Simplicity and Understandability** so as to regain acceptance. The public has a distrust not only of radiation, but also of nuclear technology. This is not surprising in view of the nonrelenting references to radiation's hazards and two accidents which were not supposed to occur. The public now desires more safety, and not simply to be told and expected to believe that there is safety, but to understand and also to have natural processes available for help in an emergency. The leading nuclear suppliers recognize this and now seek acceptance through a new generation of smaller plants that look less at technological defence in depth and severe accident mitigation, and more to passive or natural safety with no need for heroic accident efforts. The public requires this nuclear simplicity which translates into simpler design, simpler construction, simpler operations, simpler everything. Perhaps this generation's children, given a higher radiation literacy, will not need these assurances and will once again accept more easily the high technology of nuclear power. Somehow an unsure public must regain confidence in nuclear power!

Let's examine in more detail, this time with the public and the political decision maker in mind, the four identified objectives necessary to ensure a nuclear future:

- **Low Level Radiation As A Fact of Life**
- **Impact of Low Level Radiation**
- **Comparative Health and Environmental Effects**
- **Greater Simplicity and Understandability**

I do not propose to formulate the objectives any further, but only through discussion to make clear the need for them, and hopefully to promote a determined effort by the scientific community to pull together and face the key issues governing nuclear power's survival. We begin with the first objective to explain our radiation environment.

o LOW LEVEL RADIATION AS A FACT OF LIFE

Ionizing radiation, unlike substances only recently added to our environment, has always been part of our surroundings. It has been widely researched and analysed. UNSCEAR (United Nations Scientific Committee on the Effects of Atomic Radiation) has played a major role in obtaining and evaluating worldwide data and the ICRP (International Commission on Radiological Protection) and the IAEA have formulated recommendations which govern the safe use of radiation sources. At the core of these recommendations is the linear dose-effect relationship with its no-threshold hypothesis implying it is not possible to be at zero risk when exposed to radiation. Although there is no evidence of health effects at low doses to prove it, the radiation biologist calls his theory eloquent and simple. Many violently disagree, some believing it ignores biological defence and repair mechanisms built up over multiple generations, while others argue that hormesis, or the stimulating beneficial effects of low exposures, governs the situations. Contradictory opinions can have their moments; witness the cold fusion controversy. But, before going further with this contentious aspect, let us look at the exposures of real interest.

UNSCEAR tells us that from recent studies the current average annual individual radiation dose to the global population from natural radiation is 2.4 milliSievert (mSv), with half due to lung exposure from radon. This value representing a weighted absorbed radiation energy can be taken as a useful reference measure, equivalent to 365 days of average background exposure. The actual exposure for typical individuals, depending on factors such as where they live, varies from about 1/3 to as much as 2 times the reference. Less typical individuals in some locations are known to receive many multiples of that value, up to 100 times greater than the reference exposure. People living in Denver, Colorado annually receive the equivalent of an additional

150 days or 1/2 year exposure to natural background as compared to those living in a more average exposure location as typified by New York City. Naturally occurring radon in the average Swedish home can add several years of exposure annually with additions of 100 years not rare.

To the yearly background we must add man-made exposures arising mainly from diagnostic medical irradiation which on a world basis is about 30% of our reference, but can be as little as 5% and as high as 400% depending on one's country. Thus, medical exposures principally from X-ray examinations add as little as 15 days or as much as 4 years of equivalent natural exposure annually. Past nuclear test explosions continue to contribute 10 days. Flying round-trip across the Atlantic can add 2 days from the extra cosmic radiation received. Turning to nuclear power, its releases currently contribute on average less than one hour, a lesser amount than contributed by the radioactivity releases from burning coal. For the small populations most exposed around nuclear facilities, it contributes typically 5 hours, but up to a very atypical 20 days.

Thus, radiation sources differ enormously in their contribution to the radiation environment. A more startling presentation reveals that for people typically exposed to nuclear power production, their daily exposure from nuclear facilities is 1/10 th of their exposure from the earlier atmospheric testing of nuclear weapons, and is almost 1/100 th of their exposure from medical irradiation. It is 1/1000th of their exposure from the natural background. In other words, such individuals' total daily exposure is more than 1000 times the minor exposure arising from day-to-day nuclear activities. For the average world inhabitant, the total exposure exceeds the minor contribution from the world's nuclear power facilities by more than 10,000 times. The nuclear exposure plays a trivial role. Have we communicated this to our unsure public?

With this array of relative numbers, as an individual, would you rather live in Denver or near a nuclear power plant located outside of New York City? Would you forego a flight across the Atlantic? A simple and easy response would only be possible if such decisions were determined solely by the actual daily radiation exposure. But decision making is complicated by the real or perceived health risk, which we are about to discuss, and by much more weighty social and emotional factors. Only if radiation effects are perceived to be high will they play a major role. We must bear in mind that for many practical situations people do weight the daily radiation factor as low or consider it not at all, except for nuclear power which ironically contributes the lowest exposure. To explore what the public is already accepting, let us turn to the second objective on the Impact of Low Level Radiation.

o IMPACT OF LOW LEVEL RADIATION

The radiation biologists of UNSCEAR attempt to give us some guidance on the health effects of low doses in their 1988 report to the United Nations General Assembly. They state:

> **"AN EXTRA DOSE THAT IS SMALL in relation to the background dose WILL NOT SIGNIFICANTLY AFFECT AN INDIVIDUAL, i.e., it will not change his total exposure situation noticeably. While the individual might still wish to avoid such a small extra dose, he would know that IT DOES NOT IN ITSELF PRESENT ANY SUBSTANTIAL RISK. THIS DOES NOT MEAN THAT THE DOSE IS ACCEPTABLE just because it is small: rather, acceptability would depend on the total harm the source is likely to cause and on society's appraisal of that harm."**

In essence, UNSCEAR avoids the crucial assessment by delegating the decision. The radiation biologists' deferral of the decision to society is entirely appropriate. But, the task is exceedingly difficult. The society is asked to make decisions based on often controversial information supported by scientific statements which are not easily interpretable; the quoted UNSCEAR guidance serving as a prime illustration of the dilemma. The scientists of UNSCEAR comfort us by explaining that small doses pose no substantial risk to an individual, but then burdens the decision maker with an impractical task of evaluating the total collective harm to society from a summation of trivial individual acceptable risks.

In seeking an answer, the decision maker may turn to the radiation safety specialists. The moralist among them advises to protect against all risks, even the smallest, now and into the distant future as well as on a global scale; an impractical approach unmatched by other industries. The theoretician among them advises to protect to some optimal level. To keep radiation effects As Low As Reasonably Achievable (ALARA) some propose a cost-benefit analysis. This well meaning scientific approach only compounds the basic problem. For the actual situations involving low doses, which are of real interest, the highly judgemental inputs necessary to balance the benefits against continuously changing and difficult to measure economic, social or political costs, make the results not meaningful. No matter how judgemental it also is, a simpler and a more understandable approach is desirable. But before attempting this, what are the radiation realities we are avoiding?

The health effects

We know that for very high exposures there are acute fatal doses and evidence of increased fatal cancer incidence. For lower exposures which are many multiples of annual natural background there is no evidence of human health effects. For the very small exposures of daily life which are fractions of the natural background, contrary to anti-nuclear pronouncements, there has been no observed overall increase in cancer rates for people who live near nuclear plants or for radiation workers, or for those in higher radiation environments such as airline pilots and those living at high altitudes. But, let us assume that as with almost all activities there is some risk and accept as a working hypothesis the UNSCEAR dose-effect relationship, although it may overstate the real radiation consequences. In Western Europe's population of 300 million, natural sources of radiation would cause annually about one in 50,000 people to incur a hypothetical fatal cancer, which translates into about 6000 early hypothetical deaths. Nuclear energy production would affect about one in 40 million or result in an additional 8 hypothetical fatal cancers. As a reference there are 600,000 real fatal cancers yearly, caused in part by 300 known carcinogens, along with one million fatal heart related incidents and 50,000 automobile deaths. For both natural background and man-made radiation we are calculating not only hypothetical, but also micro-effects. Have we communicated this to our unsure public?

More revealing is the conversion of these micro-numbers of fatal cancers into the effect on lifespan, a more meaningful measure for risks of all kinds. Each year natural background radiation might be reducing the average individual's life expectancy by 1 day while nuclear energy production might reduce it a further 30 seconds. Automobiles do not kill the old alone, and each year they are reducing average life expectancy by several days. Over a lifetime, automobiles will reduce life expectancy by almost 1 year; nuclear power might reduce it by 10 minutes. Somehow nuclear power must be presented in perspective.

The regulatory limits

Let's examine some existing and proposed regulatory exposure limits fixed by safety specialists whose task is to define a resonable safety level. In most countries, for the general public they are based on ICRP recommendations which restrict the average yearly lifetime exposure from man made sources to no more than 40% of the reference average yearly natural background exposure. It has already been noted that there are groups of people, including substantial fractions of several large populations exposed to radon gas, showing no adverse effects from yearly exposures to multiples of 10 times the reference value. If we must talk about micro-health effects, a lifetime additional exposure to the current limit might reduce an individual's life expectancy by 20 days which is the same theoretical radiation impact for someone moving at an early age from New York to Denver.

So called de minimus exposures, or more properly, the trivial exposures which arise from practices exempt from or below regulatory control as they are of no consequence to individuals or society, are being only hesitantly proposed between 1/1000 and 1/100 of the general public's exposure restriction. This is much less than the yearly fluctuations of the natural background for any person and is equivalent to between 1/2 hour and 5 hours calculated decrease in average life expectancy if an entire population were exposed to the cut-off value. In probabilistic terms the bases are a negligible lifetime individual risk of a fatal cancer less than 1 in 10 million to 1 in one million, which corresponds to about 3 to 300 fatal cancers in a population of 300 million.

Interestingly, today's exposures from the small effluent releases of nuclear power plants fall into this exempt category, as do those of today's consumer products such as smoke detectors and the many luminous time pieces which have an annual impact four times as great as from nuclear power. In no way could nuclear facilities with their potential for much larger releases be considered exempt, but the public's and the scientist's frame of reference must acknowledge the real trivial exposures from day-to-day operation. The efforts to establish exposure limits equivalent to death by lightening are admirable, but are we numbering ourselves to death? Are unrealisticly low radiation goals diverting us from the real priorities, as well as depriving us of benefits such as from food irradiation while exposing us to the negative effects of alternative energy sources?

How do we answer the need for prudent policy guidance if the radiation biologist cannot help and the safety specialist does not help? We must look for a third party who can assist in the judgemental aspects of radiation safety and the process of radiation acceptability. It is clear that the public does accept a large spectrum of radiation exposures, knowingly or unknowingly. The small level of risk is only one balancing factor among many non-measureables that determine acceptability. A missing element is effective risk communication which recognizes the complexity of risk acceptability and can explain the risk realities to all levels of society; the public, the regulator and the decision maker.

Risk communication is not a public relations activity; it must be undertaken by scientists who could participate in formulating guidance for policy makers as well as for effective and practical regulation. They must speak in a fuller and more comparative context. They would recognize that ionizing radiation may be hazardous, but they would also recognize that today's low man-made exposures pose a relatively minor public hazard when compared to other health and environmental disturbances. They would understand that radiation safety requirements governing small collective and future risks, are not only less relevant but certainly much less practical for society than those which focus on today's individuals. They would recognize that even assuming they could all be measured, the cost of protection and the cost of regulation of trivial exposures may far outweigh any benefits.

> Perhaps it is time we stop pursuing risk limits which are neither realistic nor practical for protection and which only reinforce the public's fear.
>
> Perhaps it is time that we stop pursuing ALARA in its impractical and imaginary search for optimal solutions for micro-effects.
>
> Perhaps it is time we consider returning to simple, realistic, and practical objectives which do not confuse the safety engineer, the practicing health physicist, or the public.
>
> Perhaps it is time we recognized and acknowledged the true radiation safety needs of society and gave proper priority to non reactor activities.

My concluding remarks will include a proposal for accelerating the risk communication process by establishing a concerted international effort in the field of radiation acceptability. But, before this, let us turn now to the subject of comparisons.

o COMPARATIVE HEALTH AND ENVIRONMENTAL EFFECTS

After effectively communicating the real radiation picture, our third objective to evaluate and compare the overall impacts of the various energy alternatives becomes manageable. The current objections to nuclear power, present or expanded, center on day to day operations and the accident mode as well as on waste disposal. These factors alone are not enough, as the entire production cycle from mining to waste management has varying negative aspects. For every energy source each stage must be assessed to give the total comparative impact, the sum of all detriments to the general public, to the worker, and to the environment.

The environmental risk

For normal operation, we can to some extent treat the environment expeditiously. To many, excluding the confirmed anti-nuclear activist, in view of the acid depositions, air pollutants and possible greenhouse contributants from the large SO_2, NO_x and CO_2 emissions of fossil fuels, nuclear power's small and controlled releases can convincingly be shown to have the lesser impact on the environment. There are other striking comparisons of environmental disturbances which can be made in terms of land demands for mining, transportation needs and power plant site space requirements. Waste disposal, another key environmental issue can be addressed in some measure by demonstrating that contained nuclear waste in terms of its limited quantity and ability for substantial decay, is potentially a rather small problem in comparison with the alternatives' whose voluminous dispersed and toxic waste will be continuously present.

The health risk

A common approach to health effects is to estimate, per quantity of electrical energy generated the delayed deaths caused by fatal illnesses incurred as a result of normal operations, and the acute deaths caused by accidents. For the undetectable impact from nuclear power we incessantly estimate radioactive releases and their potential effects through the dose-effect relationship. For the detectable signs of increased respiratory illnesses from fossils through SO_2, NO_x and particulates, what is missing is not only systematically collected emission data, but also recognized dose-effect relationships for toxic emissions which are only at an early stage of development. We discuss leukemia clusters near nuclear plants but fail to note that if they indeed exist, they should also be found near many fossil facilities with their release of coal borne radioactivity. A coal burning plant commits almost 2 times the radiation exposure as an equal sized nuclear plant. Electricity generation is a relatively minor man made contributor of radiation exposure when compared to the 100 times higher contribution from the phosphate industry through fertilizer and gypsum use. Have we communicated this to our unsure public?

With all of the uncertainties, it is easy to question comparative studies, but they are of value and necessary for informed decision making, although frequently misused. The results of numerous investigations have been reported in the literature. They consistently show that the health risks from routine nuclear power prodcution are generally lower than those from the other viable energy options, particularly for the general public.

For the production of 1000 MW of electrical energy each year, the occupational health risks are relatively low for all common sources of energy. They are the highest for the coal and wood cycle, being in the order of several cases of fatal illness and acute death. They are lower for oil and gas, and are close to zero for nuclear. For the same annual 1000 MW production, the public health risk, however, can be high. The coal and oil cycles under normal conditions can be each associated with up to 30 fatalities, with some estimates for these fossils of 20,000 cases of various non-fatal illnesses for an urban population which results in a significant amount of productive days lost. The risk for the nuclear cycle is only up to one acute death and one fatal illness.

The accident risk

It is clear from these figures, that in any comparison of fossil versus nuclear, the only factor which could alter a conclusion that nuclear is by far the more acceptable is the effects, both to the environment and health, from a large-scale accident such as Chernobyl. What were the Chernobyl effects? There were 31 fatalities out of about 280 who suffered acute injuries, all on-site plant staff or emergency response workers. No clinical symptoms of acute radiation syndrome were seen in the 135 000 people evacuated from a 30 km zone. For a severe accident, the acute effects of Chernobyl do not compare to the far greater technology-based deaths from the many mine disasters, capsizing oil platforms, refinery fires and explosions, gas pipeline explosions, and floods from over-flowing dams.

As for the potential long-term health effects to the exposed nearby population where no doubt some had high exposures, multiples of 10 higher than background, but in the range of occupationally allowed exposures, there have been no observed effects to-date for the exposed individuals. Ongoing follow-up studies may be difficult to interpret owing to numerous factors, including the increased medical attention which may improve health and life expectancy compared to a more average population. There may very well be a small increased incidence of leukemia, which seems to be the first cancer to emerge in a population after radiation exposure. Nobody desires increased leukemia. However, we must recognize that substitution of Chernobyl's 4000 MW of nuclear electricity by coal or oil would not be risk free. Pollution episodes from the burning of fossils have been found to increase death rates and serious illnesses among people with heart and lung desease. The health effects of the Chernobyl disaster must be examined in a fuller context.

Apart from the serious but local consequences of the accident, which included relocation of local inhabitants and contraints on land and water use, the accumulated information suggests that public health in Europe and beyond was not significantly affected. For Byelorussia, which included the more affected regions near Chernobyl, UNSCEAR estimated the first year's additional exposure after the accident as equivalent to one year of natural background. Elsewhere in Europe, the highest first year additional exposure outside the USSR occurred in Bulgaria where it amounted to less than one third of background. To the world population, the accident added a few percent of background. Estimates of hypothetical increased cancer deaths have little significance when compared with the 20% of the population whose multiple millions of deaths will be attributable to "natural" cancers.

As for the many evacuations, it may be advisable to re-examine the Chernobyl situation. Because, early on, the nature and potential course of the accident were unkown, decisions to evacuate are understandable. Subsequently, on the grounds of public health protection, evacuations were undertaken and are still being contemplated to ensure that no inhabitant would exceed a lifetime exposure over a 70 year period of 0.35 Sieverts. This corresponds to 140 times our reference natural background exposure or an average of 2 times background annually, a value well below the variations that people customarily tolerate worldwide from medical exposures alone. Importing and consuming uncontaminated food, using processed food, as well as changing medical diagnostic practices are remedial measures which could be equally effective. With no preventive measures, an individual's expected lifetime might hypothetically decrease by one day annually. A repetition of a Chernobyl like response was undertaken in Goiânia, Brazil after the incident involving a Caesium-137 therapy unit. Remedial actions, including evacuation, demolition and removal of seven homes along with large quantities of soil, were based on even more stringent criteria of a first year exposure limit similar to that at Chernobyl and a long term yearly exposure limit 1/5th that of Chernobyl.

What is abundantly apparent from all of this, is the need for a more realistic understanding of radiation safety goals. The frame of reference used by the radiation safety specialist has been a desire to formulate and implement extremely conservative levels of safety in design and practice for situations which are somewhat predictable and controllable. This mind-set is not at all suitable for post-accident situations where the specialist is faced not with preventing exposure, but dealing with it. For the latter case much less stringent exposure criteria may be perfectly acceptable, particularly when a variety of remedial measures are readily available, and where the risk is low but the financial and psychological implications for individuals and communities may be high.

The similar situation involving the large populations currently living in homes where radon exposures exceed existing limits could be seen as presenting the same dilemma. If the exposure criteria for Chernobyl and Goiania were applied, thousands of inhabitants would have long ago been removed form their homes. Have we communicated this to our unsure public? The widespread radon situation illustrates the need not only to deal more realistically with low level radiation, where the risk if any is small, but also to appreciate the difference between planning protection and dealing with actual consequences, particularly non-measurable ones. The need is urgent to present a balanced picture to society.

o **GREATER SIMPLICITY AND UNDERSTANDABILITY**

Finally, after dealing with the three radiation oriented objectives, let us turn to the need for Greater Simplicity and Understandability in nuclear safety as we search for tomorrow's reactors. Experience is telling us that smaller and simpler may be the real requirements for new plants in the less industrialized countries. For many others, simplicity in construction, operation, and maintenance shows promise for economic advantages. But for all, it may be the general concern about safety and public acceptance which will drive the downsizing which in turn allows more forgiving safety systems. Experience has shown the public that today's reactors have a potential for very severe accidents. We can tell them that tomorrow's designs will exclude these events, while pointing out that we have not thrown out yesterday's automobiles with the introduction of new models with safer breaking systems and 4-wheel drive.

What are the basic requirements for tomorrow's new generation of plants? With the following three days to focus on this issue, permit me now to briefly speak for the disenchanted public who desire small, simple and safe. To this public, small amd simple translates into less complexity and more safety. But the key to an acceptable safe design for the substantial number of intended reactors, will be one which conclusively and not probabilistically prevents large accidental radioactive releases. To the real sceptic, this means three requirements: no core melting, along with a back-up containment and a low population site.

The first requirement may not be sufficient, but is surely necessary. Low power density reactors capable of passive emergency cooling systems, static through a capacity to store decay heat or dynamic through natural coolant flow phenomena, is one way to meet this goal. This would provide time, the key ingredient in preventing severe accident consequences. It would permit the operator to determine what is happening and to deal with it, or even allow time for specialists to arrive at the site if necessary. The need for and availability of time is the common lesson of TMI and Chernobyl. The second and third requirements are somewhat linked and will require back-up containments of the old style or possibly through innovative new concepts to assure at least the nearby population, large or small, that the expert's forecasts are not once again in error.

PROPOSALS

Successfully dealing with the safety objectives for an unsure public will substantiate nuclear power's friendliness to the environment. This is not so for many of the viable energy alternatives with their threatening global implications. What can we do now to convince the public and the decision makers? Perhaps nothing, but implementing several proposals emanating from the four objectives may help.

First, in dealing with **Low Level Radiation As A Fact of Life,** the public needs understandable, factual and unemotional information. The radiation specialist can contribute by avoiding non-communicable Bequerels and Sieverts, and surely collective dose commitments, as well as hypothetical cancers and deaths in addressing the public. Natural background radiation comparisons and possible lifespan changes may be more meaningful and clearly less threatening. A long term programme directed by the entire nuclear community is necessary to communicate radiation's real nature to the lay and the scientific audience. Would any of you have eaten fresh mushrooms from Europe after the Chernobyl accident? The IAEA is speaking to that question through increased public information brochures and presentations to explain natural sources and the small man-made contributions, be it from the use of fertilizers, the burning of coal or nuclear power. The Division of Nuclear Safety now has full time staff for editing and technical writing. We have also newly renamed the technical section dealing with ionizing radiation's effects, from the Radiation Protection Section to the Radiation Safety Section which more properly characterizes its work.

Second, in dealing with the **Impact of Low Level Radiation**, we must clearly distinguish between the science of radiobiology necessary to study health effects, the techniques of radiation safety necessary to achieve safety and the skills of communication necessary to gain radiation acceptability. Each of these three areas requires different capabilities. The IAEA is considering for its next-biennial programme an entirely new activity devoted to radiation acceptability, an area not yet explored at an international level. A first step would entail establishing an Advisory Group on Radition Acceptability composed of credible scientists and effective scientific communicators who would provide and explain risk related statistics and comparisons, and who could also aide in the formulation of practical regulations. A profitable second step would have this group, with some haste, reassess the past and on-going suitability of the radiation safety response to the Chernobyl accident within the framework of a fuller and more comparative view of the effects of low level radiation, and of course with the full benefits of hindsight.

Third, in dealing with **Comparative Health and Environmental Effects**, the public must be shown that generating electricity by nuclear power is a clean and safe method, both absolutely and in comparison with alternative methods. Here again, the IAEA is establishing a new programme on Comparative Assessments of Nuclear Power with Alternatives. It will develop techniques to facilitate, within the decision making process, the consideration of the environmental and health effects of nuclear and alternative energy systems together with other technical, economic, and fuel supply factors. An International Senior Expert Symposium on Electricity and the Environment in co-operation with a number of intergovernmental bodies and non-governmental groups will be held in Helsinki, Finland in May 1991. The concrete output would be a series of scientifically backed issue papers addressing the future supply of electricity in an environmentally sustainable manner.

Fourth, in dealing with the public's current need for **Greater Simplicity and Understandability** it is time to unequivocably admit the value of re-examining and pursuing the simpler and safer small plant option. Next month's IAEA General Conference will feature a 2 day special scientific meeting on "The New Generation of Nuclear Power". Three technical sessions will address the Plant Owners' Requirements, the Views of Regulators and the Suppliers' Readiness. A final panel discussion will deal with the need for governmental support. Surely some development support and a more unified approach to regulation may help, but winning acceptability for nuclear power must have priority. The last item could assuredly benefit by enhanced international co-operation.

CONCLUSION

There is a need for action. Time is not on the side of the nuclear proponent. If we wait for the public to perceive a need for nuclear power, it could very likely be too late.

THE INSAG-3 BASIC SAFETY PRINCIPLES

H.J.C. KOUTS
Brookhaven National Laboratory,
Upton, New York,
United States of America

Abstract

The report of the International Nuclear Safety Advisory Group on Basic Safety Principles for Nuclear Power Plants (INSAG-3) is discussed. The fundamental and the specific principles as well as their application to plants of future types are presented.

Background.

A reasonable starting point for discussing the safety of nuclear installations of the next generation and beyond is a review of the principles on which safety of existing types of nuclear plants is based. These principles are contained in the document numbered INSAG-3, and issued by the International Nuclear Safety Advisory Group (INSAG) in 1988. The document is titled, "Basic Safety Principles for Nuclear Power Plants."

INSAG is a group established by the Director General of IAEA in 1985 as a nuclear safety advisory body. One of the more important activities assigned to it was to formulate, where possible, commonly shared safety concepts. This activity led to the preparation of INSAG-3 as the Group's view of the set of principles underlying safety of electricity generating nuclear plants.

The immediate reason for preparing and issuing INSAG-3 was that the international consequences of the Chernobyl accident had emphasized the need for common safety principles for all countries and all types of nuclear power plants. As drafting went on, it became evident that the means for attaining safety of nuclear power plants had progressed to the point where a complete set of commonly shared principles for ensuring a very high level of safety could now be stated for all nuclear power plants. It is believed that the document as it was finally completed achieves this objective.

Introductory Comments.

At the outset, INSAG stated that the document concerns the safety of nuclear power plants used to generate electricity. However, it added that most of the points are also valid for nuclear power plants used for other purposes. It was also stated that the principles in the document do not constitute a set of regulatory requirements. However, it may also be noted parenthetically that steps have been taken in several places to extend the applicability beyond that envisaged by INSAG. The Basic Safety Principles have been incorporated into regulations in some countries, and in the United States a generalized form of them is being developed to apply to all types of nuclear facilities of the Department of Energy.

Yet the point remains that the Basic Safety Principles are not meant to supplant the NUSS series of guides and standards issued by the IAEA. NUSS is formulated in terms more easily adapted to regulations than is INSAG-3. NUSS issuances are presently under review to make their content and emphasis more nearly parallel to INSAG-3, though I have not found any place in which the two contradict each other.

I return to the document. INSAG begins the exposition by making a number of general statements. Among the more important are the following.

-The use of INSAG-3 will not guarantee absolute safety, because there is no such thing. But it will lead to a very high level of safety.
-Some of the public concern as to safety of nuclear power plants is caused by their use of high technology. But it is high technology that makes the plants safe, through defense in depth.

-Decisions on improving safety should be balanced. Resources should not be used where the improvement would be marginal.
-There is a connection between safety and reliability of a nuclear plant. A plant that is safe will tend to be reliable in generation of electricity.
-Nuclear plants are now safer than they were before the large accidents of recent years.

General Features of the Document.

INSAG then explained some of the features of the document and the principles that it contains. It was emphasized that they were not new principles; they could not be new because they are commonly shared and have been developed over the years as the nuclear industry has grown around the world. Rather, the document contains a logically structured set of shared principles that must be used in their entirety if the benefit is to be realized.

The document proceeds from the general to the particular. Three objectives are stated. The first is very general; the second and the third have the appearance of specialized interpretations of the first and may be regarded as improving substance and structure through viewing from different perspectives. There follow twelve fundamental principles that state in general terms the means of achieving the objectives. These fundamental principles do not state in clear, unambiguous ways what must be done for safety. They are more in the nature of philosophical guides or broad concepts that require further fleshing out to take on operational meaning. That purpose is accomplished through the fifty specific principles. The specific principles could stand alone, but the objectives and the fundamental principles pull them together into a logical structure. Specific principles can be traced back to the fundamental principles, and the fundamental principles serve as a bridge to the objectives.

Each objective and each principle is stated in terse, memorable form. Since the brief sentences making the statements cannot tell all of the content, each is followed by a discussion section that rounds it out, including meaning, coverage, emphasis, and exceptions. The discussion section is just as important as the statement.

The present tense is used throughout, to indicate that the principles and their accompanying discussion describe the situation that exists in well-managed circumstances of the kind the document seeks to promote.

Emphasis.

If I had to say where the document places its major stress, I would have to say on safety culture as the most important safety ingredient of all nuclear activities, on defense in depth as the principal technical means of realizing safety, and accident management and accident mitigation as the technical and procedural backup for protecting the plant and the public.

Two other topics that are not usually emphasized in safety documents also receive particular attention in INSAG-3;these are firm and well-structured management practices based on line management and on placing authority and responsibility in the same places, and experience feedback as the means of disseminating information of safety importance within and among nuclear organizations.

Objectives.

Let me now turn to the content of the document and discuss the objectives and the principles. To do so I must abbreviate them by leaving out much of the discussion and shortening the statement of each even more than was done originally. This will be at the expense of fidelity to the total content.

The first safety objective is a general one, which is: to protect individuals, society, and the environment from radiological hazard. A standard of protection is given: the level of risk from generating electricity in nuclear plants should not exceed the risk from making electricity by other viable methods.

This is followed by a radiation protection objective which illustrates one feature of protection. It has three parts. First, routine radiation exposures should be held below values assigned as limits by standards and regulations. Second, these exposures should also be held as low as reasonably achievable. Third, exposures from accidents should be mitigated. This last means not only that measures should be taken if an accident were to start, but preparations should be made beforehand through emergency planning.

The third safety objective is termed "technical." It also has three parts. The first and most important is that accidents are to be prevented. The second is that radiological effects of accidents that might conceivably occur are to be small. The third is that severe accidents with large radiological effects should be highly unlikely. The discussion includes definitions of engineered safety features, of design basis accidents, and of risk as the product of probability and consequences.

In addition, the discussion section accompanying the third objective contains numerical safety objectives. The probability of an accident with severe core damage should not exceed 10^{-4} per reactor year now, and 10^{-5} per reactor year at future nuclear plants, with full use of the INSAG-3 principles. The probability of an accident requiring early off-site mitigation measures should be an order of magnitude smaller.

Fundamental Principles.

The fundamental principles follow. They begin with three management principles. The first is that a safety culture is present in all activities involved in nuclear power, starting with upper management and diffusing downward, and characterized by dedication and openness. The second states that the operating organization is responsible for the safety of the nuclear plant, not only for the safety in operation but in all aspects of the plant. This does not eliminate responsibilities of designers, manufacturers, constructors, and other groups. The third fundamental management principle is that government establishes a regulatory system, with functions defined in the discussion section.

Three defense in depth principles follow. The first is that defense in depth is used as the technical means of achieving safety, based on barriers to prevent the release of radioactive material and measures and systems to protect the barriers. The second defense in depth principle emphasizes that prevention of accidents is the primary means of achieving safety. The third is that mitigation measures are used as backup to accident prevention. Mitigation assumes many forms, covered by accident management and emergency preparedness.

The remaining six fundamental principles are called general technical principles. The first states that proven practices are used at nuclear plants, covered generally by approved codes and standards. The second says that quality assurance practices are used, not only in manufacturing and construction, but also in all other activities important to safety. The third says that account is taken of human factors in safety measures and procedures. It discusses attention to the layout of the plant, training, and written and tested procedures, and the need to allow for human factors in maintenance activities. The fourth discusses required safety assessments, including both deterministic and probabilistic analyses and safety analysis reports. The fifth enlarges on the use of radiation protection practices. The last discusses the importance of experience feedback, both from operational events and safety research. It discusses the importance of studying and preventing recurrence of accident precursors.

<u>Specific Principles.</u>

The fifty specific principles that come next are divided into categories, with the numbers in each as follows:

Siting	4
Design	22
Construction	2
Commissioning	4
Operation	12
Accident Management	3
Emergency Preparedness	3

Some have commented that there should be more than two principles on construction. In fact, it is difficult two make a break between design and construction, and many of the design principles apply also to the construction phase.

The principles follow the course of realization of a nuclear power plant starting from its conception and on into its operation. Requirements for the decommissioning phase are referred to, also. The two final categories of principles cover eventualities that should never be encountered, but which must be considered in design of safety as part of defense in depth.

I will not go in detail into the specific safety principles, and I must refer you to INSAG-3 itself for a complete treatment. I will illustrate their flavor by discussing some of the design principles. The design principles are themselves divided into categories, as follows:

Design Process	3
General Features	7
Specific Features	12

For illustration, the first five principles covering specific features of design are as follows:

Protection against power transient accidents.
Reactor core integrity.
Automatic shutdown systems.
Normal heat removal.
Emergency heat removal.

The first discusses the use of negative reactivity feedback features and reliably safe shutdown systems. The second describes how the reactor core is made strong and rigid to endure effects of heating, shaking, and mechanical vibration, and is made of high quality fuel. The third discusses independence of safety and operating systems of the plant, methods of ensuring reliability of shutdown systems, and anticipated transients without scram. The fourth discusses reliable removal of heat during operation, and the use of normal heat removal systems to cool the core under abnormal conditions. The fifth refers to the use of emergency heat removal systems for ensuring a reliable final heat dump capability.

Application to Plants of Future Types.

The above exposition should give a general feel for the content and character of INSAG-3, which was specifically structured for nuclear plants of current types. The kinds of plants discussed at this workshop are of two types: those which have designs evolving from existing types of plants, to improve certain safety characteristics, and those which would incorporate innovative features to serve safety objectives through innate design. In all cases the intent is to reduce risk below the levels that have been indicated by probabilistic safety assessments to be characteristic of existing types of nuclear plants. One widely shared feature of the concepts is a trend to less dependence on human factors.

The proponents of some of the designs that will be discussed say that their nuclear plants will be extraordinarily safe. Some concepts envisage complete freedom from the possibility of reactivity types of accidents, or guaranteed shutdown heat removal from heat conduction, radiation, or natural convection cooling.

These views raise some interesting questions. If a nuclear plant could be made super safe, would this eliminate the need to consider accident management features and procedures? Would accident management have to be considered in design? Would there still be a need for emergency preparedness measures? Where design has removed a certain accident pathway, would defense in depth still be needed? And could such a plant be built and operated almost anywhere?

Another set of questions can be asked concerning the Basic Safety Principles. Would they have to be changed in application to these advanced kinds of plants? Should principles be restated with a change in their emphasis? Would the discussion sections need rewriting? Should the report be restructured? Should some principles be dropped?

INSAG addressed such questions in the document. It said, in effect, that for plants that are believed to possess more intrinsic safety features, there should be a demonstration through experiment or experiment-based analysis that each safety principle is satisfied, no matter which method is used to achieve adherence to the principle. This reflects the belief that the Basic Safety Principles are the ways by which safety is attained, whether through provision of special design and operating features and engineered safeguards or by more intrinsic means. It is simply observed that there is a possibility that the means of attaining safety will be more direct in some designs than others.

Let me close by noting a corollary to this INSAG position that can have important benefits for future designs. One application of INSAG-3, so far unexploited, would be to tailor future plants to meet the safety principles. Adherence to the principles would be deliberately built into the design and the principles would take on the nature of a check list. This would ensure their being satisfied in the future design.

PANEL PRESENTATIONS

SAFETY OBJECTIVES AND PRINCIPLES FOR NUCLEAR POWER PLANTS (75-INSAG-3)

J.T. ROGERS
Department of Mechanical and
Aerospace Engineering,
Carleton University,
Ottawa, Ontario,
Canada

1. GENERAL ASSESSMENT OF 75-INSAG-3

The Advisory Committee for Nuclear Safety (ACNS) to the Atomic Energy Control Board (AECB), the Canadian regulatory agency, reviewed the International Atomic Energy Agency Safety Series No. 75-INSAG-3 "Basic Safety Principles for Nuclear Power Plants" [1], in the light of previous ACNS reports ACNS-2 [2] and ACNS-4 [3]. The results of the review are given in ACNS report ACNS-16 [4].

The ACNS considers 75-INSAG-3 to be, in general, a very good statement of the basic safety objectives and safety principles for a nuclear power plant. The INSAG report is particularly effective in showing the interconnections of the safety objectives and principles and in demonstrating how they form an inter-related logical structure. The report also emphasizes how certain fundamental principles (i.e., management responsibilities, defence-in-depth) pervade the entire structure of safety principles.

The ACNS found that the objectives and principles stated in the INSAG report are essentially consistent with the safety objectives in ACNS-2 and with the recommended general safety requirements for nuclear power plants given in ACNS-4. In as much as the objectives in ACNS-2 have been accepted and endorsed by the AECB and as the proposed requirements of ACNS-4, with the exception of certain specific proposals for a more risk-based approach to reactor licensing, represent current Canadian practice, the objectives and principles o the INSAG report are consistent in general with present Canadian practice relating to nuclear power plants.

The ACNS response to the INSAG report thus is consistent with that of the rest of the international nuclear community, which was very positive in general [5].

Some specific comments provided in ACNS-16 are discussed in the rest of this presentation. Also presented here are some additional comments arising from subsequent on-going consideration of nuclear safety issues by the ACNS but which, at this stage at least, represent the writer's views only.

2. SAFETY CULTURE AND INSTITUTIONAL QUALITY ASSURANCE

While there are no conflicts between the INSAG management principles and the thrust of ACNS-4, the ACNS now believes that more emphasis than is given in ACNS-4 needs to be placed on such factors as a sound "safety culture" in organizations involved with nuclear power and on the effectiveness of such institutions in ensuring the safety of the operation of nuclear power plants and related activities. To this end, the ACNS has made recommendations to the AECB [6], arising from its assessment of the Ontario Nuclear Safety Review [7], commissioned by the Ontario government in the wake of the Chernobyl accident, on identifying the elements of a sound "safety culture" and on improving the institutional effectiveness of the AECB itself with respect to reactor safety. In addition, the ACNS believes that more effort is required to ensure that institutions involved in activities related to nuclear power perform in a safe manner. While conventional nuclear quality assurance standards require, to some extent, certain standards for the management of organizations involved in nuclear activities [8], and while the Institute of Nuclear Power Operations has developed performance objectives and criteria for utility management [9], the ACNS believes that more emphasis needs to be placed on the quality of all institutions involved in nuclear power including the regulatory bodies. To that end, it is preparing a document making recommendations to the AECB on Institutional Quality Assurance [10].

3. NON-RADIOLOGICAL SAFETY IN NUCLEAR POWER PLANTS

The INSAG report is restricted to questions of radiological safety only. The neglect of non-radiological safety in the INSAG report could lead to this question being relegated to secondary importance, which could lead to poor performance in this area and which could detract from the development of a sound safety culture. Unlike the INSAG report, ACNS-2 [2] does include a safety objective with respect to non-radiological hazards. The importance of not neglecting non-radiological hazards in nuclear power plants was underlined in the report of the Ontario Nuclear Safety Review [7]. The ONSR suggested that Ontario Hydro, in concentrating on the nuclear component had not paid enough attention to conventional occupational risks.

4. RADIATION PROTECTION PROCEDURES

In paragraph 240 of the INSAG report, it is stated that "Specialist staff under the control of plant management provide a comprehensive radiation protection service". This statement, and the remainder of the paragraph, does not recognize the practice of Ontario Hydro of having all nuclear generating station staff being responsible for their own radiation monitoring (the radiation protection specialists play an auditing and advisory role). This practice was commented on favourably in the OSART review of the Pickering NGS undertaken in 1987 [11]. In the writer's judgment, this practice would contribute more to the development of a safety culture among all the workers at an NGS than the conventional practice of having a specialist group responsible for radiation monitoring.

5. MINOR POINTS

The INSAG report gives little attention to the problems of solid waste management at nuclear power plant sites. Also, insufficient attention is paid to the need to consider plans for eventual de-commissioning of nuclear power plants during the design stage and for updating of these plans as experience is gained.

6. OBJECTIVES AND PRINCIPLES FOR THE NEXT GENERATION OF NUCLEAR POWER PLANTS

Although this panel is concerned with current safety objectives and principles, a few words about requirements for "the next generation and beyond" appear appropriate. By their nature, there should be no changes required in the safety objectives stated in 75-INSAG-3 for the next and future generations of reactors. One would also hope that "Basic Safety Principles for Nuclear Power Plants" would not represent a transitory set of requirements, needing updating every few years. With a few exceptions, it appears that the principles stated in 75-INSAG-3 should stand the test of time.

7. CONCLUSIONS

One element stands out in many of these comments; the emphasis on "safety culture" and institutional quality assurance. Reviews of catastrophic accidents, both nuclear and non-nuclear, show that although blame was often attributed to design error or operator error or both, the essential failure in many cases was institutional [10,12]. This fact emphasizes the need for greater efforts in these areas to define more precisely what is meant by safety culture so that the concept does not become counter-productive [13]. It is also essential that the elements of an effective institutional quality assurance be clearly identified and eventually incorporated into an overall quality assurance program to ensure the continued safety of nuclear power.

ACKNOWLEDGEMENT

The writer has drawn on comments in a letter written by J.A.L. Robertson, now a colleague on ACNS, to Dr. Rosen of IAEA covering 75-INSAG-3. He is also indebted to Mr. Robertson for generating an increased awareness of the need for attention to institutional quality assurance in the nuclear industry.

REFERENCES

1. Basic Safety Principles for Nuclear Power Plants, IAEA Safety Series No. 75-INSAG-3 (1988)

2. Safety Objectives for Nuclear Activities in Canada, ACNS-2, AECB INFO-0055/REV-1 (1982)

3. Recommended General Safety Requirements for Nuclear Power Plants, ACNS-4, AECB INFO-0116 (1983)

4. Assessment of IAEA Safety Series No. 75-INSAG-3 "Basic Safety Principles for Nuclear Power Plants", ACNS-16, AECB INFO- (1989)

5. Basic Safety Principles for Nuclear Power Plants: INSAG Evaluation of the International Response, IAEA Bulletin, 31,1 (1989), 44-45.

6. Recommendations and Comments on the Report of the Ontario Nuclear Safety Review, ACNS-15, AECB INFO- (1988)

7. The Safety of Ontario's Nuclear Power Reactors, Ontario Nuclear Safety Review, 6 vol., Ontario Ministry of Energy, Toronto, Ontario (1988)

8. Basic Quality Assurance Program Requirements for Nuclear Power Plants, Canadian Standards Association Standard CAN/CSA-N286-0 (1988)

9. Performance Objectives and Criteria for Corporate Evaluations, Institute for Nuclear Power Operations, INPO 87-030 (1987)

10. A Proposal for Institutional Quality Assurance, ACNS-17, in preparation

11. Operational Safety of Nuclear Installations. CANADA. Pickering Nuclear Generating Station OSART Mission, IAEA-NENS/OSART/87/11 (1987)

12. MOSEY, D., and WEAVER, K., A Discussion of Institutional Failure and its Importance to Nuclear Safety, Proc. 9th Annual Conference, Canadian Nuclear Society (1988)

13. WEAVER, K., Treading Warily with Safety Culture, Bulletin of Canadian Nuclear Society, 10, 2 (1989), 5-10

SOME GENERAL IDEAS FOR DISCUSSION ON THE SUBJECT OF SAFETY GOALS AND OBJECTIVES

J. PALOMO
Hidroeléctrica Española, SA,
Madrid, Spain

Establishment of some Kind of safety goals and objectives, based upon the extended use of probabilistic risk and safety assessments, is needed and therefore this subject is gaining increase acceptance in the nuclear community as an appropiate mechanism for dealing with residual risk of nuclear power plants operation.

Important issues have come into place to develop more specific plans for using safety goals and objectives as it has been stated by different Organizations across the board. I have picked up the following three issues, at least:

1. To set up an adequate framework for discussions between regulatory authorities and the operators and designers.

2. To provide a rational basis for a coherent and consistent approach to nuclear safety as a whole.

3. To recognize the strength of proabilistic risk analysis tecniques and progressive solution of its limitations such as the human factors problem, systems dependencies, models uncertainties and data base completeness.

Nowadays we have to consider the possible use of safety goals as aspirational targets for judging the effectiveness of current regulatory requirements and future changes and to be cautious if they are perceived as candidate quantitative criteria or standards to be required to meet. This is a common thinking shared among the nuclear industry and regulatory bodies in many countries.

At present, the main approach to nuclear safety is still based on deterministic techniques for most countries, fundamentally based upon a set of engineering principles and safety factors. However some countries begin to jointly use deterministic and probabilistic approaches in evaluating and improving safety.

In the future, we can foresee a challenge to any Nuclear Regulatory Commission to integrate probabilistic analysis in the regulatory process, and improve the basis for discussion and communication on safety issues, as probabilistic safety assessments become a powerful tool for continuous operational safety management and periodic safety analysis. Meanwhile, relations between probabilistic safety analysis results and deterministic criteria and limits ought to be clarified.

The using of probabilistic safety assessments, for regulatory decisions and for the management of plant safety, can be thus perceived as one of the most important and promising areas to prevent serious accidents from happening and to improve and harmonize safety levels, for current and future plants, and we therefore are going to need those goals to be clearly defined.

In the 1960's and 1970's the safety concept was adhered to the "defense in depth" philosophy, however nowadays there is an extension of that protection concept into the range of beyond design basis accidents and the using of additional safety principles and objectives covering areas such as accident management, probabilistic risk analysis and evaluation of operating experience etc. The general attention is focused first toward incidents and accidents prevention and secondly around accidents mitigation mechanisms.

The existing residual risk is low in comparison with other risks in our civilization, as it is recognized by anoyone, and it could be further reduce by looking for excellence in plants operation, subjects like early detection of faults, man-machine interface, man-man communication and comprehension, training, safety culture, emergency procedures and accident management have been and will continue being addressed to look for strong recommendations to accomplish carefully chosen objectives so as to enhance plants safe operation.

I am frequently asked: "How safe are nuclear power plants ?". I always answered qualitatively by saying that the license garantee a reasonable assurance to protect the public health and safety; and quantitatively by stating that nuclear risks are much lower as compared to other every day risks. We know that two questions are involved in fact:

(1) How safe are the plants design ?

(2) Are the plants safely operated ?

The first question can be addressed by probabilistic safety assessment methods and for the second question we have indicators of licensees performance so that we can already answer positively to both questions. On the other hand, for good licensee performance, we absolutely need management involvement, right utilities policies and the operators effectiveness and awareness for safety culture.

Thus, a complete set of goals is necessary to meet excellence, going beyond the minimum envelop of previous safety concepts, in order to say that nuclear safety is completely treated as a whole, in a more harmonized and consolidated way, addapting it to the advancing state of science and technology.

Every one recognizes that the INSAC-03 report provides the logical framework for understanding and underlying objetives and principles of nuclear safety, from the upper level of risk to the lower level of plant operations performance. Regulators may set forth numerical reliability rules for nuclear risks and the most important safety functions, and here two trends emerge depending upon to limit the probability of severe accidents or to limit its consequences. Licensees, on the other hand, could further conduct systematic evaluations of plant structures, systems, components and overall performance and set objetives at the system level and for performance indicators and if those goals are not meet the licensee should set goals at lower levels, i.e. key components level, to improve systems availability and plant operability performance.

The licensee should also factors the effects of aging into maintenance programs and establish a reliability program to monitor plant performance. Furthermore, ALARA programs and operating experience feedback analysis should continuously be carried out and its results factored in the whole process.

Let me now tell you what is the current status in Spain on safety objectives.

At present, the licensing framework remains deterministic; nevertheless the spanish nuclear Regulatory Body (CSN) in promoting and enforcing the performance of plant specific probabilistic safety analysis (PSA) to every plant in the country.

The CSN has established and initiated a national integrated PSA program, whose main objective is that all spanish plants have specific PSAs within a few years. A PSA has already been completed for Garoña and Almaraz NPPs and two more are being started for Asco and Cofrentes NPPs.

Even when at this time the CSN has not made any commitment regarding the future use of PSA results within the regulatory process, it is the understanding of the spanish utilities that PSA will be given a credit commensurable with the importance it does have for being jointly use with the deterministic approach in evaluating and improving safety.

Within this regulatory philosophy it can be foreseen that in the future some kind of safety goals and backifitting and cost-benefit criteria will be used in order to determine how safe each plant is and which modifications could be warranted accordingly, if any.

PRA-Levels II and III analyses are perceived as a long term effort that will not be defined until the outcome of the severe accidents programs allows sound conclusions and guidelines.

We think that PSA and Safety Goals will be off course used to detect and correct potential vulnerabilities, if appropiate, according to cost-benefit criteria.

SAFETY OBJECTIVES
(continued)

(Session IV)

Chairmen

E. BECKJORD
United States of America

H.J. TEAGUE
United Kingdom

THE CASE FOR MORE STRINGENT SAFETY CRITERIA

J.F. AHEARNE
Sigma Xi,
New Haven, Connecticut,
United States of America

Abstract

More stringent safety criteria may be needed to guide design of advanced reactors, although the NRC safety goals provide an adequate design envelope, and INSAG-3 describes a suitable process. New designs do raise issues which go beyond current criteria, and may require additional criteria. A major question is when will a prototype be required. New criteria could be proposed to win public acceptance of nuclear power. Public acceptance will not be gained easily, and will require government and industry implementing new developments in risk communication.

---

1. INTRODUCTION

The safety criteria issue could be posed for at least three generations of nuclear installations:

(1) presently operating or under construction, i.e., the current generation, recognizing that the term "current' includes many types of reactors.

(2) so-called evolutionary designs, which are hoped to be the next reactors ordered. These plants are modifications of existing designs and, at least the vendors hope, are similar enough to current plants so that regulatory authorities will certify these plants, based on analysis and a minimum of experimental work, and will not require extensive experiments and certainly will not require prototype plants be built.

(3) advanced reactors, significantly different from current designs.

An entire paper could be devoted to the question of whether more stringent safety criteria should be applied to current generation plants. This subject includes, at least in the United States, the issues of backfitting and racheting. Because this conference is devoted to the future generations of plants, I will not discuss new criteria for current plants.

The separation betweeen evolutionary and advanced designs is not the "bright line" of legal definitions. The boundary is fuzzy. Consequently, some of my remarks will refer to advanced designs whose proponents may argue are not "advanced", but only "evolutionary".

Before addressing what new criteria might be required, I first would like to comment on whether the industry joins its critics in concluding that so far nuclear power has not been beneficial. The industry does not, and frequently argues that nuclear power is good. A few representative statements follow:

"The harnessing of nuclear energy for electricity generation has been a remarkable technological achievement and a major public service."[1]

"Worldwide, 414 plants are operating in 26 countries ...accounting for 16 % of the world's generating capacity. This tremendous block of power has been delivered, on the average, with greater safety, with less environmental impact, and at less cost than most other prevailing methods of generating base-load electricity."[2]

"Existing nuclear plants are safe, reliable, work-horses. In saying that we need to demonstrate the advanced nuclear technology that is now in hand, we are not saying tht [the] nation's choice of light-water reactors in the 1960's and 1970's was a bad choice. Every utility that has an operating nuclear reactor today is very, very glad to have it."[3]

I am confident similar statements can be found made by nuclear proponents in other countries. I have heard them from scientists, engineers, and utility executives from France, Japan, the FRG, the UK, Taiwan, and the Soviet Union.

Attribution of enthusiasm to owners of nuclear plants may be disputed by some U.S. owners, such as the Sacramento Municipal Utility District, owners of Rancho Seco, and Gulf States Utilities, owners of River Bend. However, the positive statements do raise the question: why should safety criteria be reexamined? Some people will answer: because of TMI, or, because of Chernobyl. True. However, safety criteria were revised after these accidents, although this meeting is not the place to review the many changes made as a result of lessons learned from the two tragedies. Those revisions primarily addressed current plants, and the revised criteria, regulations, and guidelines are now in place. (Of course, a separate issue is how well are these revisions being followed.)

I see two reasons why new safety criteria might be desirable for the next generation of plants:

(1) To guide, force, or constrain designers. For this purpose, new criteria could be more stringent than current criteria, or they could be less stringent.

(2) To help convince the public, legislators, and utility executives to introduce new plants.

In the following I will address the implications of these two possible motives.

2. CRITERIA FOR DESIGNERS

Although safety criteria are developed in many documents, two represent fundamentally different approaches. Each represents significant effort by knowledgable experts in the nuclear community, presents criteria which may significantly affect new designs, but approaches the establishment of criteria from what appear to me to be fundamentally different directions. The two documents are the U.S. Nuclear Regulatory Commission's Safety Goals [4] and the IAEA's "Basic Safety Principles for Nuclear Power Plants", INSAG-3 [5].

Development of the safety goals began with a comment by Prof. David Okrent, shortly after the TMI accident, who suggested that the NRC should have an overall safety goal for the plants regulated by the agency. The Commission asked Prof. Okrent to prepare a paper discussing this proposal, following which the agency commissioned additional studies, held workshops, and published draft proposals for public comment. The NRC published a final set of goals in 1986. The basic philosophy represented in the safety goals appears to be that nuclear plants should not pose a significant risk of cancer to those living near the plants, above the risk expected without a nuclear plant. The goals provide an envelope, within which all plants are to reside. Latent in the safety goals is the concept that these levels should be acceptable to the public, i.e., that plants meeting these goals will be unobjectionable. Of course, adequate safety goals and public acceptance of a plant are separate issues. The public may agree that a plant meeting the goals would be acceptable, and disagree with every attempt to show that a specific plant meets the goals. Nevertheless, the safety goal approach is an attempt to force designers and operators to insure plants fit within an envelope of adequate safety.

I am not going to review criticisms of the safety goals. For today's purposes, I only will note that the safety goals may be less constraining than a body of regulations, and can be viewed as not stringent at all, since today's plants are supposed to be within the envelope. However, the safety goals may be very restrictive: meeting the goals requires demonstrating through analysis and experiment that new designs stay within the safety envelope. Since such designs are new, and some are quite different than existing plants, readily available analysis and experimental results may be insufficient to show that the broad safety goal criteria will be met.

INSAG-3 has a different philosophy. It lays out standards of good practice for designers, constructors, and operators. Although the general nuclear safety objective is "[t]o protect individuals, society, and the environment...", the document is oriented more to the process than to the result. The INSAG-3 philosophy appears to be that if all the steps are done correctly, the product will be a safe plant. In fact, the INSAG overall objective is qualitatively similar to that of the Safety Goals: "When the objective is fulfilled, the level of risk due to nuclear power plants does not exceed that due to competing energy sources and is generally lower."

INSAG-3 contains several objectives which could affect the development of new generation reactors, if not the design:

(1) Defense in Depth: "To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment." However, several new designs hope to reduce costs or improve the perception of safety by eliminating some of the traditional barriers.

(2) General Technical Principles: "There are several underlying technical principles which are essential to the successful application of safety technology for nuclear power plants." The first is "Nuclear power technology is based on engineering practices which are proven by testing and experience, and which are reflected in approved codes and standards and other appropriately documented state-

ments." This principle can be met, with some effort, by the evolutionary plants. However, by their very nature, the advanced plants are not proven by testing and experience and, in some cases, operate in regions or with techniques that are not addressed by existing codes and standards. Development of applicable analyses, experiments, codes, and perhaps standards will take many years. But the designers need funding now, which may be difficult to obtain until funders have greater confidence the designs can meet safety criteria.

(3) Prototypes. INSAG-3 implies the need for prototypes of new designs: "The design and construction of new types of power plants are based as far as possible on experience from earlier operating plants or on the results of research programmes and the operation of prototypes of an adequate size." INSAG-3 specifies "...the general process of designing a nuclear plant to be safe..." The second of three principles is to use proven technology: "Technologies incorporated into design have been proven by experience and testing. Significant design features or new reactor types are introduced only after thorough research and prototype testing at the component, system or plant level, as appropriate." I expect many debates in the 1990's as to whether INSAG-3 requires an operating prototype of a new design before the regulatory bodies can approve the design, and before a utility will order such a plant.

3. GAIN PUBLIC ACCEPTANCE

Although I know it is controversial, initially I will separate countries into two categories:

(1) Countries with a solid technical base, many engineers, and a pool of educated, skilled people to build and operate nuclear plants.

(2) Countries without such a base, but which have a growing demand for electricity. You may question why a country without a broad technical base would need more electricity. Basically, I accept the arguments of Columbo and Starr that economic growth is strongly correlated with increasing use of electricity.

I further subdivide the first category:

(1a) Countries where there is little opposition to nuclear power. In the early 1980's, France, Japan, and the Soviet Union would be included, but this category now may be a null set. The opposition in Japan is growing rapidly, as can be seen by the formation of a political party called "People Who Don't Need Genpatsu [nuclear power plants]". [6] Following the Chernobyl accident, public concerns, coupled with the new openness and tentative democratization in the Soviet Union, have led to public opposition to new and existing nuclear stations. Even in France, where opposition has been quiet since the early 1970's, the director of the Paris office of an international environmental organization said "...[t]he stirring of protest against four proposed nuclear waste sites in France...is 'the first indication that some people have understood' the problem [of nuclear power]". [6]

(1b) Countries with substantial opposition, even if it is only local. To a large extent, local opposition characterizes the United States, as opposed to Sweden. However, although opposition may be local, it can strongly affect national legislation because, as Tip O'Neill, a long-time Speaker of the U.S. House of Representatives, noted, "all politics are local".

My purpose in dividing the world into these three categories is to address new safety criteria. For (1a), industrialized countries with little nuclear opposition, there will be no perceived need for new criteria. The dominant position will be that plants run well, are safe, and are accepted by the public. Consequently, current criteria are sufficient. Probably France comes closest to this position.

For (1b) and (2), new criteria may be perceived as needed, but for different reasons. In (1b), industrialized countries with nuclear opposition, some nuclear proponents will argue that new criteria are required to convince the public, utilities, and the government that new nuclear plants should be built. For these countries, new safety criteria may be necessary to lift nuclear power above a threshhold of objections. For countries in (2), new criteria are required to insure adequate safety. As stated in INSAG-3: "At the design stage, consideration is given to the needs and performance capabilities of the personnel who will eventually operate the plant...."

I conclude there are two different motives for looking into more stringent safety criteria for the next generation of nuclear power plants. It is important to recognize the difference, because it will make understandable the reaction by some in the industry to specific proposals. If the motivation is to make the next generation of plants more resistant to accidents and less of a hazard to the public, then new criteria will be established independent of the difficulty of compliance. On the other hand, if the motivation is to increase public acceptance, the focus will be on public perception and achievablity -- on what criteria will convince the public that new reactors are acceptable, while at the same time being cautious not to propose criteria which will be extremely difficult to meet. With regard to the last point, I would not be surprised to find advocates of one type of reactor arguing for a particular safety criterion which they know their design can meet but competing designs cannot .

The following is representative of the view that improved safety features are necessary to convince the public to accept additional nuclear power plants:

"Technical advocates of [certain types of passively safe] reactors believe that current reactors are safer than other methods to generate electricity; but safety per se is insufficient to insure expansion of the nuclear industry. A 'technical fix' is needed to solve economic and public acceptance issues associated with nuclear power. The use of passive and inherent safety systems rather than artificial intelligence, management changes, or other techniques to solve these problems is based on a particular set of viewpoints about public acceptance of nuclear power and the reliability of the plant operator." [7]

4. ISSUES FOR DESIGNERS

Even this category can be subdivided:

(1) new criteria that are required because new designs should be safer; and

(2) new criteria that are required because new designs pose issues not covered by current criteria.

The first category is related to, but not identical with, criteria to win public acceptance. Some advocates of nuclear power note that some characteristics of current generation LWRs stem from the rapid development of commercial nuclear power plants, and incorporate many features of fossil fuel plants, such as control room instrumentation. Criteria requiring status displays could require state-of-the-art technology, which most, if not all, current plants do not have. Other criteria could require walk-away or hands-off accident response capability, such as requiring that a reactor withstand a severe accident without operator intervention for at least 24 hours. Another criterion could be to ban positive void coefficients, or to require a complete, independent, second shut-down system.

Any detailed criterion should be based upon meeting an overall objective, such as the probability of fuel melt, the probability of release of an amount of radiaoctive materials greater than some threshhold, or the probability of an offsite dose of greater than some threshhold. Regulators will not license, and the public will not accept, plants tht do not have a sufficiently low probability of offsite release of large amounts of radioactive material. Utilities will not endorse plants which do not have a sufficiently low probability of fuel damage, and subsequent plant contamination and damage.

However, I do not perceive any new general criteria which are required for new plants because of generic design weaknesses in current plants. The U.S. safety goals are adequate for an envelope, and INSAG-3 provides sound guidance for the process. Specific designs may require additional criteria because new designs do raise new questions. A major question posed by new generation plants is whether existing criteria cover all features of the new designs. In a draft Safety Evaluation Report (SER), the U.S. NRC staff already has indicated present criteria are inadequate for the MHTGR: "...adequately developed criteria do not yet exist in a number of important areas and will have to be developed at a later design stage in order to support an actual application." [8] The following are some questions already raised by the new designs. More will arise as design work continues and additional designs are proposed.

(1) What should be the design basis accidents for passively safe plants?

(2) What criteria must be met to accept elimination of control rods, ECCS pumps, emergency diesels, containment, etc.? These questions have been posed already by design information. For example: "A gravity-driven ECCS system [in the AP-600], in-containment refueling water storage tank, and depressurization capability eliminates the need for a pumped ECCS system." [9] "The capability provided by passive safety features in the AP-600 and the SBWR plants can accomodate all design basis events, and

there is no need for a safety-grade emergency diesel generator...." [9] The U.S. NRC advanced reactor policy statement can be interpreted as encouraging new approaches to achieve safety: "...the Commission expects that advanced reactors will provide enhanced margins of safety and/or utilize simplified, inherent, passive or other innovative means to accomplish their safety functions." [10] The MHTGR design, containment in a pellet, proposes to eliminate the standard containment. In the draft SER, the NRC staff is skeptical of this proposal: "...the Commission will need thorough and detailed justification to support any design proposal that does not include a containment structure."

(3) What criteria should apply to integrated circuit control-by-wire systems?

(4) Should regulatory authorities license expert systems in a manner similar to licensing operators?

(5) For passively safe plants, should a license condition be that operators need not take action for "x" minutes? And how is "x" determined?

(6) What is required to eliminate some existing criteria and regulations? For example, what analyses and experiments would be necessary to eliminate the requirement for off-site emergency planning?

One example illustrates the problems advanced technology may introduce. Many of us have been critical of the obsolete technology represented in most reactor control rooms. Inspite of extensive industry and external criticism, most control rooms continue to resemble those of fossil plants rather than reflecting high technology. I recently visited the control room of a new U.S. plant, accompanied by a visitor from an Eastern European country. He looked around and commented that he was surprised to see such old technology.

There is movement towards incorporating modern control systems and human factor analysis into control rooms, although some so-called advanced designs still demonstrate too-close a link to steam-electric generation than to aerospace developments. However, designers and regulators must beware of removing the operator entirely, thereby returning to the pre-TMI belief that the machine is invulnerable. The aviation industry has pioneered commercial application of improved instrumentation and controls. Recently NASA published the results of a three-year study of pilots' reactions to the automated cockpit in one of the most modern commercial aircraft. The study indicated "disagreement [among the pilots] over whether automated cockpits actually reduce workload and whether they might cause some safety problems." [11] Two major concerns were identified. First, "[n]early half of the pilots were concerned about the possible loss of aviation skills with too much automation. About 90 % of the pilots said they hand-fly part of every trip to keep up their skill level." Second, if the automated systems requires, or permits, the operator to reprogram a set of procedures, then during some critical periods the reprogramming consumes too much attention. Such can occur during aircraft descent, when, according to a member of the Airline Pilots Association human performance committee, "the intellectual attention required by reprogramming makes it hard to do anything else."

You may question whether such automation will be part of proposed new reactor designs. I believe it will, in part to win acceptance from opposition groups. Such stimulation can be seen in the following comment on desirable features of future reactors, part of Congressional testimony given earlier this year by a senior representative of a U.S. environmental group:

"It is important to mention that successful demonstration of idiot-proof reactors is decades off, if it should prove possible at all." [12]

The more difficult issues relate to what level of analyses and experiments will be required to gain regulatory approval for the truly new ideas in some advanced designs. The PIUS is a good example. The PIUS reactor's safety is based on a new approach. Are new codes required to demonstrate acceptability? Will regulators insist on benchmarking such codes? Against what? Will a semi-scale facility be required? The designers claim a 7-day hands-off capability. Will regulators, or utility executives, require a demonstration? With irradiated fuel? Can such be done? Where?

As I indicated earlier, INSAG-3 can be read as strongly urging, if not requiring, a prototype for new designs. This may produce a dilemma, as seen in two recent events in the United States. Two U.S. utilities asked the NRC to review PIUS, stating PIUS would be one design, of many, the utilities would examine were they to order a nuclear plant. Shortly thereafter, the NRC Chairman commented that the NRC possibly may only review and certify designs if the NRC concludes U.S. utilities will order those designs. He suggested the NRC may use a requirement that a vendor have an order before the NRC will review the design. [13]

The prototype issue is probably the largest question facing industry on advanced reactors. The issue is how to convince the utilities and the regulators a protoype is not needed, or how to convince industry and government to fund a prototype. Perhaps some of this maneuvering can be seen in a 1986 report to the U.S. Secretary of Energy by a panel of the Energy Research Advisory Board (ERAB) commenting on a strategic plan for reactor development: "The Panel recommends the DOE concentrate its development efforts on two advanced-reactor systems: the liquid-metal reactor (LMR) and the high-temperature gas-cooled reactor (HTGR)." [14] Examining the leading passively safe reactor designs, the head of EPRI's nuclear program recently concluded that prototypes would not be necessary for licensing LWR designs, but would be necessary for both the LMR and the HTGR. [2] The NRC draft SER on the MHTGR concludes: "Final determination on the acceptability of the MHTGR stnadard design is contingent on....(4) successful... operation of a prototype reactor before design certification."

Finally, there are some aspects of the new designs which although not represented by proponents as requiring safety analysis may not be so kindly viewed by regulators. For example, as a former regulator my attention was caught by the following description by one of the vendors of a part of its new design:

"Economic operation of the plant depends greatly on the reliability of the steam generator.....Extraordinary care is required in the design, manufacture, and operation of the steam generators." [15]

5. PEOPLE

There is one area in which I believe additional and more stringent criteria should be developed: regarding the people who build, operate, and manage nuclear power plants. I will restrict these comments to the United States. I suspect the public in many countries may be concerned about this issue, but I do not have the information on which to base comments for other than the United States.

The greatest weakness in U.S. nuclear power has been some of the people involved in operating and managing commercial nuclear plants. In the 1970's and for much of the 1980's, the industry denied any weaknesses within its membership. That attitude has been changing, perhaps driven by the Institute for Nuclear Power Operations (INPO). It was not common for the U.S. NRC to criticize plant management. It was common for industry to reject any such NRC criticism, noting that the NRC was not competent to judge management and that the NRC had very few staff members who had ever operated a nuclear plant. However, INPO is composed of industry experts, people who have operated nuclear plants. Therefore, INPO's criticism is not easily dismissed, and INPO has been quite critical of some plant operations.

Last year Norman Rasmussen pointed out that for the U.S. nuclear industry to recover, it needs no more Peach Bottoms, no more Pilgrims, no more TVAs. In writing about what must be done to convince U.S. utilities to order nuclear plants, an industry group wrote: "The primary responsibility for achieving this rests with the industry itself." [1] One step U.S. utilities must take is to recognize nuclear power is not just another way to make steam. A senior executive of a U.S. nuclear utility wrote that what is required to rekindle utility interest in nucler power is "a fresh viewpoint on engineering for safety....We can start by giving a deeper recognition and acceptance to the fundamental differences between nuclear engineering and fossil engineering." [16] Nuclear engineers worry about new designs, and come to meetings such as this one, but fossil people still make many utility decisions about nuclear power.

The United Kingdom recently stresssed the importance of the operating staff: "The sum of these measures [to establish a 'safety culture'] is, and is intended to be, an atmosphere of rigour and strictness surrounding the daily operation of any nuclear plant. But such an approach at plant level will not be effective unless the organisation itself has a very high level of commitment to safety. In this the lead has to come from the very top, the Chairman and Board of the company. They must...ensure that their commitment permeates every level of the organisation...." [34] INSAG-3 also addresses this requirement, in the first principle under management responsibilities: "An established safety culture governs the actions and interactions of all individuals and orgainizations engaged in activities related to nuclear power." [17] Unfortunately, economics will intrude on any development of safety criteria, and economic pressures frequently will be oppose new safety criteria. I believe many U.S. state regulatory commissions, and some utility managers, do not understand that: "The bases for economic decisions in engineering a nuclear plant are vastly different from those applied to fossil plants. This has not been recognized widely, and the failure to do so has had a deleterious effect on overall safety." [16]

U.S. nuclear plants on average have not run well: "...the average capacity factor in the United States is about 60 %, compared to a range of 75 to 85 % in some countries. In addition, U.S. operations and maintenance costs are averaging roughly twice those of other countries." [2] Understanding operations would lead to increased emphasis on training, competence, and staffing. Ignorance would look to cut personnel costs. This lack of understnding can be seen in the requirements laid on by some utility senior managers to reduce operating staff and cut training budgets, often under the euphemistic label of "cost containment". The basic philosophy of such programs appears to be to see how close to the operating margin can a utility come; how much extra work will their best people absorb before quitting; how much training can be eliminated before maintenance and operating errors multiply. The lessons of TMI and Chernobyl have been forgotten by some utility executives, if the lessons were ever learned.

Hence, I advocate more stingent criteria on who manages and operates nuclear plants. I would restrict nuclear plant operation to utilities which can demonstrate a commitment to the safety culture; which are willing to invest in competent engineering staff, in extensive training, and retraining, for operators and maintenance staff; and which are run by people who understand nuclear power and are committed to safety.

6. PUBLIC ACCEPTANCE

I believe that much of the industry interest in discussing new safety criteria relates to the hope that meeting such criteria will win over a skeptical public. This hope has been rekindled by recent debates about the greenhouse effect, which is a significant new factor in disussions about the acceptability of nuclear power. [18] For example, the U.S. National Audubon Society in 1980 stated that its position was to " 'make the nuclear fission era as brief and as limited as possible.' Nevertheless, as a result of concern about climate disruption from fossil fuel carbon dioxide, National Audubon staff is undertaking a careful review of the nuclear option." [12] The Audubon Society notes, however, that "...safety and quality assurance problems...have caused the public to lose all faith in the technology." An Audubon scientist recently described what he believes should be the design goals for reactors, if the objective is to change the public's position:

"1) Reactor cores that will neither melt nor catch fire upon any conceivable operator action or sabotage, including abandonment of the site....

2) Reactors that are safe from catastrophic airborne releases following attack with explosives by sub-terrorist groups...

3) Reactors that are safe from catastrophic airborne releases following earthquakes...." [12]

However, the Audubon scientist noted "the low probability that any kind of nuclear option will prove both economically viable and sufficiently idiot-proof to overcome public concern about the safety of the nuclear fuel cycle."

He concluded "Is there any realistic role for nuclear power in preventing climate disruption? Not likely, in Audubon's opinion."

Not only environmental groups have identified public mistrust of things nuclear. A U.S. utility executive wrote:

"Many persons in the nuclear industry feel that our problem is primarily the fault of the public, or the media, or the schools, or the anti-nukes. But if we step back one pace, and are honest with ourselves, we must agree that in a broad sense the public's distrust has its foundations. We said we were designing and building plants in which a core meltdown was essentially impossible -- and then came TMI-2. We then argued we could have meltdowns but not energetic reactivity accidents -- and then came Chernobyl. We argued that we might contaminate a power plant but not a neighborhood -- and now reindeer in Lapland and lambs in Wales are part of the nuclear debate. The public -- our public -- citizens, media, public utility commissions -- come away doubtful and with a feeling of having been misled." [16] This executive believes "the public's antipathy to nuclear energy will change only when it is convinced that nuclear safety is genuinely and visibly improved from what it presently believes it to be."

Many suggestions have been made on how to convince the public. The U.S.DOE Energy Research Advisory Board endorsed two initiatives:

(1) informing the public about the advantages and the problems of nuclear power, and

(2) "a credible nationwide radiation-monitoring program that keeps the citizenry apprised at all times of the extent of its exposure." [14]

The purpose of the monitoring system appears to be to convince the public that normal operation of plants produces much less of a dose than does exposure to normal background. This recommendation appears to be based on countering claims of large, hidden releases from operating plants. However, there may be a weakness in this recommendation. A trade journal recently reviewed international public attitudes about nuclear power, and noted:

"One article of faith embedded in the industry's collective consciousness is that public trust will be gained by safe efficient, operation of nuclear plants. So far, there's little indication that's necessarily true."

The article cites Switzerland, Sweden, and Finland as examples. [6]

Before embarking on a new federally funded development program, the U.S. Congress would like to be confident any new reactor would get the acceptance of federal and state government, vendors, regulators, the financial commmunity, and the environmentalists. [3] I believe the industry may be mistaken in its approach to gaining public acceptance. I believe three conditions must be met, and then a different approach taken.

The three conditions are the following:

(1) electricity demand must continue at a rate requiring new capacity. Energy conservation, wheeling, import of power must not be sufficient. The public must agree new capacity is needed, and fossil fuels must be seen as unacceptable or, at least, undesirable.

(2) Operating nuclear plants must run well -- both safely and economically. I believe this will require replacing some managers, and even closing some plants.

(3) new designs must be convincingly less difficult to operate, more resistent to accident, and more certain in costs -- which must be competitive.

These steps alone will not restore public acceptance of nuclear power, but they are necessry. The government and the industry also must learn how to communicate with the public. A major step would be to incorporate new developments in risk communication. These developments can be summarized as follows [19] [20]:

(1) Many disputes are about values, not facts. The public and the government or industry often disagree on the distribution of risk and benefits, about the claimed similarity of voluntary and involuntary hazards, and about which harms are most worth avoiding or which benefits are most worth seeking.

(2) Effective risk communication is two-way: the agency or industry must learn what issues are troubling the local community or the affected groups. Dialogue, including real listening, is necessary.

(3) Risk communication is successful when interested parties are adequately informed.

(4) Poor risk communication nearly always will make a situation worse. However, improved risk communication may not reduce conflict, because people do not all share common interests and values. Therefore, better understanding may not lead all people to the same conclusion.

(5) Credibility is easily lost. To retain credibility requires competence and honesty.

7. SUMMARY

Are more stringent criteria needed?

First, current criteria should be applied conscientiously.

Second, some management should be replaced -- if to do so requires new criteria, new criteria should be developed.

Third, for new designs, new criteria will be necessary to handle new issues.

Fourth, new criteria will be necessary if nuclear power spreads beyond industrialized countries.

Finally, new criteria will not alone restore public acceptance of nuclear power.

REFERENCES

[1] Nuclear Energy for the Future...What we must do, Nuclear Power Oversight Committee, USCEA, Washington, DC (1989).

[2] TAYLOR, J.J., Improved and safer nuclear power Science 244 (1989) 318-325.

[3] JOHNSTON, SEN. J.B., The Nuclear Agenda:1989, Nuclear Power Assembly, Washington, DC (1989)

[4] Safety Goals for the Operations of Nuclear Power Plants: Policy Statement, U.S. Nuclear Regulatory Commission, Washington, DC (1986).

[5] Basic Safety Principles for Nuclear Power Plants, Safety Series No.75-INSAG-3, IAEA, Vienna (1988).

[6] Outlook on public acceptance Nucleonics Week 30 26 (1989) 1-18.

[7] FORSBERG, C.W., New Developments in Reactor Design, Oak Ridge Natl Lab., TN (1989).

[8] WILLIAMS, P.M., KING, T.L., WILSON, J.N., Draft Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor, Rep. NUREG-1338, U.S. Nuclear Reg. Comm., Washington, DC (1989).

[9] STAHLKOPF, K.E., DEVINE, J.C., JR., Passive Reactor Development in the United States, Canadian Nuclear Assoc. Intl Conf., Ottawa (1989).

[10] Regulation of Advanced Nuclear Power Plants; Statement of Policy, U.S. Nuclear Reg. Comm., Washington, DC (1986).

[11] HUGHES, D., Glass cockpit study reveals human factors problems, Aviation Week & Space Technology 131 6 (1989) 31-35.

[12] BEYEA, J., Is There any Role for Nuclear Power in Preventing Climate Disruption?, U.S. House Subcommittee on Energy and Power, Washington, DC (1989).

[13] WEAVER, D., Carr says NSSS vendors could need order in hand to get NRC review Nucleonics Wk 30 32 (1989) 1-12.

[14] Review of the Proposed Strategic National Plan for Civilian Nuclear Reactor Development, DOE/S-0051, Washington, DC (1986).

[15] BERGLUND, R.C., TIPPETS, F.E., Prism, the Plant Design Concept for the U.S. Advanced Liquid Metal Reactor Program, GE Nuclear Energy Division, San Jose, CA (1987).

[16] KINTNER, E.E., Rethinking Next Generation of Nuclear Power Plants, ANS Meeting on Safety of Next Generation of Power Reactors, Washington, DC (1989).

[17] The tolerability of risk from nuclear power stations, Health and Safety Executive, London (1987).

[18] AHEARNE, J.F., Will Nuclear Power Recover in a Greenhouse?, Rep. ENR89-06, Resources for the Future, Washington, DC (1989).

[19] AHEARNE, J.F., Risk Communication, Colloquia, Los Alamos Natl Lab., NM (1989).

[20] Improving Risk Communication, Natl Academy Press, Washington, DC (1989).

ONE UTILITY'S POINT OF VIEW

R. CARLE
Electricité de France,
Paris, France

Abstract

A utility operating a nuclear plant is legally responsible for the safety of this plant. The safety strongly depends on the quality of operation.

The safety of the existing plants is good but can be improved. To achieve this goal we must take benefit of the experience feedback, the probabilistic reliability analysis and the modern methods of operators training.

International exchange of informations, for example in the framework of IAEA or WANO, improves the number of data available and is of utmost importance.

At the beginning of next century we shall have to choose the plants which will replace the existing ones at the end of their life. To prepare this decision we must keep in mind :

- the interest of using existing experience,
- the importance of keeping a good balance between automatic systems and human action,
- the progress which could be made by using passive systems.

But we should be careful not to discredit current technology by the hope of so called inherently safe reactors, which will never exist.

Choosing small-sized reactors could have some advantages but would increase the cost ; in fact, size is strongly dependent on the clients needs.

Only a limited number of standardized systems should be developed in the future.

Finally, quality of these systems will be the key to achieve better safety, in the continuity of the past achievements.

In every country in the world, a plant operator is legally responsible for that plant. This basic principle, of course, also applies to nuclear installations. However, whereas this responsibility is clearly defined and accepted, the operating organization cannot decide by itself which level of safety should be achieved. Worldwide, this level is defined by public authorities, who are not directly involved in operating results, thereby guaranteeing that public safety, public interest, will be taken into account. But this does not mean that there is no dialogue between the parties involved. The operator must provide input, not only in his own interest, but also in everyone's interest.

We cannot ensure safety if it remains nothing but a set of abstract rules imposed from the outside. It is the task of public authorities to set goals ; and it is the operator's task to define and implement the practical methods to attain these goals. The public authorities must then monitor operating quality, and the operator has to point out everything that may help improve safety. The daily life of the operator is full of lessons ; and it is his duty to learn from these lessons. In other words, we are living in the era of experience feedback.

SAFETY LEVELS - SATISFACTORY BUT STILL PERFECTIBLE

The main results of our operating experience concern the safety level reached by our reactors. As of the beginning of 1989, the cumulative operating experience logged by pressurized water reactors totalled 1,417 years of operation, including nearly 300 in France. From the startup of Shippingport in 1957, this type of reactor has been operating for over 30 years worldwide. The basic principles behind the design and development of safety arrangements over these years have shown that they are solidly grounded.

Of course, the TMI accident in 1979 immediately led to a safety reevaluation of our projects. This reevaluation did not call into question the basic concepts of our safety approach. Indeed, it is reassuring that this type of accident, involving a significant core meltdown and a temporary break in the reactor coolant system, did not lead to any significant outside release of radioactivity. The true usefulness of the containment building, as well as other safety arrangements, was amply demonstrated ; Chernobyl, on the contrary, highlighted the catastrophic consequences of the absence of containment.

I do not have to remind you of the resulting modifications, including control room design changes and operator-aid systems. This accident underscored the importance of so-called "precursor" incidents, which allow us to forecast the occurence of more serious situations if these incidents are taken into account and brought to our attention in time.

Significant incidents are systematically counted and reported to the Safety Authorities. The most important of these incidents are extensively examined. For this, nothing can replace the cumulative experience of many years of operations. Our data banks have collected over 30,000 such events. Due to this relatively large number, we have had to institute a system of ranking accident seriousness. We must avoid an erroneous data interpretation on the part of the media leading the public to believe that everything is wrong with our reactors. Therefore, starting in April 1988, we defined a severity scale for incidents and accidents. The application of this scale over the last eight months of 1988 showed that most of the 323 incidents declared to the French Safety Authorities were not important enough to fall within the scale ; only 45 could be classified as Category 1, which covers operating anomalies ; two incidents were classed as Category 2, involving incidents likely to lead to later developments, and there were none in the four most serious categories :

- Category 3 : incident reducing significantly the plant level of safety or incident releasing limited quantities of radioactive material, equivalent to 10 % of the authorized annual limit ;
- Category 4 : minor accident leading to releases equal to the annual limit ;
- Category 5 : accident presenting off-site risks (e.g., Windscale or TMI) ;
- Category 6 : major accident, such as Chernobyl.

The safety of our reactors is not a frozen quality, and various features can still be improved. Exploiting data on these incidents, as well as observations on the equipment used, can lead to modifications of equipment or installations. Based on experience feedback, one methode is to undertake a probabilistic reliability analysis. In most cases, the results of this type of study overlap the conclusions of user common sense : a simple installation is better than an overly complicated installation.

Experience feedback also concerns human behavior and the role played by human factors in incidents. Some of the most noteworthy actions we have implemented include ongoing, advanced training programs for line staff. Simulator-based training is systematically used to confront operators with extraordinary situations which they would probably not encounter in a real power plant environment. Indeed, their day-to-day experience is relatively unhelpful because nothing particularly noteworthy tends to happen in the control room. An evaluation of these training sessions and certain incidents shows that we need as much rigor as possible in our written procedures. And it also points out the great need for operator-aid systems in case of accident. This was one of the great lessons of TMI, and the design of our new control rooms as well as modifications to existing control rooms were carried out with this in mind.

Our cumulative experience and safety analyses have clearly shown that the risk of a serious accident does not come from extreme design parameter conditions. In other words, we have much less to fear from a sudden break in a primary system pipe than a chain of isolated, minor incidents leading to a break in the primary coolant circuit, as was the case in TMI.

This reasoning is one of the primary factors behind our interest in the study of precursor incidents, and the importance we attach to collecting the widest range of experience possible. The IAEA and the NEA are working in this direction. At this point, I would like to emphasize the long-standing close collaboration between E.d.F. and INPO, as well as with the World Association of Nuclear Operators (WANO), presided by Lord MARSHALL, CEGB Chairman. WANO's main priority is to implement an information exchange system, based on the event notification report (ENR) and the event analysis report (EAR). WANO expects to receive from 0.5 to 0.75 ENR/EARs per year and per plant, which more or less corresponds to Category 1 events on our severity scale. There may be more EARs than the in-depth analyses carried out under the aegis of the OECD. This synergy is a fair reflection of the advantages of international cooperation and the sharing of resources and experience.

WANO will also be in charge of organizing a program involving the exchange of good operating practices, based on on-site visits : small international teams will carry out technical enquiries on a special subject in a given power plant. We have great expectations for the confrontation and cross-fertilization between the points of view of different operators. This idea has already been implemented by international experts within the scope of the IAEA's OSART program (Operational Safety Review Team) ; this international agency has already published international safety standards, including operation, in the NUSS programme.

As you can see here, current safety levels, although very satisfactory, can still be improved and we are already working on it. The most widely used reactors are obviously the most likely candidates for information exchange based on the specific points shared by these reactors.

CHOOSING THE NEXT TYPE OF REACTOR - SAFETY OF FUTURE REACTORS

Today in France, we have 52 reactors in service and 6 under construction. A few more should be added to this total in the coming years. Most of these units are relatively young and will not be replaced for many years. This situation applies to most countries worldwide. With few exceptions, such as perhaps in Japan, the current batch of reactors will grow through the completion of reactors under construction rather than building new units. We will not really be confronted with the problem of replacing these reactors for another ten years or so. During this time, we'll have to do some serious thinking. In my opinion, several important points should guide our thinking.

First point : we do not have to start all over again with a clean slate. Some of us - longer in the beard than others - may remember what Admiral RICKOVER wrote in 1963 concerning the difference between the reactors of the time - costly, long to build and experiencing operating incidents - and the reactors then on the drawing board, which were to be inexpensive, easy to operate, safe and offering all the advantages anyone could want except one - they did not exist ! It would be absurd to make a clean sweep of our experience on the proven types of reactors just because we are well aware of their weaknesses or inconveniences. Given the many possible combinations of fuels, cooling fluids and moderators, it is obvious that only the most promising possibilities were explored and that many others remained. But should we develop new type of reactors and reinitiate research into the previously abandoned paths ? To develop these other type of reactors and demonstrate their operating feasibility would be extremely expensive in terms of both time and money, if we want to attain a degree of knowledge similar to our current reactors. Let me ask just one question straight from the shoulder : who is going to pay for this ? And I would like to give at least a partial answer : certainly not the utilities ! We should stop dreaming, stop chasing these exorbitantly expensive fancies. In other words, let's take advantage of our own experience, and not start on adventures which in the long run will improve neither safety nor our financial position.

Second point : We should not, taking safety as a pretext, aim at eliminating operator intervention and replacing him by automatic control circuits. Nor should we ask our staff to be supermen and superwomen. We have to know how to choose the right balance of human intervention in the whole system. Under accident conditions, automatic control circuits are required in the initial phase ; they allow the operators the time required to analyse the situation and determine the best operating procedures to follow - those that will minimize consequences to the environment and installation. The accident management procedures developed for these extraordinary circumstances are designed to help the operator and provide him with certain guidelines. But it is at this point that man becomes irreplaceable. No electronic or artificial intelligence system has as many resources as the human brain, especially when the analysis is carried out simultaneously by several expert groups at the disposition of the managers.

<u>Third point</u> : Beware of the utopia of a "riskless" power plant. Given the very nature of the nuclear reaction, this type of installation cannot exist. There will always be a risk, although low, of radioactive fission products being diffused in the environment. We have reduced this risk to very low levels in our reactors, and we can reduce this even more. But we must not allow the public to believe that the proverbial riskless reactor is actually possible. And we have to be careful about presenting so-called "100%safe" (inherently-safe) reactors, because an in-depth examination of these reactors would show that there are always certain residual risks, even though it may be very low. And if this comes to pass, we will have discredited the existing installations, without having convinced public opinion of a totally safe nuclear future ; and, I hasten to add, without having improved safety to any real degree. The operator cannot be satisfied with totally passive systems ; for instance, to take an extreme case, operating a sealed, inaccessible reactor. In this case, the operator would have to remain passive in case of accident and, under the pretext of total safety, would stand-by powerless, as the whole plant was destroyed. The operator must be able to react and must have the means to react. Our reactors' control systems can be replaced in large part by automatic control systems. But as a last resort, they have to provide for priority given to manual intervention in those situations which do not follow expected scenarios. In this case, other procedures, such as the symptom-based procedures will guide the operator.

However, do not conclude from my remarks that there is no progress to be made. A very inert reactor will more easily forgive an error or a cooling or reactivity incident. For this latter type of event, negative feedback on the temperature and power levels will play a primary role. We have known this for some time. In terms of the removal of residual power, the reactor's thermal inertia is an important safety factor. Take sodium pool reactors, for instance ; in the case of a loss of coolant accident, the thermal inertia of the sodium coolant system offers a buffer zone of several hours to return the situation to normal. Last point : How big should we make the reactors of the future ? It is obviously to our advantage to keep them reasonably sized. Today's plants have proven their worth. They have remained on a human scale, and their size is well adapted to that of our grids. Smaller units, on the other hand, would be relatively more expensive. But they would be better adapted to lower-level needs and, to a certain extent, it would be more convenient to spread them out in time, by splitting commitments, and in space, as well as easier to locate them closer to the consumer. In terms of removing residual power, a "small" reactor definitely has passive cooling capabilities not enjoyed by a larger reactor. The thermal capacities of the containment and structures are larger in relation to the amount of energy to be evacuated. This is obviously a step in the right direction.

However, when we increase the number of reactors, we also increase the possibilities of staff or equipment-caused failures. We will have to conduct a detailed analysis of the situation before deciding whether we should change our policy in this field. And the conclusion is even less obvious, since our current generation of reactors draws on a long history of operations, contrary to the reactors to be built.

PREREQUISITES FOR SUCCESS

Be that as it may, we have to limite ourselves to a very small number of models based on well-established technology. We have to take maximum advantage of our accumulated experience, only adopting a new component after validating it by a qualification testing process which is long enough to be significant. Fuel elements, for example, can still be improved. But we must not scatter our efforts ; for each type of reactor we should limit the number of variants to be introduced. Standardization has been one of the keys to the success of the French nuclear program. This key strategy should be adopted everywhere ; not only does it produce savings, but it is the main guarantee of nuclear safety. All our resources can be concentrated with this in mind. For example, take the construction of high-performance simulators ; thanks to the standardization policy, all lessons learned from experience can be shared and easily transposed, whether we are considering precursor events and their analysis, human and equipment behavior, or procedures under severe accident conditions.

Should we go even further in this respect and unify our safety doctrines and practices ? Basic principles have been the same everywhere for quite some time. No major idea has appeared in a nuclear operating country without being analyzed and often taken into account in the other nuclear countries. There is of course a certain amount of diversity, based on local conditions, laws and traditions. But all in all, our doctrines are already coherent. An agency like the IAEA has done quite a bit to establish a minimum degree of coherence. Its actions have remained flexible in order to maintain efficiency, and we must continue along this path. Public opinion demands it. And this opinion is right to demand a coherent quality and safety level from our installations. In the western world, we have actually reached this level of coherence for quite some time now ; this has been proven to the safety experts through all the comparative studies we have carried out, through the safety reviews comparing one type of power plant to another, a German plant to a French plant, or even submitting the Superphenix fast breeder reactor to the NRC safety criteria. Unfortunately the varying ways of setting out the legal requirements allows the public to believe that there are differences in safety approaches. I believe that there are actually very few real obstacles in this field, and it is only up to us to overcome these and make clearly visible for the public and the politiciens our basic consensus.

International cooperation is implied in the very nature of nuclear energy. Since the very beginning, or at least since Geneva and Atoms for Peace, the civil nuclear power sector is truly inernational. Neither public opinion nor accidents are restricted by borders. The problems of nuclear power have been resolved in common by various countries. The problems still posed today require the same type of cooperation, and the same sharing of intellectual and financial resources, resources which are very finite and most effective when used in common and not in competition. It is our mutual challenge to reconquer the public's confidence, severely rattled since Chernobyl, and this is a challenge we will meet together.

CONCLUSION

The nuclear world of tomorrow will not be the same as that of yesterday. It will be even safer, simpler and more standardized, less costly in terms of investment and time, and it will offer advantages over its rivals in terms of supplying basic electrical needs. Solidly based on experience, it will not require changing our current technology. I would even venture to say that it requires absolutely no radical change, nor does it call into question any of the fundamental solutions which have already proved their worth.

The path to progress is lined with increasing concern for quality - fuel quality, equipment quality, procedural quality and human quality.

The path to progress implies rigor in our daily lives, without sterile formalism, and fully conscious of our many responsabilities.

This requires the ongoing testing of our plants' states and operations ; and it means faultless monitoring of the environment and releases. Globally, it means being a "model" industry, like the aerospace industry and like all industries which want to survive into the 21st century.

The path to progress also lies in an opening to the world, i.e., intensifying our exchanges of experience and comparing our points of view, so we can take advantage of constructive criticism. Beyond even the current trend, this means practicing total transparency, a transparency which provides both media and public with the elements to place the operation of our nuclear reactors into perspective and fairly evaluate the advantages as well as the disadvantages.

We have embarked on this path with confidence, in an ongoing movement which now comprises current reactors and which will continue with the reactors of tomorrow in developing this still-young technology.

PANEL PRESENTATIONS

SAFETY OBJECTIVES FOR LARGE-SCALE DEPLOYMENT OF NUCLEAR POWER

H.J. SCHENK
Kernkraftwerk Philippsburg GbmH,
Philippsburg,
Federal Republic of Germany

1. The Present Situation

I like to start with a short remark on the present situation. Most of the operating experience has been gained with light water reactors (260000 MWe net, 229 PWR, 87 BWR, in total about 5000 operating years). It has been proved, that such plants can be operated in a safe and reliable manner; in most of the cases they are economicaly competative.

At present our plants are licenced and operated on the basis of their proven quality to prevent accidents and on their capability to cope with design accidents. Quality assurance, automatic safety actions, well trained operators and an appropriate industrial infrastructure are the main tools to achieve this goal.

The possibility to cope with accidents beyond the design limits by effectiv accident management procedures was introduced some years ago and will be developed further more in the future. This enables the operator to cope with core melt scenarious identified by an probabilistic risk analysis or at least mitigate very unprobable and unforeseen accidents mainly by manual actions.

Accident management procedures enables us to stop very unprobable core melt scenarious early enough to avoid or to limit damages to the plant itself and to protect the surroundings.

I think, these are good conditions for a large scale deployment of nuclear power.

2. Some Safety Objective-Goals for Large Scale Deployment

If a substantial amount of the world's energy needs should be covered by nuclear power, the number of nuclear power stations would have to be increased by a factor of about 10. They will be operated in many different countries and have to be accepted by many different societies.
Therefore, nuclear power plants should be designed and operated worldwide in a way, that neither design accidents nor accidents beyond the design limits cause unacceptable risks to the people and the surroundings. This safety objective is rather strict, because - most probably - the potential of the environmental impact has to be minimized even more in the future in order to get this technology politicaly accepted. Therefore the continuity in the development of reactor systems should be maintained in order to minimize the risks involved and to be successful in large scale deployment.

The present LWR-types and our HTR-concept for example, have still a large potential for further development; the same can be said for the fast breeder. Here I like to mention some important areas for such developments (Fig. 1):

If nuclear power should be used on a large scale worldwide, on the first hand a capable industrial infrastructure related to the different groups of nuclear plants is needed in order to design, to build and to maintain the plants in a safe and reliable manner.

Second, the utilization of fuel should be improved as far as possible. An effective and economical usage of the uranium reserves and a reduction of nuclear waste would be one result.

The third area is the consequent confinement and the safe final storage of nuclear waste. Public acceptance is needed in this areas too.

safety objectives should be achieved by:

- continuity in the development of successful designs
- capable industrial infrastructures
- fuel integrity up to a very high burn up
- consequent confinement of radioaktive waste, safe final storage
- possibility to exclude severe accidents for the environment based on design features and a reasonable accident management

FIG. 1. Large scale deployment of nuclear power.

A further most important area is the continuous improvement of safety features to protect the people and the environment by avoidance or at least by an acceptable mitigation of severe core melt accidents. In Fig. 2 several general design features are mentioned, most of them are already considered in many plants, but they are certainly important to meet the safety requirements for a large group of reactors and should be further developed:

A conservative and failure tolerant design with as many passive safety features as reasonable is the fundamental requirement to achieve the safety objectives mentioned. We need in safety relevant areas a "General Basis Safety" design and construction. In Fig. 3 several such design features are enlisted. Important examples are:
- an optimal choice of the capacity of a single nuclear unit, considering the requirements discussed here;
- measures to limit human errors and
- last not least a design assuring a safe plant reaction in a loss of power situation.

Avoidance and Mitigation of Severe Accidents by

- conservative and failure tolerant designs with as many passive safety features as reasonable
- strong and reliable containment
- reliable emergency heat removal
- reliable emergency power supply and independance of the shut down plant from external energy supply
- reliable and simple safety related man-machine-interface, under "loss of power" conditions also
- reliable fast depressurization of the reactor system
- quality assurance for the plant, its operation and maintenance

FIG. 2. Avoidance and mitigation of severe accidents.

- fail-safe-designs, inherent and passive safety
- broad tolerance bands for operational values
- effective protecting devices for components
- data processing to enable fast reliable diagnoses
- limit human errors by design measures
- safe plant reaction to loss of power
- possibility to repair or exchange components

FIG. 3. Examples of failure tolerant features.

The most important role as last barrier in the defence in depth concept has the containment. It has to protect the environment in case of accidents which could not be excluded by the laws of nature or their extreme low probability ($< 10^{-7}$). Therefore it must be possible to exclude an open or a destroyed containment.

In order to maintain the containment function, a reliable emergency heat removal even without external energy supply should be available over the necessary time period.

It should be possible to exclude a total station black out because of its extrem low probability. Therefore a reliable emergency power supply over the necessary time is a main requirement. I think it is desirable, that

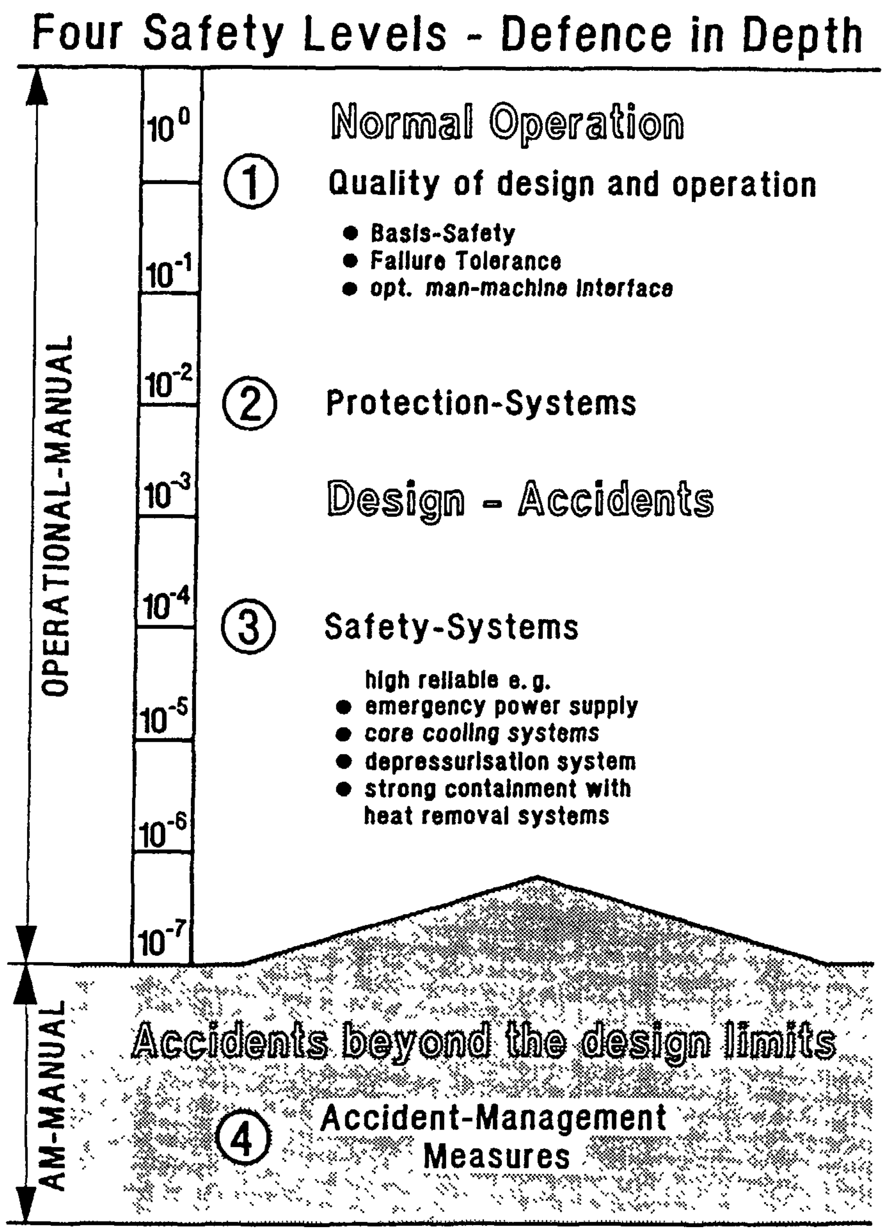


FIG. 4. Safety structure goals.

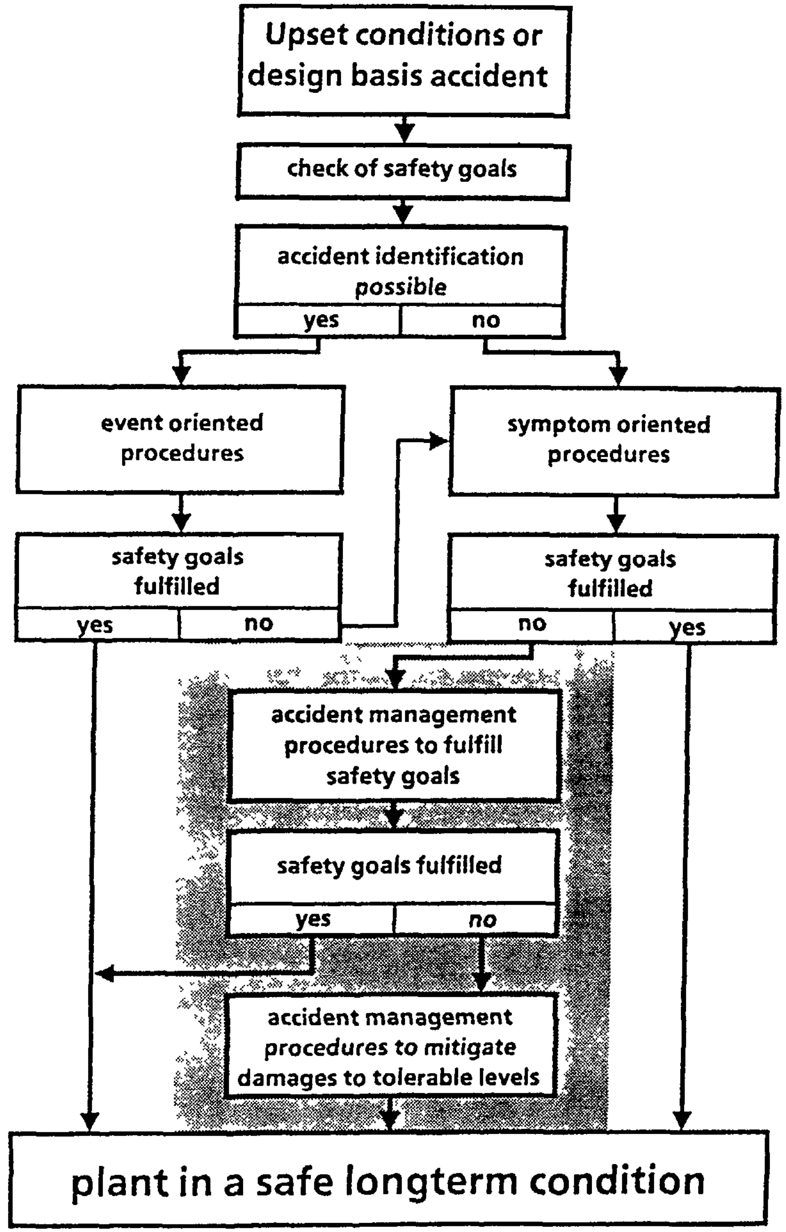


FIG. 5. KKP emergency procedure guidelines.

the "shut down plant" should be independent from external energy supply and - after some time - independent from operators too. In addition the loss of power shouldn't cause an unsafe disturbance of the manmachine-interface, e.g. faulty signals and unwanted reactions of plant components should be avoided.

In case of an accident situation (beyond the design limits), characterized by a reactor-system under high pressure without normal heat removal possibilities, the fast depressurization of the system should be possible in a reliable manner. It should be possible to exclude high pressure core melt down scenarious and to avoid or stop a "low pressure core melt down" by using at least one of several low pressure cooling possibilities.

Besides the design features mentioned already, quality assurance in the operation and maintenance of the plant is an essential part for its safety. Qualified reliable operators, an effective independant controlling organization and a capable industrial infrastructure are necessary preconditions for the safe operation of such plants.

It seems to me, that such safety objectives can be achieved and the mentioned design features (Fig. 4 and 5) can be realized, for example with LWR's, HTR's and fast breeders, in an economical competitive manner, last not least by reasonable standardization.

SAFETY OBJECTIVES FOR LARGE-SCALE DEPLOYMENT OF NUCLEAR POWER

K. SATO
Tokai Research Establishment,
Japan Atomic Energy Research Institute,
Tokai-mura, Naka-gun, Ibaraki-ken,
Japan

While the greenhouse effect and other environmental issues urges us to re-evaluate the roles of nuclear power, the basic incentives for nuclear option may not be exactly the same in each country depending on the energy situation and policy. For example in Japan, this is primarily due to the fact that Japan has virtually no domestic energy resources, thus from the energy security point of view it is a prerequisite to diversify energy sources one of which is nuclear energy. To this end it is our fundamental strategy starting from LWRs to proceed LMFBR so that dependency of nuclear fuel materials on foreign countries could be reduced.

Situation may be different in some countries where ample energy resources are domestically available. Thus, technical requirements, development schedule etc., may be different in individual countries.

Nevertheless, I believe that the basic safety objectives should be common worldwide. We should be well aware of the international nature of nuclear safety. Needless to say if we have another Chernobyl, or even TMI, anywhere in the world, further development of, or even maintaining current, nuclear energy will surely be seriously impeded. Therefore, the level of safety of any nuclear installations must be sufficiently high without exceptions all over the world.

In 1988, INSAG of the IAEA published "Basic Safety Principles", in which the safety objectives are clearly defined. As far as I could see, there is no reason that these objectives become irrelevant in next generation nuclear facilities. However, if the scale of the future deployment becomes significantly large, one should bear the following in mind.

One of the key factors of a large scale deployment is the public acceptance. There might be some controversy as to whether the safety level achieved by the existing nuclear plant operation is sufficiently high worldwide. Many experts may agree that current safety level is high enough, but there is some doubt if also the public is so convinced. The public perception on nuclear safety may not readily be improved even if we show them some beautifully worded safety objectives. Rather, it is first necessary to actually demonstrate that nuclear plants could be operated safely and reliably. Thus, for the next generation, it is a prerequisite to show an excellent performance today.

Furthermore, it is obvious from the technical point of view that if we have more reactors of same safety level, then the probability of serious accidents will increase proportionally to the number of reactors. On the other hand the public would not be so generous to allow a higher accident frequency even if the number of reactors is increased. This means that if we want a larger scale of deployment than before, the safety level of individual plants must become higher.

Such a higher safety level may not be realized only by more stringent criteria and regulation. In addition to them, I would like to stress the need for the "safety culture" that have been expressed in the "Basic Safety Principles" should prevail all over the world.

SOME FUTURE DEVELOPMENTS IN SAFETY OBJECTIVES

J. HANNAFORD
Health and Safety Executive,
H.M. Nuclear Installations Inspectorate,
Bootle, Merseyside,
United Kingdom

1. INTRODUCTION

The Nuclear Installations Inspectorate (NII) is a division of the Health and Safety Executive (HSE), a body which has among its various responsibilities the statutory power to grant licences for civil nuclear installations in the UK. Those installations include nuclear power stations, research reactors, fuel manufacturing and reprocessing plants and a disposal site for low level radioactive waste. The installations must satisfy the NII in a regime of assessment and inspection through all stages of their lives, from design through to decommissioning. Any statement of safety objectives for the future must derive, therefore, from a position where the NII's safety requirements are laid down in its safety assessment principles (SAPs) [1, 2] and in conditions attached to the nuclear site licences, and where existing installations are judged satisfactory when measured against those requirements.

Of course, no set of requirements is immutable and both the SAPs and site licences are being reviewed at the present time. Any changes to the SAPs, however, will be mainly aimed at making them more understandable, though the aim of this paper will be to discuss some ways in which regulatory objectives and the emphasis placed on them are likely to change in the future. The UK is currently building the first of four proposed PWRs and so those plants have figured strongly in our thinking and in the discussion on objectives below. Before going on to that, however, it may be helpful to point to the part played by the public in bringing about these changes.

2. PUBLIC INQUIRIES

Public opinion is a powerful force affecting change in the UK. It may be manifested through the media, through petitions and demonstrations and, more formally, through public inquiries into proposals to build houses, roads, factories or other new installations. The extent of the involvement of public inquiries in proposals to build nuclear installations has grown over the last ten years. The UK is currently involved in its second major inquiry into pressurised water reactors and sandwiched between them was a shorter inquiry into a proposed fuel reprocessing plant. Public inquiries might be expected, therefore, to be a major influence on any future large-scale deployment of nuclear plants.

As the licensing body, the NII participates in these public inquiries. Participation is a two way process: the NII gives evidence about the safety of the plant and it listens to and learns from views expressed by other witnesses. Each inquiry is followed by a report making recommendations to Government in relation to the proposal and often to other bodies involved, like the NII, when they are likely to impinge upon safety policy and objectives.

3. TOLERABILITY OF RISK

Sir Frank Layfield, the Inspector who presided over the inquiry into the proposed PWR at Sizewell 'B', made various recommendations in his inquiry report [3]. One of these asked the HSE to formulate guidance on the tolerable levels of individual and social (societal) risk to workers and the public from nuclear power stations and to initiate public and parliamentary discussion on this subject. The HSE responded to this request in its tolerability of risk (TOR) paper [4] published in February 1988. Evidence on the topic was given subsequently at the Hinkley Point 'C' PWR Inquiry.

The paper suggests upper limits, ie maximum tolerable levels of individual risk to workers and the public and a maximum tolerable societal risk from a programme of modern power reactors. The proposed maximum tolerable risk to the workers are comparable to those in conventional industry: a risk of death of 1 in 1000 per annum (though the calculated nuclear risk is that of delayed cancers rather than the immediate actual fatalities occurring in those industries). For the public, the proposed maximum tolerable risk is a factor of 10 lower than that for the workers. This is to recognise that the public contains susceptible groups (the young, chronically ill, etc) and also that the public has little choice about whether or not to accept the risk.

Below the proposed maximum tolerable individual risk levels, the as low as reasonably practicable (ALARP) principle applies. The current design standards in the UK are such that the individual risks from accidents are estimated to be much less than from exposures to direct radiation and authorised discharges in normal operation, and both are judged to be within the TOR limits.

The proposed maximum tolerable societal risk from accidents is a new regulatory concept in the UK. One of the difficulties with societal risk is that it is a composite of several risks, for example:

early deaths,

late health effects such as cancer and heredity defects,

contamination of land etc,

initiation of the emergency plan for the site with the consequent social disruption,

the socio-economic risks to the nuclear programme (eg as in Sweden, Italy and the Netherlands after Chernobyl).

Rather than try to add these together, the TOR paper has chosen to represent the societal risk by the number of eventual cancer deaths caused by accidents. (Early deaths were not chosen as an appropriate indicator, since most accidents will not lead to early deaths.) The paper proposes therefore, as the limit of tolerability from nuclear reactors, the frequency of an accident occurring anywhere in the UK and leading to doses of 100 mSv at 3 km from the site (it being pessimistically estimated that this might cause 100 cancer deaths). On the basis of current risk estimates, the paper suggests that if there were 20 modern power reactors in the UK, this would take up about a fifth of the proposed limit. (While this indicates a comfortable margin for the presently envisaged programme, there is a clear implication that, for the future, there should not be an unlimited proliferation of power reactors without a corresponding improvement in the safety standards achieved.)

Our SAPs are currently being revised and consideration is being given to incorporating the ideas set out in the TOR paper, including the individual and societal risk criteria. As a result, the SAPs may extend by several decade steps into the region beyond the design basis. This compares with the present situation in which no distinction is made between smaller and larger release accidents in that region.

4 HUMAN FACTORS

Our second area for consideration is one where the emphasis rather than the objective is changing. It is a familiar one, both from incident reports and from everyday experience. The public perceives human error as a major concern in safety - both TMI-2 and Chernobyl-4 have made this impact on people's attitudes. At the Sizewell 'B' Inquiry, human error emerged as a significant issue. The NII presented evidence on human factors [5], and the Inquiry Inspector Sir Frank Layfield responded with the recommendation that "the NII must ensure that the CEGB's (Central Electricity Generating Board) commitment remains strong and is applied thoroughly and consistently to the remaining design stages, construction, commissioning, operation and maintenance . . . ." [3]. Translated into probabilistic safety analysis (PSA) terms, we must ensure that the contribution of human error will not dominate the risk from the station.

The objective is easily stated, but its realisation is more difficult. The human operators, and all of the other personnel involved in the station, cannot yet be modelled so that we can determine and control their precise contribution to risk; indeed, there are persuasive arguments that such a degree of understanding of human and social processes will never be achieved. Nevertheless, at a more pragmatic level, we were able to report to the Hinkley Point 'C' Inquiry further progress towards reducing the incidence and effects of human error. For design, both operations and maintenance tasks have been analysed, and the results translated into design of the control room and other plant areas. For operational management, the CEGB is reviewing its approaches to organisation and management on the station, a comprehensive training programme for all staff is being developed, and operating procedures are being designed and analysed for resilience against human errors.

The above topics are concerned with maximising human reliability in all transactions between the station staff and the plant. Can the outcome be stated in quantitative terms? Most safety cases up to now have not included human operations in the fault and event trees: this can be justified in part by the "30 minute rule" (NII Safety Assessment Principle 124) - "The protection system should be automatically initiated. No operator action should be necessary in a timescale of approximately 30 minutes. The design should, however, be such that an operator can initiate protection system functions . . . . perform necessary actions . . . . but cannot negate correct protection system action at any time."

NII considers that comprehensive quantification of human reliability is not practicable at present, but we do expect the licensee to incorporate relevant and valid human error quantification where possible. As part of the continuing discussions with CEGB on the development of the PSA for the Pre-Operational Safety Report (POSR) for Sizewell 'B', it appears that some significant developments will be made in human reliability assessment. There are intentions to include certain human safety actions in fault trees, to quantify human contributions to unavailability of protection or safety systems, and to have special procedures for adding other significant human contributions into the PSA calculations. Our future objective is that this small beginning should be progressively extended. How far it can be taken is difficult to predict. However, the golden principle that good engineering must precede

PSA extends to human factors also - the qualitative assessment of all the human factors areas listed above is of equal importance to the defined human reliability quantification [6].

5. USE OF COMPUTERS IN PROTECTION SYSTEMS

As indicated above, human error has been targeted as an important objective. In one specific aspect of this topic, the use of computerised protection systems in new plants, concern has been expressed at the Hinkley Point 'C' Inquiry over the ability of the current software production techniques to generate the required level of reliability for safety-critical applications.

We recognise the concern but also recognise the positive contribution which can be made by computerisation. Computers have characteristics of capability and versatility that can bring benefits in improved safety strategies, both operational and through self-monitoring. The objective in this case should be to take advantage of the benefits while ensuring that those same characteristics do not work to the detriment of safety.

In our view, that aim can be achieved by keeping the systems simple while adhering to the principles applied with success to protection systems in the past, in particular redundancy and diversity. Computers forming part of a protection system should not be used for non-safety functions or operational control. The software should be designed, manufactured, and maintained in such a way as not to degrade the overall protection system reliability. Defensive programming approaches should be used which protect against hardware and software malfunctions. Unsafe programming practices should also be prohibited. There should be independent assessment of the software. The best methods should be used for analysing and testing the software to check that it is error-free and satisfies its specification. Quality assurance plays a major part in reducing the errors in software but equally the software manufacturers must employ a team of competent personnel who are not only well-versed in computing but have a thorough understanding of the nuclear plant for which they are designing.

As with all disciplines, computing is making advances. New techniques of mathematical design and analysis are emerging and will feature increasingly in future safety objectives and strategies as a means of maintaining and improving the current high levels of safety integrity in protection systems.

6. CONCLUDING REMARKS

In introducing this paper, I pointed to the background in the UK of licensing and regulating a variety of nuclear plants against a set of safety objectives and more detailed requirements. The NII has to be satisfied that these plants are safe, otherwise they would be shut down. Therefore, the first objective (though it hardly needs stating) must be to ensure that plants in the future are at least as safe as those of today.

The main part of the paper dealt with the HSE's proposals on tolerability of risk and the implications for the NII, particularly as far as societal risk is concerned. This development implies that any new plant would have to be considered in the context of the overall risk which the UK's nuclear power commitment poses to the public, not just the risk to individuals in the vicinity of that one plant.

The remaining points were matters of detail, but significant nevertheless. The topic of human factors is widely recognised as important. The NII believes that licensees in the UK are moving in the right direction and, as a future objective, we intend to ensure that they continue to do so.

The concern about developments in the use of computerised protection systems and, in particular, about the software used in them, involves a specific aspect of human factors. Our objective will be to ensure that these developments are to the benefit of safety.

Finally, the NII is aware of the moves towards "safer" designs of plant. We have not chosen to set such plants as an objective; it is for industry to make the running in those matters. Nevertheless, we welcome the move but will be looking just as closely at the safety of the new designs as we do for existing plant concepts, if and when proposals are put forward to build them in the UK.

REFERENCES

[1] Safety Assessment Principles for Nuclear Reactors, HMSO, ISBN 0 11 883642 0 (1979).

[2] Safety Assessment Principles for Nuclear Chemical Plants, HSE, ISBN 0 7176 0153 6 (1983).

[3] Sizewell B Public Inquiry: Report by Sir Frank Layfield, HMSO 0 11 411576 1 (1987).

[4] The Tolerability of Risk from Nuclear Power Stations, HMSO, ISBN 0 11 883982 8 (1988).

[5] Sizewell B: A Review by H M Nuclear Installations Inspectorate, Supplement 13: Human Factors (Evidence to the Sizewell B Public Inquiry), NII 01(Supp 13) (1983).

[6] WHITFIELD,D., "A regulatory perspective on human factors in nuclear power, Human Reliability in Nuclear Power (Conf. Proc. London 1987), (ANTHONY R.D., Ed.), IBC Technical Services Ltd., London (1988).

APPLICATION OF SAFETY OBJECTIVES TO SAFETY STANDARDS AT THE NEXT STAGES OF NUCLEAR POWER DEPLOYMENT

V.A. SIDORENKO
USSR State Committee for Supervision
of Nuclear Power Safety,
Moscow,
Union of Soviet Socialist Republics

Simultaneously with the elaboration of "Basic safety principles for NPPs" by the INSAG group, the new edition of "General principles for providing NPP safety" was being worked out in the Soviet Union. This is the top document in the hierarchy of safety standards that regulate nuclear safety. Therefore, in the updated 1988 version of the document not only the experience gained in this country following the Chernobyl accident, but also international experience has been used.

The document is to become valid beginning from June 1990. Thus the development of the new NPP generation will be conducted on its basis. Some safety targets expressed in probabilistic terms are introduced in this document.

First of all, it's the probability of an intolerable event taken as 10^{-7} per reactor per year. Evacuation of people from densely populated areas with number of inhabitants exceeding 100 thousand people may be regarded as such an intolerable event.

Since standards in the Soviet Union provide that the distance from a nuclear district heating plant to an area with such population must not be less than 5 km, and must not be less than 25 km for an NPP, evacuation with such a probability must be excluded beyond those distances. Designing of auxiliary technical accident management systems must serve this objective.

In safety standards this is reached through setting a limited value of emergency radiation emission. The probability of a fatal reactor vessel brittle destruction is also defined by this value; the capability of achieving it must be provided in the project. The target reference value for excluding beyond design basis accidents with severe core destruction or core melting has also been introduced. It equals the probability of 10^{-5} per reactor per year.

The setting of such reference targets in General Safety Rules-88, expressed in probabilistic terms, does not mean quantitative control over nuclear power safety. Gosatomenergonadzor is not ready for it, and such an approach is scarcely capable to prove itself reasonable. This is due to the subjective and theoretical origin of the assessed probabilities, based on a number of conditions that are not once and forever fixed and undergo constant changes in real life. They are influenced by many factors, including such an unpredictable one as human behaviour. That's why it would be premature to regard the indicated values as absolute criteria. Along with such assessments and values that are undoubtedly important for correct decision-making, some deterministic criteria of the acceptable safety level must be available. One of them is included into the General Safety Rules-88 and is called inherent safety. Special engineered safety features may not be needed in case when the application of such a principle and principles of reactor design excludes design- basis accidents with severe core damage or core- melting.

The assessment of the acceptability of NPP siting from the viewpoint of emergency evacuation being possible is primarily based on the maximum permissible accidental release and maximum permissible radiation burden at emergency conditions: internal exposure of a child's thyroid gland at inhalation- 30 BER, and external radiation exposure for adults- IO BER during the first post- accident year.

To our mind, the most stringent criterion substantially limiting the tolerable probability of accidents is the societal criterion based on an anticipated level of global societal consequences of the severe accident. This concept characterizes the current state of nuclear power and its acceptance by public. In the course of the foreseeable term of nuclear power development (about 50 years), no matter how many NPPs are constructed or in operation, not a single severe accident with a radioactivity release , exceeding the maximum permissible value, should occur.

At the expected scale of nuclear power development a similar criterion seems to be the economic-ecological one, that characterizes the acceptable damage to the station, territorial alienation, etc.

The accepted reference value for an untolerable event- IO^{-7} per reactor per year proves to be reasonable for a long- term period. Significant errors must also be taken into account. They emerge at assessing severe accident probability for certain advanced power units.

Reactors of different generations will probably approach the reference value in different ways: the next generation must provide aa compliance with the auxiliary reference value- the decrease of severe core destruction probability to the figure of IO^{-5} per reactor per year, and the decrease of the worst release probability to IO^{-7} per reactor per year due to the enhancement of measures of localizing the consequences of a probable reactor destruction / accident management systems/.

Reactors of future generations, that are to a larger extent inherently safe, will provide a simultaneous compliance to necessary requirements due to the decrease of the reactor core destruction probability up to the reference target of 10^{-7} per reactor per year.

SAFETY ASPECTS OF THE NEXT GENERATION OF CURRENT-TYPE NUCLEAR POWER PLANTS

(Session V)

Chairmen

A.A. ABAGYAN
Union of Soviet Socialist Republics

P. BYSTEDT
Sweden

SAFETY ASPECTS OF NEXT-GENERATION CANDU REACTORS

G.L. BROOKS
CANDU Operations,
Atomic Energy of Canada Limited,
Mississauga, Ontario,
Canada

Abstract

Since it is obvious that safety improvements should be evolved within the context of a coordinated overall reactor development program, the paper firstly discusses the overall requirements established for next-generation CANDU reactors. Specific safety-related requirements are then identified within the context of these overall requirements. Finally, the paper describes the general directions being followed to satisfy these safety-related requirements.

The overall requirements for next-generation CANDU reactors have been established to satisfy the needs of a broad spectrum of "stakeholders" in the projected rebirth of the nuclear power industry. Such stakeholders include the general public, the owner utilities, regulatory bodies, and political leaders. All of these stakeholders have a vital interest in safety. Most do, however, have other needs which must also be satisfied, e.g., economic electrical generation to name but one. A balanced approach is therefore appropriate and, indeed, essential. Fortunately, with such a balanced approach, worthwhile safety improvements can, and will, be achieved while satisfying these other stakeholder needs.

Much is heard today of concepts such as "inherent safety" and "passive safety". These concepts are discussed, both in general and in the context of CANDU development. While future CANDU reactors will embody appropriate applications of these concepts, the emphasis in CANDU development will be on logical evolution rather than on revolutionary new design concepts.

---

1. Introduction

While, in keeping with the theme of this conference and session, this paper is concerned primarily with the safety aspects of envisaged next-generation CANDU reactors, the subject of safety cannot be considered independently from other development directions. For this reason, the paper firstly discusses the question of overall requirements for such next-generation reactors. Safety-related requirements are then identified within this overall context. Having described what we believe to be an appropriate set of such safety-related requirements, the paper then discusses the directions we will be taking in satisfying them.

2. Establishing the Requirements

In considering the question of next-generation reactors, I recognize that there are those who believe that safer reactors are essential to the rebirth of a healthy nuclear power industry. Indeed, some proponents of this view would seem to suggest that if only we could develop such "safer" reactors, suddenly all of our problems with public acceptance would disappear and utilities would form long lines waiting to purchase such marvellous machines. I do not share such a simplistic view nor, indeed, do many of my colleagues in the international nuclear power industry. Are, however, such safer reactors a necessary, if not sufficient, requirement for industry rebirth? I believe that this question cannot be answered in the implied narrow context of safer reactors. I prefer to deal with the question in the broader context of risk and, furthermore, not just risk to the general public in the sense of accidents, but rather in the context of risk to all of the "stakeholders" who would be involved in a rebirth of the industry. Such stakeholders include, for example:

- <u>the general public</u> - both in the sense of benefitting from low cost, low environmental impact electrical energy and in the sense of acceptable risk of injury and economic loss through reactor accidents;

- <u>the owner utilities</u> - in the sense of economic and reputational risk arising from construction delays, cost overruns, poor operating performance, and the potential economic and reputational risk arising from serious accidents;

- <u>regulatory bodies</u> - in the sense of reputational risk arising from both potential accidents and risk of excessive costs to electrical ratepayers;

- <u>political leaders</u> - in the sense of responsibility to their constituents and in the sense of risk to their personal reputations arising from power shortages, potential accidents, environmental issues, consumer advocacy campaigns, etc.

While safety in the sense of the subject of this conference has significance to all of the foregoing stakeholders, it is clearly not the sole criterion. This suggests that the requirements for next-generation reactors must be broadly defined and that an overly narrow focus on safety could well be counterproductive to the overall interests of the stakeholder community at large.

I believe that one further question bears close examination before discussing the subject of specific requirements for next-generation reactors. This question can be simply stated as follows: Can there be such a thing as an "inherently safe" reactor if by safe we mean zero risk. Clearly the answer is no. Fission reactors produce fission products. Most fission products are radioactive. The radioactive decay process produces heat which provides a thermodynamic potential to disperse the fission products unless, of course, the reactor power level is extremely low. Hence, in the case of power reactors, zero risk is inherently unachievable, no matter how clever we are. We have to recognize that the vocal anti-nuclear community will always be able to invent doomsday scenarios to frighten the public, irrespective of what we do as designers! Claims of "inherent safety" will not silence the noisy nuclear power debate.

Why is the foregoing point significant? Its significance lies in the fact that if zero risk is inherently unachievable, then we are unavoidably faced with the long-standing question of "how safe is safe enough?" If we start with the public, there are, I believe, two answers to this question, at least qualitatively. If the public perceives that nuclear power provides no net personal benefit, or is simply not needed, then they will only accept zero risk. If, on the other hand, the public perceives a net personal benefit, then they will accept some measure of risk. The latter is demonstrated by the case of air transport. Private automobiles provide another demonstration. In my view, nuclear power has failed to capture the acceptance of a large segment of the general public because the perception of net personal benefit has not been established. This is true today in most countries of the world. Fortunately, however, this suggests a potential key to solving our current dilemma. Once the public becomes convinced that nuclear power plants can be built to schedule and within budget, can operate reliably, and can produce electricity at costs significantly below alternative sources, they will much more readily accept some, albeit perhaps small, measure of risk. Put in other terms, to become comfortable with nuclear power, the public must perceive it as being manageable in all of its aspects. In my view, this is very much tied to perception of risk in the safety sense. The sad record of too many nuclear power plants in terms of long construction periods, overrun budgets, licensing problems, poor capacity factors, etc., does not instil confidence that we in the industry know what we are doing. Inevitably this lack of confidence extends to perceptions of safety or, more specifically, a lack thereof. These problems also relate back to the question of perceived advantage to the public. Too often, the promise of lower electricity rates has not been fulfilled.

If the foregoing thesis is correct, then we are fortunate because the directions we must take in gaining public confidence are generally compatible with the directions we need to take to build confidence with the other stakeholders. It is interesting, in this regard, to note that the requirements we should adopt, as implied by the foregoing discussion, are generally consistent with those developed by EPRI in leading an industry-wide effort to establish a technical foundation for the design of the next generation of light water reactors in the United States [1]. Specifically, EPRI has established three "fundamental standards" for a next-generation nuclear power plant:

- It must be an excellent power plant in all respects, including safety, reliability, maintainability, and compatibility with the environment.

- It must be economically competitive with fossil-fired electricity generation.

- It must provide a very high level of protection for the owner's investment, in terms of predictable construction costs and schedule, assured licensability, predictable operating and maintenance costs and very low risk of a severe accident.

Moving now from these broad requirements to what I will call a "lower-risk", next-generation family of reactors", we need to examine, specifically, the question of appropriate safety requirements and how these fit within the context of lower overall stakeholder risk requirements. It is at this point that we face an apparent paradox. On one hand, I note that most responsible members of the world nuclear industry believe current generations of commercial reactors are, indeed, "safe enough". On the other hand, many industry leaders currently support the view that safer reactors are needed. How do we explain the existence of these apparently divergent views? The answer, I believe, lies in judgments and perceptions of marketability in a broad sense.

Dealing firstly with marketability to the general public, there is little question but that a substantial segment of the public perceives that current reactors are not safe enough. This leads many to the conclusion that next-generation reactors must be demonstrably "safer". If we then focus more closely on this issue, it has been suggested by some that the requirement really centres on those who lead public opinion. As the "facts of life" become progressively more apparent regarding such claimed panaceas as energy conservation, and renewables, coupled with rising concerns regarding the greenhouse effect, we must provide a way for a sizeable number of these leaders to gracefully move to a position supportive of nuclear power. By providing demonstrably safer reactors, we will avoid the need for these leaders to admit that they were previously wrong regarding the safety of nuclear reactors.

There are, of course, hazards involved in following this approach which would need to be carefully considered. Firstly, in moving to safer designs, we could inadvertently appear to acknowledge that current reactors are "unsafe". Secondly, we could develop safer designs which are, however, counterproductive to the broader spectrum of stakeholder risks discussed earlier, e.g. designs which are economically uncompetitive, particularly if major R&D costs must be amortized. Thirdly, we could be seen as promising more "safety" than we can actually deliver, e.g. by overselling such imprecise terminology as "inherently safe" and "passive safety". Despite these hazards, I believe that this is the basic direction in which we must move.

I believe the best approach to avoid the hazards noted above is to follow a course which reduces, in a balanced manner, all (or at least the greatest possible number) of the full spectrum of stakeholder risks.

Having set this broad requirement, we must return to the question of "how safe is safe enough?" More specifically, in terms of the foregoing discussion, the question can be rephrased as "how much extra safety is needed to permit an adequate number of public opinion leaders to move to a position supportive of nuclear power?" Obviously there is no quantitative answer to this question. Even a superficial review of the various published next-generation reactor design concepts shows a wide divergence of view among designers attempting to grapple with this question. In the absence of a quantifiable goal or requirement, how are we to proceed? The answer lies, I believe, in the normal engineering approach to such situations. We must seek to develop worthwhile safety improvements while keeping our eyes firmly focused on those stakeholder requirements which can be reasonably quantified, e.g. cost competitiveness, reliability, maintainability, etc. The logic of this approach will be self-evident if one considers the inevitable consequences of not satisfying these other vital stakeholder requirements! As a specific example, in following this approach to developing worthwhile safety improvements, we can satisfy other stakeholder requirements by focusing attention on means of reducing the probability of accidents which result in major reactor core damage. Such accidents are not only significant in terms of public safety considerations but would also result in severe economic loss, major political difficulties, and further erosion of public confidence.

I note that the EPRI ALWR "fundamental standards" referred to earlier in this paper are fully consistent with this approach.

As a last but important comment, in following this approach, we must ensure that the engineering solutions we develop are understandable and saleable to the public at large. While not, in itself, a solution to the public acceptance issue, such "transparency" will prove helpful.

3. Charting the Course for CANDU

In moving from the broad requirements discussed in Section 2. to specific safety-related development directions for CANDU, it is appropriate to firstly consider the current status. As discussed in reference [2], the PRA results for current-generation CANDU reactors compare very favourably with those of other contemporary designs, either in-service or under construction. Three important and relatively unique features contribute to these very low predicted core-melt frequencies:

(i) The provision of two independent and diverse full-capability automatic shutdown systems results in extremely low predicted ATWS event frequencies.

(ii) The ability of the independent moderator system to remove decay heat without core melt provides an additional defense line for a wide variety of loss of heat sink events and LOCA combined with ECCS failure.

(iii) As a further defense line beyond (ii) above, the water-filled reactor shield tank and its separate cooling system would limit the consequences of a core-melt should the moderator system fail.

These already established advantages will be retained.

Turning now to future design-related developments, I share the view expressed by a number of other reactor designers that the key to demonstrably improved levels of safety lies in several directions:

- overall plant simplification
- increased use of passive design features
- increased tolerance to operating transients and upsets
- improved man/machine interface
- improved testability and on-line "state-of-health" monitoring
- improved containment capability and reliability

While the foregoing directions are separately identified, there areclearly important linkages between them and, indeed, between these safety-related directions and the general spectrum of stakeholder requirements discussed above. In some cases, these linkages will be mutually supportive; in others, there will be conflict. The challenge to the management of the design process will lie in maximizing the overall benefit of supportive linkages and in reaching an optimum compromise in the case of conflicting linkages.

I will now discuss the individual safety-related directions in terms of some of these linkages. This discussion will be illustrative rather than comprehensive but will suffice to identify the key considerations involved.

Starting with overall plant simplification, this can directly improve the man/machine interface since, by and large, a simple plant is easy for the operator to understand. Simplification should directly assist testability and "state of health" monitoring since there are fewer things to test and monitor. A simple containment system will almost certainly be more reliable. In terms of broader requirements, simplification should lead to lower capital cost and lower maintenance cost since there are fewer things to buy, instal, and maintain.

Turning next to increased use of passive features, this can lead to simplification since passive systems are generally highly reliable, and hence, may reduce the need for back-up systems. They may well assist the man/machine interface since fewer operator control and/or monitoring functions would be necessary. Passive post-accident heat removal from containment should improve reliability of this important function. On the other hand, passive features may tend to increase capital cost and may impede testability and maintainability, depending on the specific application. Careful consideration of the trade-offs involved will be required.

With respect to increasing the tolerance to operating transients and upsets, there is a clear potential benefit in terms of the man/machine interface in that fewer operator actions will be required and more time will be available for performing these actions. However, in this case, there will almost certainly be an increase in capital cost, e.g. larger reactor core size, larger steam generator water storage, etc. Once again, careful consideration of trade-offs is necessary.

Improvements in the man/machine interface will not only benefit safety through reducing operator error but will also improve production reliability. In Canada, most designers and operators believe that this is probably one of the most important directions we should be taking in terms of potential benefit to both safety and operational reliability. Given the current rate of advance in the relevant technology areas, we believe that little, if any, additional capital cost penalty will be incurred.

The direct benefits of improved testability and on-line "state of health" monitoring are obvious, not only in terms of safety but also, potentially, in terms of enhanced production reliability. Note the word "potentially". Too often in the past, safety system testing has caused spurious reactor trips and other upsets. On-line "state-of-health" monitoring, if not highly reliable, can cause similar production problems. Simplification and man/machine interface improvements can help substantially to reduce these undesirable side-effects.

To a substantial degree, improved containment capability and reliability is concerned only with improved safety since containment fulfils no production role. However, containment impairments can adversely affect production reliability through mandated plant outages. Containment periodic pressure testing can be a critical-path activity during plant maintenance outages. Once again, simplification, improvements in the man/machine interface, and improved testability and on-line "state-of-health monitoring can be highly beneficial in improved production reliability.

4. Specific Examples

While I will not attempt, in this paper, to provide a full catalogue of specific improvements which will be incorporated in next-generation CANDU reactors, the following illustrates two typical examples:

(i) Control Room Improvements

CANDU reactors have, for many years, pioneered the application of digital computers for the on-line, closed-loop control of the reactor and many plant systems. Driven by these same computers, CANDU plants have incorporated extensive CRT displays of plant operating parameters in flexible "user-friendly" formats. Building on this extensive technological base, future CANDU plants will move, almost entirely, to the use of computer control with keyboard/CRT operator interfacing, thereby dispensing with conventional control panels.

With this approach, it becomes possible for plant operators and designers to interactively develop plant operating procedures and plant control and display software in parallel during detailed design of the plant. Furthermore, since no "hard" physical locations will exist for specific instruments, switches, etc., all operator actions needed to handle any event can be performed from one position with all required status information brought to that position. The operator will also be able to call up operating procedures on the CRT displays covering all normal, upset, and accident situations. For the latter, both event and symptom oriented procedures will be available. These procedures will be "smart" in that only those steps requiring specific operator action will be displayed, reflecting the actual status of the plant at the time. For example, if a valve is already in the required position, the step instructing the operator to change the valve to that position will be eliminated from the display. Alarm annunciation will be "filtered" to display only key messages needed to guide correct operator action. Special safety parameter displays will be available to enable the operator to quickly assess the status of these parameters.

(ii) Passive Heat Sinks

As noted in the IAEA NUSS Code of Practice-Design, one of the fundamental safety requirements relates to the need for the safe removal and dissipation of decay heat from the reactor fuel under all post-reactor-shutdown conditions, including accident conditions. In common with all other current commercial reactor types, CANDU reactors have, to date, relied on a variety of "active" systems to perform this function. In aggregate, these systems are relatively complex, particularly because of redundancy and diversity requirements. Additional complexity results from the need, in many instances, to configure the systems in specific ways to handle specific upset and accident conditions. In addition to the systems themselves, their active nature requires highly reliable, and therefore often complex, service systems such as electrical power and compressed air. All of this complexity adds to capital cost, testing requirements, maintenance requirements, and operating problems.

At the present time, several design groups around the world are attempting to develop passive systems to replace the functions performed by these complex active systems. While total "passivity" may not be achievable in all cases, we believe that the approach is fundamentally correct and should lead to major simplifications, improved operability and maintainability, reduced testing requirements, and greater assurance that safety objectives can be achieved under all circumstances. It may even be, as some claim, an important step towards improved public understanding and acceptance of nuclear power. This remains to be proven but I can certainly say that, based on long experience, explaining our current safety defenses to the lay public is far from an easy task!

As to specific passive design features we are currently studying for future CANDU application, I refer to a companion paper being presented (poster session) at this conference [3].

5. Concluding Remarks

In order for nuclear power to fulfil its appropriate role as an increasingly important source of electrical energy throughout the world, the nuclear power industry must renew its efforts to satisfy all stakeholder requirements. Of these requirements, public safety occupies a special place. A broadly-based renewal of public acceptance of nuclear power will not be achieved until the public is satisfied that adequate (to them) levels of safety can be assured. Technical improvements in the safety of future nuclear power plants will not, in themselves, solve the problem of public acceptance. They can, however, serve as a centre-piece of new public information initiatives, provided their benefit is "transparent" to the public or, at least, to public opinion leaders. New passive safety features and man/machine interface improvements would seem well suited to this "transparency" requirement. Future CANDU safety improvements will be centred on these areas.

I believe that these safety-related initiatives are essential. They must, however, take their place along with other initiatives intended to meet other stakeholder requirements. Balance must be maintained. The "safest" reactor in the world will not succeed unless it satisfies economic imperatives.

References

[1] K.E. Stahlkopf, J.C. DeVine and W.R. Sugnet, "U.S. ALWR Program Sets Out Utility Requirements for the Future", Nuclear Engineering International, November 1988.

[2] AECL-9606, "CANDU Safety Under Severe Accidents" by V. Snell et al. Paper presented at IAEA/OECD International Symposium on Severe Accidents in NPP's, Sorrento, Italy, March 1988.

[3] Passive Safety Features for Next Generation CANDU Power Plants, A. Natalizio, R.S. Hart, J. Lipsett.

SAFETY ASPECTS OF ADVANCED PWR DESIGNS IN FRANCE

P. BACHER
Direction de l'équipement,
Electricité de France,
Paris, France

Abstract

After a broad introduction explaining the French conception of a global approach to safety, based upon feed-back of experience, upon the use of both passive and active safety features, upon the quality and the reactivity of man, and upon an in depth defense and an in depth culture, the status of the present advanced light water reactor N4 is described.

The global probabilistic safety objective of a core damage due to internal events of the order of 10^{-5}/reactor year appears to be reached, and this result is achieved in a balanced manner, no individual failure path being responsible for more than 1 or 2.10^{-6}. This is quantitatively satisfactory, as accident management measures reduce by a significant figure the severe accident probability.

The discussion of improvements for future plants concludes that qualitative, not quantitative, progress is necessary. Such an analysis has been undertaken in France in the REP 2000 program, and a few examples are given, both for the evolutionary type of reactor derived from N4 or Konvoy and for semi-revolutionary types such as AP 600.

The conclusion is that whatever the types of reactors, the requirements for the next generation of reactors, to be built at the turn of the century, will most likely be worldwide or at least European and not French, or German, or British, or Spanish...

---

1. INTRODUCTION : FOR A GLOBAL SAFETY

Fashion is to simplifying slogans :

- Inherent safety

  passive safety

  walk-away reactors

  zero release

  ...

Safety -like life- is too complex to be boiled down to such slogans.

In economy, previsionnists have always under (or over) estimated the reactivity of man and society :

- oil bounty in the 60's,
- oil shocks in the 70's,
- counter oil shocks in the 80's.

In military strategy, everyone knows that the best defense is to attack :

- both the French and the Germans know that the passive "ligne Maginot" was totally inadequate to prevent the German armies from overwhelming France,

- and the only strength of the massive and passive Atlantic wall were Rommel's divisions ready to push back the allied armies into the sea.

In management policy, one of the major problems is to measure through indicators the reactivity both of the system and of man. And it is quite evident that every 5 or 10 years new theories, with new simplifying models, have to be developed to take into account man's capability to adapt himself to, and counter, any management strategy.

I could go on indefinitely that way with examples from each living activity. What I really want to point out is that **safety**, like any other activity related to man, must be **reactive** and **not passive**. Isn't this the basis of safety **culture** ? In this sense, if anyone came to me and said :

- "Pierre, here is a good reactor. No matter what happens, you can be sure, you can **walk away**",

I really would be scared because the operators might really tend to believe it. Such a proposition would be **anti-safety culture**. To me, a walk-away reactor is one you should **run away** from before it runs away from you.

There is no such thing as **passive safety**. There are, fortunately, **Passive Safety Features** : steam generators are the major passive feature which differentiate PWR's from BWR's. Gravity driven control rods are usually understood to be a passive feature. So is a lay out which enhances natural convection, or stored energy sources such as pressurised water accumulators or electrical batteries. And of course a strong containment which lacks in the RBMK's and WER 440's.

But when you go into details, what do you find ?

Table 1 identifies, for a few well-known passive safety features, some of the failure mechanism and some of the available mitigating measures. One can see that operator actions and active systems are often the only good way to cope with a passive system failure.

In other words, passive safety features are excellent things, as long as you abide by certain rules :

- ISI or (and) surveillance,

- adequate instrumentation,

- adequate control systems,

- adequate valves + motorisations,

- and... active systems to help them along,

- **and man** for good design - good maintenance - good operation and REACTIVITY to feed-back of experience.

Likewise there is no **inherent safety**. Fortunately, there are inherent safety features such as delayed neutrons and the Doppler coefficient, without which nuclear reactors would never have been built.

Table 1 : failure mechanisms of some passive safety systems

PASSIVE SAFETY FEATURE	FAILURE MECHANISM	CONSEQUENCES	MITIGATING MEASURES
Steam generators	S/G tube failure	loss of 2nd+3rd barrier	. in-service inspection . leak detection . accident procedure + operator action
Gravity-driven Control rods	ATWS	no shut down	. periodic tests . redundant + diversified protection system . operator action
Natural convection	steam or non condensible gas locks	no heat removal	back up pumps
Stored Energy Sources			
. water accumulator	. loss of pressurization . flow of pressurizing gas into the reactor	. failure to operate . gas bubble in reactor core	. instrumentation . redundancy . valves
. batteries	. loss of tension	. no control	. redundancy
Containment	no isolation	leakage	instrumentation + control

But take a negative coolant temperature coefficient : it is an inherent safety feature as regards an increase in temperature. So good. But what about a cold transient, such as that which results from a reactor shut down without stoppage of the feadwater flow. For the system as a whole to be safe, you must of course have :

- a negative temperature coefficient,
- a reliable instrumentation,
- a reliable protection system,
- reliable valves + motorisation,
- and **man** for good design - good maintenance - good operation and **reactivity** to feed-back of experience.

To conclude this introduction, I will repeat that safety is too important and complex to be boiled down to a few magic words and least of all to one single slogan (passive, inh...). Of course, **passive features** are excellent. But there are really no objective reasons to scorn **active features** (reactor protection systems are a necessity and so are valves ;

pumps are usually very useful and reliable,...). The **reactivity** of man to unforeseen events - or even to foreseen events- and to the feed-back of experience is a <u>must</u> of the safety CULTURE. Our approach to safety is therefore **global**, based upon **feed-back of experience**, upon both **passive** and **active** features and systems, upon **quality** and **reactivity of man**, upon an **in depth defense** and an **in depth culture**. **Public acceptance** is of course a major goal of our approach to safety.

This global view on safety has been the basis of the French approach to safety for the advanced N4 plants and remains so for the next generation of current-type PWR's. I shall first review where we stand today with the feed-back of experience, and then explore the possible paths for further progress.

2. FEED-BACK OF EXPERIENCE : THE CASE FOR N4

In a report by the Safety Working Group of the European Economic Commission at the NUC'SAFE Conference in Avignon last year [1], "the systematic use of feed-back of experience in order to correct weak points, thus reducing risks" was identified, supplementary to the deterministic and the probabilistic methods, as one of the most important and universally recognized method to achieve safety.

The severe accident at Three Mile Island has greatly influenced the design and operation of present NPP's, pointing out particularly the overwhelming importance of the man-machine interface in the prevention of core-melt, and of the containment in the mitigation of consequences. A contrario, Tchernobyl demonstrated the same thing.

Reliability data from operating plants begin to give a sound basis for PRA's or PSA's. They show several very interesting features related to man. First of all, during plant operation, there is a relatively large risk of human error when he has to react quickly : automatic actions are best in such situations. But there is a high probability that recovery will succeed because a man is there to understand what is going wrong. It is therefore of the utmost importance to balance correctly the respective areas of automatisms and of man. Second, there is a large risk of human error during <u>maintenance</u> (remember the auxiliary S/G feedwater valves in TMI), and this risk can be overcome either through very strict procedures, or through a very high level of data processing, or both.

R and D programs, particularly on hydrogen generation and on corium-concrete interactions, have given reliable data on some aspects of severe accidents, although additional work is still required to really know how to manage severe accidents.

Although I shall develop here only the case of the French NPP's, it is quite clear that other modern NPP's, such as the German Konvoy, have also taken advantage of the feed back of experience, and particularly of the lessons learned from Rasmussen's WASH 1400, from TMI, and from less severe but not less significant events in operating plants.

The French 1300 MW reactor safety study [2], based upon a unique reliability data base coming from the fifty odd French standardized plants, and upon detailed experimental work on human reliability, yield a global core damage probability of about 10^{-5}/reactor-year, a figure which ought, if anything, be slightly better for N4. This result is obtained through a combination of active and passive systems. Particular emphasis is placed upon the use of the energy available in the secondary steam, to drive both auxiliary feed water turbo-pumps and a small auxiliary turbo-generator. Combined, these systems give more than 24 hours of autonomy in case of station black-out.

Another feature of the global approach to safety in the N4 plants is the complementary roles of machine and man [3], through the extension of the defense in depth principle to accident procedures and operation management. This approach, initiated in the late 70's, was accelerated by the accident at TMI. The general idea was that, should preventive or mitigating procedures fail, the operator should have ways to recover.

This implied first that beyond design situations, such as station black-out or total loss of feed water to the steam generators, be integrated in the procedures. It also implied that, if symptoms of impending core damage were present (as they were in TMI), the operator should have clear and simple indications of what to do to prevent such core damage.

Another consideration had to do with the reliability of the operator himself. The accident at TMI clearly showed that even the best trained operators were in difficulty when unforeseen events happened. Further reliability studies showed that under stress conditions, the probability of human error was greatly increased. This led to the decision to reinforce accident management with a specially trained safety engineer, summoned to the control room any time an accident procedure is initiated (i.e. each time there is a reactor scram or an emergency safety injection) and whose sole duty is to monitor symptoms that might lead to core damage and to decide when to switch to the ultimate core damage prevention procedure.

Next before last in the defense in depth approach comes the severe accident management. Although we do not yet have detailed phenomenological and probabilistic studies of core melt accidents for French plants we can infer from comparison with USNRC studies [4] that the probability of early containment failure (from internal events) is very small. The emphasis was therefore placed on preventing late containment failure due to slow pressure build up with or without hydrogen combustion, and this led to the decision to install a containment vent and a sand bed filter. Venting would in most cases not be necessary before several days, but could be implemented after 24 hours, with a source term at the chimney of the plant of the order of (or less than) .001 of the non noble gases fission products.

The last stage of the defense in depth is directly related to the protection of the population and of the environment, with emergency planning providing for possible evacuation in a 5 km radius and possible sheltering in a 10 km radius, and for temporary restrictions (less than a week) on drinking-water.

In short, the cocktail of passive and active features, of man and machine, mixed in a defense in depth approach, yield, in the present French NPP's, satisfactory results. The global core damage probability of about 10^{-5}/reactor-year (and accident management significantly reduces the probability of severe accident) complies with the generally agreed safety objective, and the maximum release of fission products after a severe accident -less than 1 % of what it has been at Tchernobyl- is consistent with manageable off-site emergency planning.

Moreover, this global result is obtained in a balanced manner : there is no dominant failure path family with a probability greater than 1 or 2.10^{-6}. This is a direct consequence of the feed-back of experience which has led to implement additionnal systems and (or) procedures whenever there was a dominant failure path.

3. WHERE DO WE GO FROM HERE ?

Is there, then, a need for further progress ? If so, in what direction ? And at what cost ?

As has been shown above, there are really no objective reasons to look after quantitative improvements. There are, in fact, a number of reasons not to. One of them is the difficulty in demonstrating quantitatively a global safety objective much smaller than 10^{-5}, due in particular to common mode or common cause failures, both for internal events as discussed above, and for external events such as fires and earthquakes. Another reason is that such an objective would be difficult to justify economically, even for a utility having a very large number of units (such as Electricité de France). **But most of all, there is a very remote chance that a lower figure be more credible than today's, and enhance public acceptance.**

What we need today are more qualitative improvements :

- bring a better demonstration -to the public- that radioactive releases will be kept under control whatever the core damage,

- avoid, as far as possible, near scares, due to events rated 3 and above in the French scale of gravity [5] (such as the loss of batteries in a Bugey unit in 1984, uncontrolled steam generator tube ruptures, or the small interfacing LOCA in Biblis A),

- avoid, particularly, such events due to human error.

The first improvement will come from R and D on severe accidents, an area where international cooperation is of prime importance. But it also will be necessary to show that the results of R and D are properly applied to each individual unit, whether new or already in operation, always keeping in mind the defense in depth approach -that is the possibility of failure of successive barriers.

The other improvements concern more, perhaps, the plants now in operation than the future plants. They call for an enhanced safety culture and excellent operation management. Exchange of operating and management experience between utilities, through an organisation like WANO, will play a major role in this area. But we shall see in the next chapter that they also concern future designs, particularly in looking for simple operation and reliable systems to cope with frequent events.

4. WHAT, THEN ?

During the last few years, discussions on future light water reactors turned about two types of reactors : evolutionary and revolutionary. The first type would be derived from present large scale units such as N4, Konvoy or Sizewell. The second type would need prototypical development (PIUS, ISER). In between, such reactors as the AP 600 or SB 600 claim that they can benefit from the experience of existing units and do not require a prototype.

The most obvious path for future French (or European) light water power plants is to use the feed-back of experience to improve the N4 (or equivalent) design. A major part of this feed-back of experience will come from advanced light water reactors in Europe and Japan, but the 400 or so plants represented in WANO will also contribute. The three most important areas under consideration are (1) **defense in depth** (again !), (2) **more forgiving operation** and (3) **the role of man** :

(1) Defense in depth

One of the best ways to improve the first level of defense in depth is to have more reliable components, such as instrumentation, valves, pumps, ... [6] ; this is particularly true of steam generators and secondary side piping and valves, since today interfacing LOCAS account for nearly 25 % of core damage sequences.

For the protection of the first and second barrier, a balanced use of both passive and active systems seems appropriate, as seen in chapter one. The main objective here is to cover the whole spectrum of events, from normal operation to severe accidents, both to simplify operation and decrease the occurrence of intermediate types of abnormal events. Examples of this are : a moderale increase in the pressuriser volume which will decrease sollicitations of the pressuriser relief valves, an increase in the pressure rating of the steam generators which will simplify the protection of the S/G's against overpressure,...

. Although not a panacea, a strong containment is certainly one of the strongest arguments to convince the public that plants are safe, and is not very expensive, particularly when the pre-stressed concrete technique is used as it is in French plants.

. Future designs may also carry improvements in the containment vent and filter.

(2) **More forgiving operation** : This is certainly one of the most difficult objective in complex systems, as potential human errors are somewhat difficult to identify. A good defense in depth will of course help to limit the consequences of human error. Operating experience also shows that one of the best ways to reduce the risk of human error is to simplify operation, and particularly to have longer grace periods during which no operator action is required. This can be obtained in several manners :

. *greater autonomy of cold sink, of DC source (particularly in case of station* black-out), of pressuriser volume,...

. automatic actions for both active and passive systems,

. use of passive systems with accumulated energy (gravity, pressure accumulators, batteries, steam,...),

. increase in some margins,

...

(3) **Enhanced role of man,** with proper operator aids.

Such a future reactor should bear a strong resemblance to todays, much as the Airbus A 320 or the Boeing 767 look much like former models. But this external resemblance should not prevent major technological steps, such as the improvements in control and instrumentation which concern both modern aircrafts and modern nuclear plants. It certainly will not prevent a large number of small steps directly inspired by the feed-back of experience.

Another possible path for future French or European light water plants could be the simplified passive designs, such as the AP 600. There is clearly a convergence in objectives with our own, with similar safety objectives and similar economic objectives. It seems premature at this stage either to applaud or to condemn these designs. I shall simply state here some of the questions which will have to be answered by the designers to the satisfaction of prospective buyers :

. cost, compared to large size units,

. overall balance between preventive and mitigating measures (whether active or passive) for all categories of severe accidents ; particular attention will have to be given to all the failure paths not directly related to decay heat removal, such as interfacing LOCA's, ATWS, accidents initiated during reactor shut down, and to accident management in case of core melt,

. reliability analyses for lower severity but more frequent abnormal events,

. reliability data for passive components,

. *comparative PSA with evolutionary advanced light water reactors.*

The assessment of such designs compared to more evolutionary designs is encompassed in the REP 2000 program launched by EDF.

5. CONCLUSION

The present Workshop brings evidence of the international character of reactor safety. This is clearly the case for feed-back of experience where we all learn from problems anywhere, but where one also should learn from successes. It is also the case for safety objectives and methodology, as shown by the INSAG 3 report [7] and, regionally, by the European Commission report [1]. It will most probably be the case for the design of future plants.

In Europe, except for a few units under construction or under planning in the UK and in France, future plants are expected to be built in the latter part of the 90's or the early 2000's, and will be needed then to replace the earlier units commissioned in the 70's and to be decommissioned after 30 to 40 years of operation. Safety objectives and rules will have been harmonized by then, perhaps at a world level but at least in Europe, under the pressure of utilities, of manufacturers and of the safety authorities. A first step in this direction has been taken by the French and German governments last June. Further steps will be taken by the European nuclear utilities to share both their experience with operating plants and the analysis of their future needs and requirements.

It is too early, today, to announce what these requirements will be as far as safety is concerned, as competing designs have yet to be evaluated and this could take another two or three years. But looking into the crystal ball, I would guess that Europeans will require that future plants take full benefit, in a balanced manner, of the feed-back of experience, of both passive and active systems, of the active possibilities of man, in a global defense in depth approach and in depth safety culture.

REFERENCES

[1] P. BACHER, J.P PELE - Convergences of approaches to safety in the member states of the European Community - NUC'SAFE - Avignon 1988.

[2] Probabilistic Safety Assessment - REP 1300 - to be published.

[3] The French White Book for PWR Nuclear Safety - 1987 - Electricité de France.

[4] Severe accident risks : an assessment of five US NPP's - NUREG 1150 Vol 1.

[5] The French scale of gravity - Bulletin SN number 58 - March/april 1988 - Ministère de l'Industrie.

[6] L. REYNES - Design for operation ? Design for survival ? Are both objectives achievable ? - ANS Topical Meeting, Albuquerque, New-Mexico - September/October 1986.

[7] IAEA Safety series - n° 75 - INSAG 3 - Basic Safety Principles for Nuclear Power Plants

SAFETY ASPECTS OF ADVANCED LWR DESIGNS IN THE FEDERAL REPUBLIC OF GERMANY

H. MÄRKL
Siemens AG,
Unternehmensbereich KWU,
Erlangen, Federal Republic of Germany

Abstract

Lack of public acceptance in most of the industrialized countries presently impedes expansion of nuclear energy Regain and reestablishment of public acceptance demand safety performance improvements appropriate to convince the public that the risk of occurrence of a severe accident will be further decreased and, in addition, that even an accident sequence exceeding the design basis will not expose the environment to an unacceptable radiological impact

Probabilistic risk analysis has proven to be an excellent guiding instrument for identifying safety improvement needs

The recently commissioned 1300 MW Konvoi PWR plants have already achieved a highly acceptable level of safety, the frequency of an accident event not coped with by the safety systems amounting to approximately 1 4 x 10^{-6} per year

Following a predominantly evolutionary way of safety improvements the proven safety features are to be maintained also for the next generation of NPPs since one of the most important criteria of design advance is reflection of operating experience and incorporation of proven technology

In addition, however, some potential safety performance improvements merit consideration, especially in the following areas

- A novel I & C system using exclusively digital microprocessor-based technology as, e g ,presently under advanced development at Siemens will contribute markedly to further improve man-machine interface performance
- Implementation of preventive accident management or equivalent design measures to maintain core coolability and pressure vessel integrity after incipience of an event exceeding the design basis
- Exploration and elaboration of mitigative accident management measures and/or provision of precautionary design measures to maintain containment integrity even in course of a core melt accident

Implementation of such safety improvements will practically exclude occurrence of a severe accident with unacceptable radiological consequences to the environment.

1. INTRODUCTION

In spite of the tendency of certain energy supply saturation phenomena oberservable in some highly industrialized countries there is undoubtedly a fast increasing energy demand to be anticipated for the coming decades

Due to the rapidly growing awareness that continuation of CO_2 emission at the present or even an enhanced level will lead via the green house effect to a highly alarming climate change, construction of fossil fueled power plants will have to be decisively limited and, as a result, due to lack of alternative energy sources, the share of nuclear power will have to be increased correspondingly.

On the other hand, however, lack of public acceptance in most of the industrialized countries - with the apparent exception of France - presently impedes or even prevents expansion of nuclear energy markedly. Thus, regain and reestablishment of public acceptance is the paramount prerequisite for a viable renaissance and revival of nuclear power

The strong sentiment against nuclear power emerged in the late 1970s. The accident at Three Mile Island (TMI) in March 1979 must be considered to have marked a profound impact on or even a decisive turning point in the perception by the public of the nuclear power risk, although the TMI containment held and, thus, the radiological consequences to the environment were negligible.

The Chernobyl reactor accident in April 1986, although, in contrast to TMI, resulting in a sizable activity fallout, did not create a completely new type of nuclear issue, but it acted as a strong catalyst to the antinuclear movement violently shaking or even dissolving public confidence in nuclear power. The effects of the Soviet accident were particularly dramatic in some western European countries like Holland, Italy, Switzerland and West Germany, where plans to add nuclear power capacity had to be shelved. A new nuclear accident of a comparable impact, no matter where in the world it should happen, would practically mean the knock-out of nuclear energy utilization. Hence, there is a need for safety improvements not only for the next generation of nuclear power plants, but for the operating NPPs as well

An increasing tendency of international exchange of experience and cooperation in the field of reactor safety holds out hopeful and promising prospects of creating sort of an international nuclear safety partnership.
It will have to be accompanied by a corresponding gradual harmonization of safety and licensing standards. The 'Basic Safety Principles for Nuclear Power Plants' [1] worked out by the International Nuclear Safety Advisory Group (INSAG) on behalf of IAEA can be considered to be a valuable and promising starting point in this regard.

Clearly, the dominant motive and objective of and the driving force behind the worldwide efforts to enhance LWR safety for the next generation of NPPs is to overcome the public acceptance crisis.
For meeting this objective one group of nuclear proponents suggests pursuit of revolutionary design changes relying to the maximum extent possible on inherent and passive design features which have for the most part not yet been built
Another group prefers an evolutionary approach also considering passive and inherent design characteristics whereever reasonably practicable but claiming descent from and not giving up the solid experience base achieved with existing proven reactors.

2. GENERAL REMARKS ABOUT INHERENT AND PASSIVE SAFETY

Inherent and passive safety features have been applied in current LWR designs to a remarkable degree already [2, 3]

Examples for inherent safety characteristics:

- Shutdown of the nuclear chain reaction upon loss of coolant due to negative void reactivity feedback
- Gravity induced control rod drop
- Leak-before-break criterion that precludes, under certain criteria, a sudden failure of the pressure-retaining boundary

Examples for passive safety features:

- Accumulator safety injection of PWRs
- Isolated reactor containment
- Residual heat transport from primary to secondary circuit by means of natural convection

Passive and inherent safety features are worthwile being considered to an enhanced degree in the future whereever reasonably practicable and consistent with the requirements of operational targets.

In the past couple of years, however, numerous publications and papers presented at nuclear conferences have tried to raise the impression that the requirement for enhanced NPP safety and resulting public acceptance improvement could only be met by applying more or less exclusively passive or inherent safety features.
The usage of the term inherent safety has caused a lot of confusion to the technical community, a rise in the expectation horizon of politicians and valuable argumentation support or even ammunition to nuclear opponents since the term 'inherent safety', according to common-sense public

understanding, has often been instinctively interpreted as absolute safety, an expectation that can be quite misleading.

The various reactor types differ in kind and also in variety of inherent and passive safety features usable or used for design. But it is essential to point out that no entire reactor plant is inherently safe as a whole. [4] The use of the attribute inherent has to be restricted to certain properties of a reactor that can provide inherent safety against certain postulated events. Hence the term 'inherently safe' can be used only in such a limited qualified way as 'inherently safe with respect to...'.

Furthermore, an inherent safety feature may exhibit quite an ambiguous effect. In a reactor having negative reactivity feedback characteristics rising coolant temperature decreases reactivity, whereas decreasing coolant temperature resulting e. g. from overcooling transients can lead to an undesired reactivity increase or even excursion.

What can be considered to be the real virtue or merit of inherent and passive safety features? It can be expected to have a high availability, i. e. a low unavailability. There is certainly a good deal of truth in this assumption. But can the unavailability of an inherent or passive safety system be assumed to be zero? Certainly not, since it will be available as far as mechanical and functional design on which it is based maintains its integrity during the accident. Thus, the unavailability of an inherently or passively safe component or system will not be zero, rather a finite value will have to be attributed to it. If so, the old question arises, in case there is no absolute safety, how safe is safe enough, or, how large can the unavailability of safety systems be tolerated to be?

Even if availability and reliability characteristics of passive and inherent safety features would be superior to those of properly designed active engineered safety mechanisms, one must not disregard the fact that, where reliance is placed solely on inherent safety features or purely passive engineered safety mechanisms, it would not be possible to the operator to turn off the process after a spurious actuation or to influence the final condition of a transient. Optimization of operation and of operational interaction under upset conditions requires the existence also of active systems designed according to deterministic rules.

Hence it follows that only a rational combination of readily chosen inherent and passive safety characteristics and properly designed and proven active engineered safety features-based on the principles of redundancy and diversity - will promote achievement of a high degree of reliability and operability of a NPP.

3. PROBABILISTIC RISK ANALYSIS AS A GUIDING INSTRUMENT FOR IDENTIFYING SAFETY IMPROVEMENT NEEDS

Probabilistic risk analysis (PRA) can be and in the FRG always has been considered to be a top-level technical means of providing valuable information on functional interdependences between the various systems and on identifying relative weak points in design, thus offering an excellent basis for safety performance improvements.

Two months ago the German Risk Study Phase B performed by the Gesellschaft für Reaktorsicherheit (GRS) on behalf of the Ministry of Research and Technology (BMFT) has been officially released.[5] Already the findings of the predecessor Phase A study, based on assumptions comparable to those formulated in the US reactor safety study, WASH 1400, were used to systematicly eliminate by adequate backfitting measures those accident paths showing an undue contribution to the overall risk. As a result, a balanced overall safety concept was reached in which the risk is not dominated by specific failure modes or individual accident event paths.

Phase B represents a refinement and an amendment compared to Phase A regarding, e. g.,

- Completeness of accident analysis taking into account further initiating events
- Improvement of severe accident analysis taking into account recent results of safety research
- Inclusion of accident management measures to be implemented by the NPP staff to prevent a core melt and/or to mitigate the consequences after an accident sequence has started or a core-melt event occurred.

Table I: INFLUENCE OF ACCIDENT MANAGEMENT (AM) MEASURES ON THE FREQUENCIES OF ACCIDENT SEQUENCES UNCOPED WITH BY SAFETY SYSTEMS ACCORDING TO GERMAN RISK STUDY PHASE B

Initiating Event	Without AM		with AM	
	LP (1/a)	HP (1(a)	LP (1/a)	HP (1/a)
Loss of Coolant Accident				
- small Leak in the RCL	6×10^{-7}	4×10^{-6}	2×10^{-6}	4×10^{-8}
- Small Leak in the Pressurizer		3×10^{-6}	1×10^{-6}	3×10^{-8}
- Steam Generator Tube Failure		1×10^{-6}	3×10^{-7}	1×10^{-8}
- Leak in Connecting Line	1×10^{-7}		1×10^{-7}	
Transients				
- Plant Internal Transients		2×10^{-5}		2×10^{-7}
- ATWS		2×10^{-7}	1×10^{-7}	1×10^{-7}
General Impacts				
- Internal Fire, Flooding		7×10^{-7}	7×10-7	1×10^{-8}
- Earthquake		3×10^{-6}	1×10^{-6}	3×10^{-8}
TOTAL	1×10^{-6}	3×10^{-5}	5×10^{-6}	4×10^{-7}

Table II: CHARACTERISTIC INTERVENTION TIMES AVAILABLE FOR PREVENTIVE ACCIDENT MANAGEMENT (AM) MEASURES BEFORE INCIPIENCE OF SEVERE CORE DEMAGE

Transient	Reactor Trip	Steam Generator Dry-out (hrs)	Primary System Dry-out (hrs)	Start Core Melt (hrs)	RPV-Failure (hrs)
Station Black out	Speed Main Coolant Pumps low	1	2	2,8	3,2
Loss of Feedwater	SG-Level low	0,4	1,4	2,2	2,6

The most important results of the German Risk Study Phase B performed for the 1300 MW reference plant Biblis B are as follows:

- The overall frequency for accident sequences not coped with by the design basis safety systems amounts to 3×10^{-5} per year, three times lower than in the Phase A study. (Table I)
- Quantification of the high degree of conservatism of the safety systems confirmed considerable safety margins (minimum systems requirement for accident control appreciably lower than demanded in licensing procedures).
- Identification and quantification of available intervention times (grace periods) for performing accident management (AM) measures (Table II).
  AM measures reduce the severe accident probability by an order of magnitude from 3×10^{-5} to 4.5×10^{-6} per year.
  Should an accident not coped with by the safety systems occur, there is a 90 % chance that AM measures will restore core cooling, a 10 % chance that the measures will fail and result in a low pressure core melt, and a ~1 % chance that AM would fail and result in a high pressure core melt that could potentially lead to early loss of containment integrity.

By far the dominant contributions to the beyond design events result from non-LOCA transients (> 60 %) and from small break LOCAs (~ 25 %) The accident sequences uncoped with result predominantly from postulated failure of heat removal via the steam generators, i e., loss of the main heat sink combined with the loss of main feedwater, leading to uncontrolled high pressure conditions within the primary circuit that constitute the main subject of preventive AM measures

In the Federal Republic of Germany, the required nuclear safety standard has never been considered to be of a static nature, rather, a dynamic approach has always been taken in the sense that new findings resulting, e g , from operating experience, from safety research and development results or from probabilistic safety analyses, had to be and were fed back into new designs and retrofit into operating plants in the shortest possible period of time Hence, following the German Risk Study Phase A, numerous safety related improvements have been carried out, referring, e g , to

- decoupling of operating from safety systems
- physical segregation of redundant subsystems
- increase in redundancy and capacity of steam generator feed system and main steam removal system
- enhancement in degree of automation
- energy supply security
- human factor engineering

As a result, for the more recently commissioned 1300 MW Konvoi plants the probability of occurrence of an accident sequence beyond the desgin basis has been assessed on the basis of realistic assumptions for minimum systems requirements to be as low as $1\,4 \times 10^{6}$ per year, without regard for AM measures

Striving for further improved safety standards of the next generation of LWRs must not disregard the safety standard achieved with current LWRs based on an enormous background of operating experience feedback, safety research results and licensing practice
Since no new concept or redesign of an old concept can be based on this depth of experience it would be an irreversible mistake to leave this solid experience base completely and head for a potentially uncertain future
On the other hand, it would be neither justified nor prudent to lean back and to be happy with what we have achieved Safety has to be considered to be of a dynamic nature meaning that improvements of safety and reliable operation have to be performed in a predominantly evolutionary way whenever the need for such improvements is recognized. If, however, a major safety deficit should be discovered, deviation from a purely evolutionary approach is not to be ruled out a priori

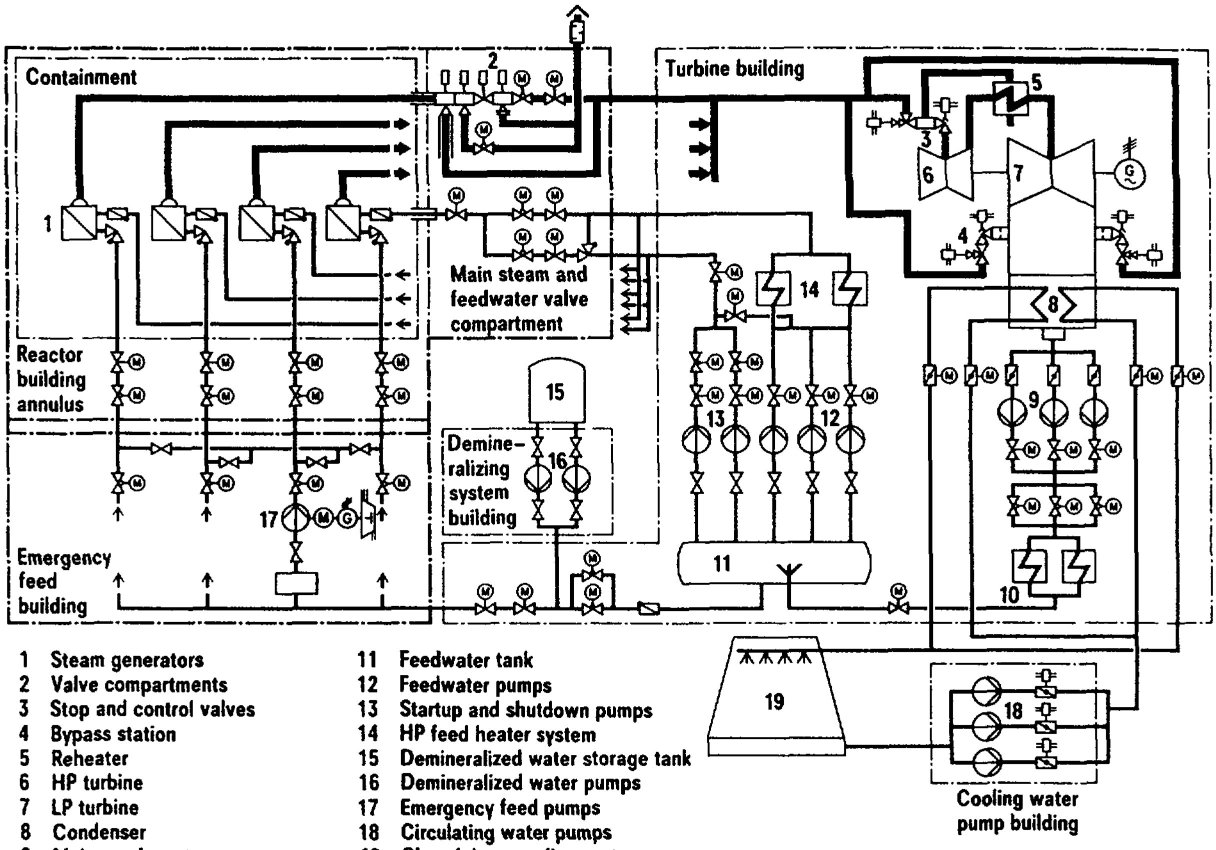
4. SAFETY CONCEPT OF THE NEXT GENERATION OF PWRs

4 1 ADVANCED SAFETY CHARACTERISTICS OF THE 1300 MW KONVOI NPP GENERATION

As mentioned in chapter 3, for the recently commissioned Konvoi NPPs the frequency of occurence of an accident sequence beyond the design basis, i e , of an accident event not coped with by the safety systems, has been assessed to be as low as $1\,4 \times 10^{6}$ per year, not taking into account AM measures that can be effectively used to prevent severe core damage even if the accident exceeds the design basis This would readily meet or even surpass the probabilistic safety objective as generelly agreed upon and as laid down, e g , in the EPRI specification for the ALWR Utility Requirements Documents [6]

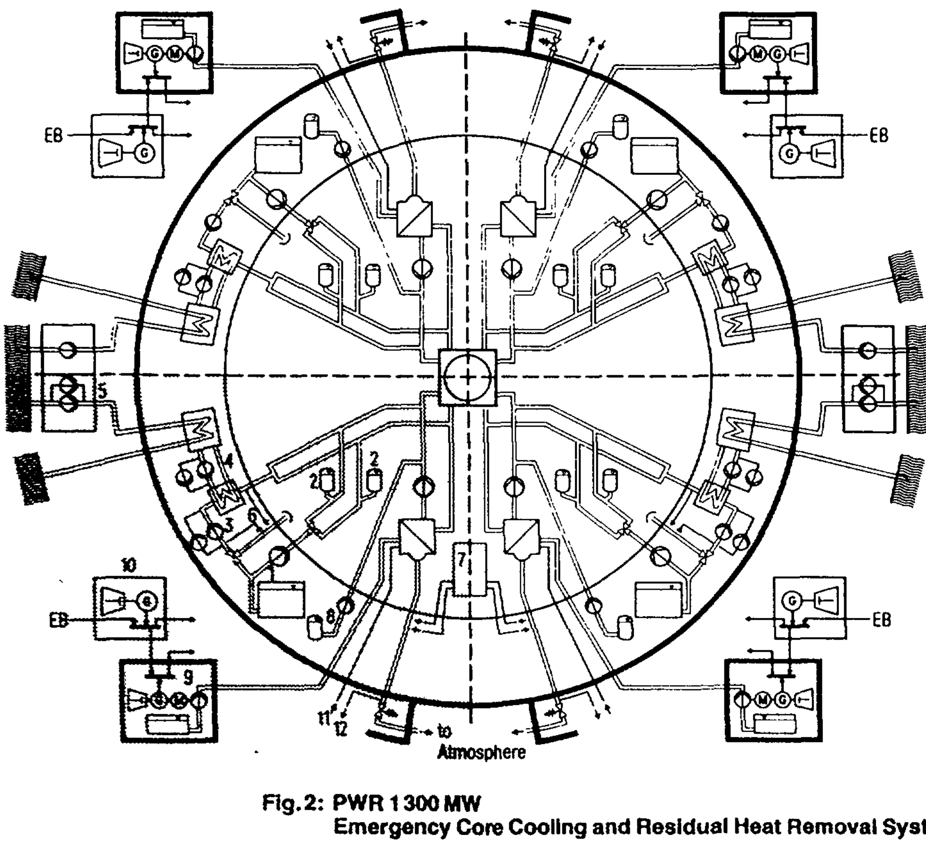
In endeavouring to adequately improve NPP safety further it appears appropriate to base the required scrutiny on the safety level achieved with the latest class of NPPs built and commissioned, the 1300 MW_e 4-loop PWR NPPs [7]

In the FRG the design of the safety systems has never been limited to cope only with a double-ended main coolant pipe break as the maximum credible accident.
Rather, as soon as in the early seventies small break LOCAs have been perceived as a source of higher potential risk This recognition resulted in requirements for reliable fast primary circuit cooldown and residual heat removal through the steam generators (SG).



1 Steam generators
2 Valve compartments
3 Stop and control valves
4 Bypass station
5 Reheater
6 HP turbine
7 LP turbine
8 Condenser
9 Main condensate pumps
10 LP feed heater system
11 Feedwater tank
12 Feedwater pumps
13 Startup and shutdown pumps
14 HP feed heater system
15 Demineralized water storage tank
16 Demineralized water pumps
17 Emergency feed pumps
18 Circulating water pumps
19 Closed-loop cooling system

Fig. 1: PWR 1300 MW
Systems for Secondary Side Heat Removal



1 High pressure safety injection system
2 Acumulator
3 Low pressure RHR-system
4 Intermediate cooling system
5 Auxiliary service water system
6 Integrated fuel pool cooling system
7 Spent fuel pool
8 Extra borating system
9 Emergency feedwater system
10 Auxiliary diesel generator
11 Feedwater
12 Main steam line

EB Energy supply via house load

Fig. 2: PWR 1300 MW
Emergency Core Cooling and Residual Heat Removal Systems

Consequently, the SGs have to have a reliable supply of feedwater and a corresponding steam dump capacity, resulting in highly redundant systems design.Fig. 1 shows the secondary side heat removal systems existent for a 1300 MW PWR plant:

- a 3 train main feedwater system
- a 2 train startup and shutdown feedwater system with emergency power backup
- a fully independent 4 train emergency feedwater system with dedicated Diesel engine drive as part of the self-sustained so-called 'bunker-system' that protects against external events like airplane crash and gas explosion blast wave.
- 4 steam dump stations each dedicated to one steam generator

The emergency core cooling and residual heat removal system (ECCS) is shown in Fig 2.
It consists of:

- a 4 train high pressure safety injection system
- a 4 train low pressure safety injection and residual heat removal system
- 2 x 4 = 8 accumulators injecting water into both cold and hot legs of the primary circuits (combined injection).

Each of the four loops has a dedicated borated water storage tank with a capacity of 450 m^3

The 4 trains are consistently required to be physically and spatially separated from one another in order to avoid common cause failures.

In general, a four train redundancy for all safety systems is being applied meeting the so-called (n + 2)-redundancy demand where n is the minimum number of required systems and the two additional redundancies account for a postulated single failure and the repair case.
Due to the conservatism designed into the safety systems the minimum requirements for emergency core cooling, residual heat removal and primary circuit depressurization via the SGs would be readily met by typically only one out of the four redundant systems

Fast primary circuit cooldown through the SGs with a rate of 100 K/h required to cope with small break LOCAs and certain rare non-LOCA transients is automatically initiated thus avoiding manual measures in meeting the so-called 30 minutes licensing criterion required by the German licensing rules, according to which safety systems shall be designed such that manual intervention must not be demanded within 30 minutes after accident initiation. This licensing rule generally resulted in a reasonably high degree of automation relieving the operator from the need to react quickly and under stress conditions

Similarly, the so-called 10 hours autarky criterion has to be met: In case the control room, e. g., due to external impact, is not in a functionable state, it has to be assured that the emergency systems are able to transfer the plant into a safe state without the need for manual intervention, and that the plant is capable of remaining in this state for at least 10 hours

The risk of large scale loss of primary coolant through the coolant pump shaft seals following, e. g., a station black-out transient, is ruled out with long term efficiency due to the existence of standstill seals in the primary coolant pumps.

Concerning station power supply, supplementary to the 380 kV main power supply system a 110 kV reserve power supply system has been provided for with automatic changeover from the main to the reserve supply system

Licensability in the FRG in contrast to other countries, includes consideration in design of rare external events such as supersonic military aircraft crash and blast wave
As a result, all safety systems are therefore protected against external impacts by thick penetration proof walls

Progress has been achieved also in the area of man-machine interface by increasing diagnostic aids
E g , in addition to loose parts, vibration monitoring and leakage detection systems a pressure vessel level monitor has been introduced that is being integrated into the automatic reactor protection system

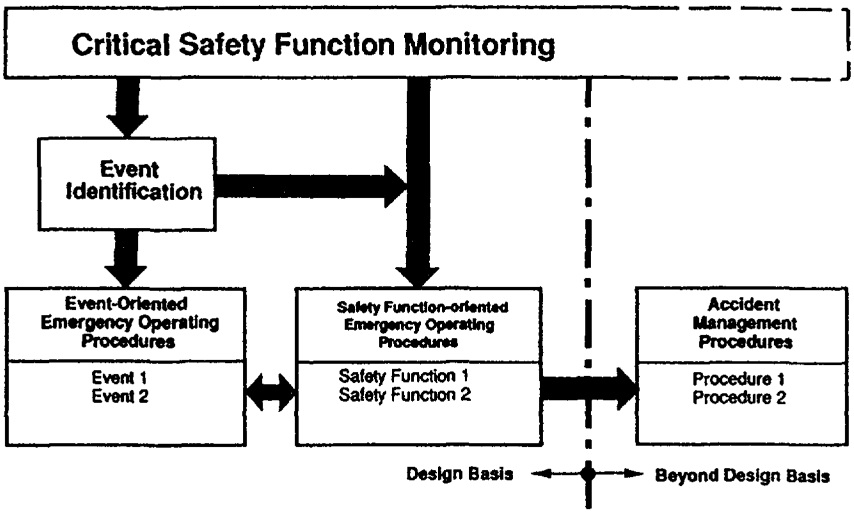


Fig.3: Emergency Operating Procedures for SIEMENS-KWU-PWR

The emergency operating procedures have been augmented to better account for not easily identifyable transient events (Fig 3)
If the operating personnel succeeds in making a correct accident diagnosis, i. e. identifying the accident cause and event sequence, the plant can best be brought into a long-term safe condition by means of so-called event-oriented strategy programs that have always been part of the emergency operating procedures (EOP) contained in the operating manual. In case unambiguous event identification is not possible, safety function oriented procedures also provided in the operating manual will be applied These procedures ease fulfilment of the critical safety functions, e g reactivity control, primary coolant inventory and secondary heat sink as well as radioactivity control

Qualified operator interaction is decisively facilitated if it can be based on computer aided diagnostic capabilities.
Such a computer aided process information system named PRISCA™ has been installed in the recently commissioned Konvoi NPPs [8]
Four distributed data acquisition computers located in the four rooms of the redundant instrumentation and control (I & C) equipment sample about 2500 analog and approximately 14 000 binary signals and transmit them to the two data processing computers These two host computers feed 30 visual display unit (VDU) controllers and several other recording devices, i e each VDU is driven by a separate controller, a 32 bit micro-processor of modern design

The VDUs together with their controllers and their host have full-graphic features
Various types and formats of pictures and displays are selectable to generate and store roughly 1000 different pictures with widely varying complexity and content, e g. systems diagrams for status information, curves and trajectories for trend information, display of safety function status .

The quality of the proven safety features that have been described in this subchapter are to be maintained also for the next generation of PWR NPPs, since one of the most important criteria of design advance is reflection of operating experience and incorporation of proven technologies

In addition, however, some potential safety performance improvements merit consideration, especially in the following three areas

- Novel I & C system using exclusively digital micoprocessor-based technology

- Implementation of preventive accident management or equivalent design measures to maintain reactor pressure vessel (RPV) integrity after incipience of a beyond design event, particularly following high pressure transients

- Exploration and elaboration of mitigative accident management measures and/or provision of precautionary measures to maintain containment integrity after a core melt-down accident

Downsizing of power output is not being considered to be required to enhance safety performance. 1300 MWe units already representing a high level of safety offer the potential for achievement of further safety improvements to a wholly acceptable extent.
Smaller units are being looked at for countries or utilities that expect a need for capacity addition in smaller increments than in the past.

4.2 INNOVATIONS IN ADVANCED INSTRUMENTATION AND CONTROL (I & C) SYSTEMS USING MICROPROCESSOR-BASED DIGITAL TECHNOLOGY

The next generation of LWR NPPs to be built in Germany will make full use of a development well underway at Siemens characterized by and directed toward introduction of a microprocessor-based digital I & C system to be applied not only in the non-safetey rélated operational I & C but also in the I & C systems important to safety. [9] 'Intelligent' digital computer systems replacing previous hardwired analog technique will take over supervision and control of the entire plant during both normal operation and accident events.

Reactor plant I & C design follows essentially the hierarchical defence-in-depth philosophy as practiced in the Konvoi NPPs maintaining the three step categorization:

- non-safety grade operational controls
- safety-grade limitation functions that return parameters to nominal values or prevent further deviations overriding, if necessary, operational controls and manual actions
- safety-grade reactor protection system that actuates the redundant engineered safety systems overriding, if necessary, the limitation system

In applying this advanced digital I & C most stringent requirements regarding both hard and software reliability and verification will have to be met particularly for the safety relevant I & C.

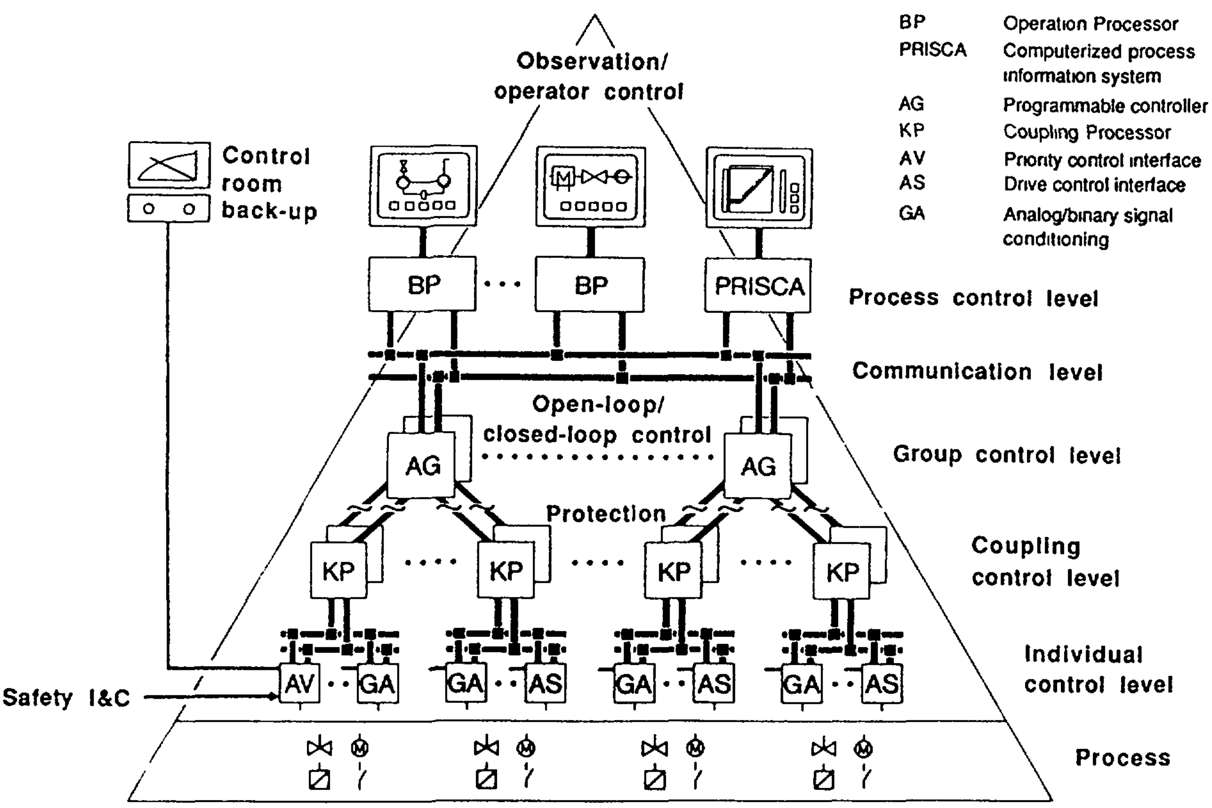


Fig. 4: Structure of Digital Operational I&C (BELT-D) for NPPs

Decentralization of signal processing and drive control in conjunction with electrical and fiber optic data busses will contribute to limiting the consequences of common cause failures and to reducing drasticly number and quantity of cable trays .

Failure recognition and elimination is facilitated through enhanced self-checking (parity-check, watch-dog) and by using integrated test computers for automatic diagnostics.

The hierarchical structure and architecture of the operational I & C is shown in Fig. 4.

Particularly great innovation and progress have been achieved in the areas of observation, information and operation systems that are part of the process control level. These subjects are closely related to human factor engineering and man-machine interfaces.
The computer aided process information system PRISCA™ as described in the previous subchapter will be an integral part of the process control level.
Process observation and process operation will be performed with a special type of screen, a touch sensitive plasma display.

Commands are entered by touching elements and symbols depicted on the plasma display and simultaneously releasing them.

The command processor consists of a 32 bit computer with high computational capability and a 32 Mbyte random access memory (RAM). It has two interfaces to the redundant process bus of the communication level.
Touch-sensitive screens are particularly suitable for use in process control because direct manipulation gives the operator the feeling of participating more directly in process events and narrows the gap between the operator's thoughts and the physical conditions in the system being operated.

Conventional control room technology based, as of today, on mini-module techniques with extensive use of coloured mimic diagrams set up on desks and panels will in the next nuclear power plant generation be replaced by a cockpit type of control room with exclusive use of visual display units (VDU) and extensive use of computer capacity.

Fig. 5 shows a control room arrangement and architecture of future NPPs of Siemens design. The information panel is located in front of the operator panel. The number of VDUs of PRISCA™ will be markedly increased.

4.3 PREVENTIVE ACCIDENT MANGEMENT MEASURES TO MAINTAIN REACTOR PRESSURE VESSEL INTEGRITY IN BEYOND DESIGN EVENTS

In the FRG there has been a traditional adherence to two key safety principles:

- The multiple barrier concept with several fission product barriers acting in series. The containment is designed as a leak and pressure tight spherical steel shell surrounded by an outer concrete shield building acting as a protection against external events, with the accessible annulus in between housing the emergency core cooling systems.

- The multi-level defence-in-depth safety concept as illustrated in Fig. 6.
  The measures to be taken within the first three levels are required to prevent to the highest possible extent the occurrence of any accidents, particularly severe accidents.The compliance with this safety objective is subject to the rigid licensing requirements.

Deterministic safety design and corresponding accident prevention will continue to be a high priority objective. As a result, accidents beyond the design basis will be extremely unlikely - the estimated probability for the occurrence of a beyond design event being approximately 1.4 x 10^{-6} per year for the as-built Konvoi NPPs.

An integral frequency of $\leq 10^{-6}$/year for accident sequences not coped with by the safety systems appears to be a desirable and realistic target also for future LWRs.

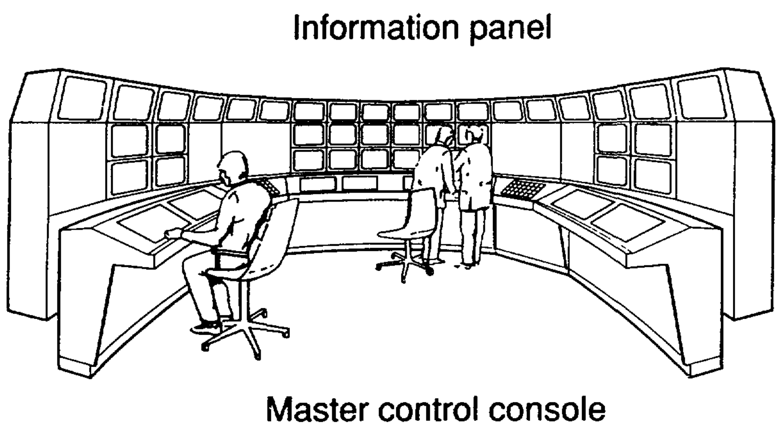


Fig. 5: Visual Display based Control Room for NPPs (Draft)

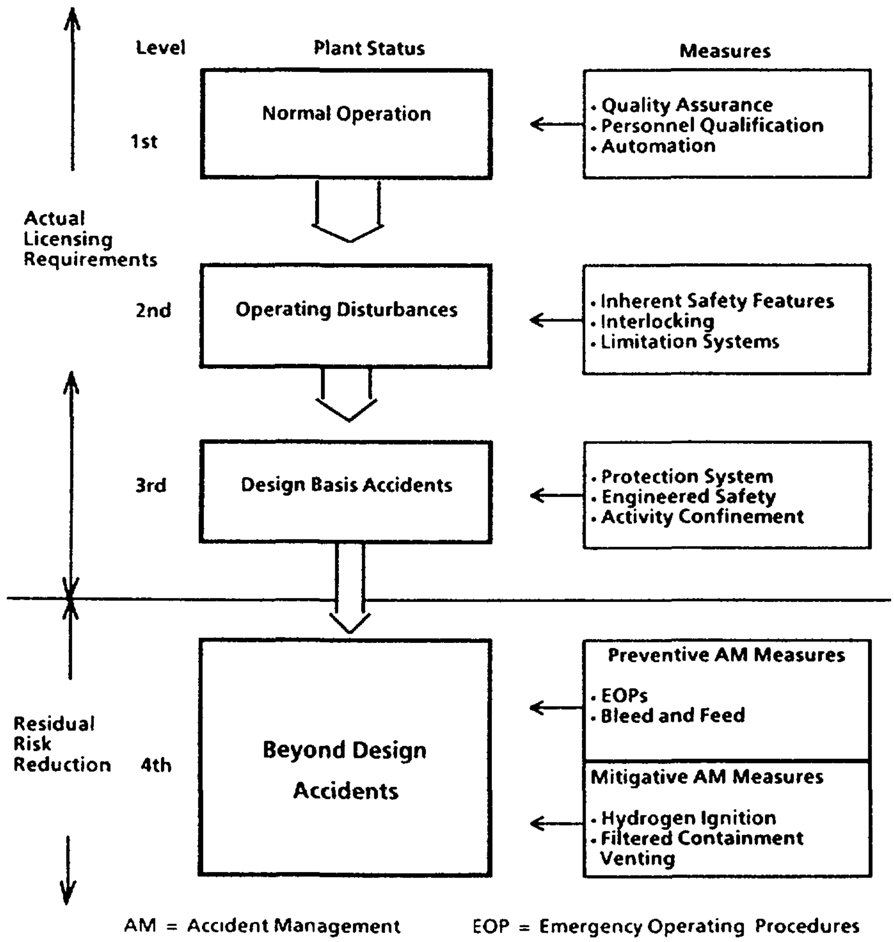


Fig. 6: Multilevel Defence-in-Depth Nuclear Power Plant Safety Concept

The German Risk Study Phase B clearly revealed that event sequences not being coped with by the safety systems will not necessarily result in a core meltdown

Preventive AM measures offer the potential to restore core coolability in incipient beyond design events and to reduce the probability of occurrence of a core melt-down by an order of magnitude leading to an integral core melt frequency of ~ 10^{7}/year.

Mitigative AM measures, as described in the next subchapter, will additionally reduce the probability of occurrence of a severe accident with unacceptable radiological consequences to the invironment to a value of the order of ~ 10^{8} per year. This, according to the rules of practical good sense, can and should be considered to be deterministicly safe.

AM measures can be initiated and performed through appropriate operator intervention based on flexible use of both non-safety grade operating systems and possibly still available safety systems. For such AM measures to be reliably effective two prerequisites are to be met·

- Simplicity of the operator actions to be taken
- Period of time before operator intervention is required (grace period) to be sufficiently long

The objective of preventive accident management measures is to maintain a coolable reactor core configuration thus avoiding severe core degradation and, as a consequence, loss of reactor pressure vessel (RPV) integrity

AM measures have therefore been added as a fourth level within the multi-level defence-in-depth concept (Fig 6) exhibiting a broad scope of intervention potential for further reducing residual risk.

As stated in chapter 3, a particular effort has to be made to combat those beyond design transients that could lead to core melt sequences under high primary circuit pressure condition potentially resulting in early loss of containment integrity

By far the dominant contributions to this type of beyond design events result from transients due to loss of heat removal function via the steam generators as, e. g , loss of main heat sink in conjunction with loss of main feedwater

The appropriate AM procedure to be applied for temporary compensation of the failed function [10, 11] is bleed and feed (B & F) with priority given to secondary-side B & F.

In a first step the feedwater tank, a component existent in all German NPPs, is pressurized via the pegging steam system Subsequently the SGs are depressurized via the steam dump valves

In a second step the content of the feedwater tank is fed into the SGs The feedwater volume available in the feedwater tank can maintain feedwater supply for more than two hours Longterm feed can be provided by a mobile pump via a nozzle to be installed at an accessible location

Alternatively or in addition to secondary side B & F, primary-side B & F measures can be taken to reduce the primary system pressure by opening the pressurizer relief valves enabling consecutively high pressure safety injection (≤ 11 MPa), accumulator injection (≤ 2 5 MPa) and low pressure injection (≤ 1 0 MPa)

Practically all non-LOCA transients and small-break LOCA events leading without recovered heat removal to core melt sequences under high pressure can be avoided or at least be transferred to a low pressure scenario by applying these two B & F procedures

Reassessment of certain systems design features is being carried out with the objective to optimize intervention intervals (grace periods) desirable to effectively perform AM measures. Design parameters subject to such optimiziations are, a o

- SG secondary side water inventory
- pressurizer volume
- accumulator volume and prepressure
- RPV elevation, height and water inventory

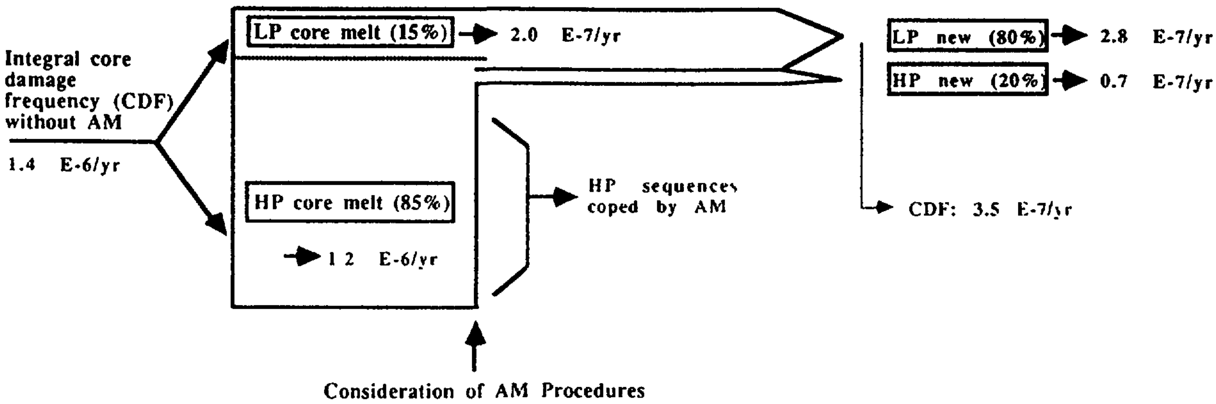


Fig.7: Influence of Accident Management Procedures on Integral Core Damage Frequency for Recent PWRs (absolute and relative HP/LP events; approximate values)

Projection of the described AM measures into a probabilistic valuation of the recently commissioned 1300 MW PWR Konvoi plants suggests the following conclusion:
The estimated core damage frequency with preventive accident management measures not assumed to be taken turned out to be approximately $1{,}4 \times 10^{-6}$/year the high pressure (HP) path contribution being 1.2×10^{-6}/year (= 85 %) (Fig. 7)
By taking the described preventive AM measures, 75 % of the overall uncoped sequences can be ultimately controlled reducing the integral core damage frequency to $\sim 3.5 \times 10^{-7}$/year and the more adverse HP contribution to less than 1×10^{-7}/year, the latter being diminished by roughly 95 %.

Alternatively to AM measures new systems designs have been and are being looked at capable of coping with accident sequences resulting from loss of heat removal through the SGs, e. g.,

- HP primary residual heat removal (RHR) system equivalent to that realized for the Atucha NPP, or a passive version thereof making use of a natural convection dry cooling tower on the secondary side of the HP-heat exchanger.
- Due to the excellent HP heat transfer capability of the existing SGs, priority should be given to a secondary side passive emergency condenser The steam generated in the SGs will be condensed in an emergency condenser, that can be fed with water from a pool having an elevation sufficiently high to warrant passive water inflow
  The capacity of the pool should be dimensioned such that primary side cooldown and decay heat removal is readily possible for at least 24 hours

Even in the extremely unprobable case of both failure of heat removal via the SGs and subsequent failure of performing the afore mentioned AM measures core melt and subsequent RPV failure under HP condition would not necessarily lead to early containment failure if upward thrust on the RPV - depending on the RPV failure mode - and the resulting load on the RPV support structures are assumed to be high enough to cause failure of the support structure. Design studies are underway with the objective to explore whether and how the RPV support structure in conjunction with geometrical reshaping can be enforced in such a way as to withstand uncontrolled RPV upward movement that could otherwise endanger containment integrity
As a result, the AM measures in conjunction with design improvements indicated in this subchapter will reliably prevent core melt under high pressure condition In the worst case the high pressure scenario will be transferred to a low pressure core melt sequence that can be coped with by appropriate mitigative AM measures in conjunction with adequate design precautions as to be described in the subsequent subchapter.

4.4 MITIGATIVE ACCIDENT MANAGEMENT MEASURES TO MAINTAIN CONTAINMENT INTEGRITY IN BEYOND DESIGN EVENTS

In case the preventive AM measures taken in a beyond design event have not been successful, i. e. prevention of core melt-down with subsequent failure of the RPV under low pressure (LP) condition has not been possible, **mitigative AM measures** can be and will have to be taken.

The dominant aim of mitigative AM measures after a severe core damage accident has occurred is to maintain the containment integrity such that the environment will not be subjected to unacceptable radiological consequences, and off-site emergency measures, e. g , large-scale evacuation, are not needed.

Failure frequency of early containment isolation has been estimated in the German Risk Study Phase B to be below 10 8/yr and can thus be considered negligible.

Hydrogen produced during the melt-down of the core might contribute to early pressure peaks and corresponding containment loads due to H_2 deflagration phenomena In order to ensure adequate safety margins to containment failure, combustion of hydrogen should be triggered as early as possible whilst H_2 amount and local concentration are low. Hydrogen recombination or ignition should constitute the first mitigating AM measure
For that purpose two types of H_2 recombiners - catalytic and battery powered igniters - requiring no energy supply from outside have been developed and qualified at Siemens/KWU Installation in PWR plants of such igniters or, alternatively, of catalytically acting foils also under development in the FRG is currently under discussion It will decisively reduce the probability of occurence of large scale H_2 detonations that could endanger containment integrity

In-vessel **steam explosion** has been under discussion as a potential contributor to the risk of early loss of containment integrity.
A thorough and careful evaluation of experimental and theoretical investigations has been carried out in the German Risk Study Phase B (DRS-B) This led to the conclusion that a violent steam explosion exhibiting a mechanical energy large enough to endanger pressure boundary and, as a potential consequence, containment integrity, can be practically excluded or at least assumed to be extremely unlikely. As a result, steam explosion as a risk relevant accident path has been neglected in DRS-B

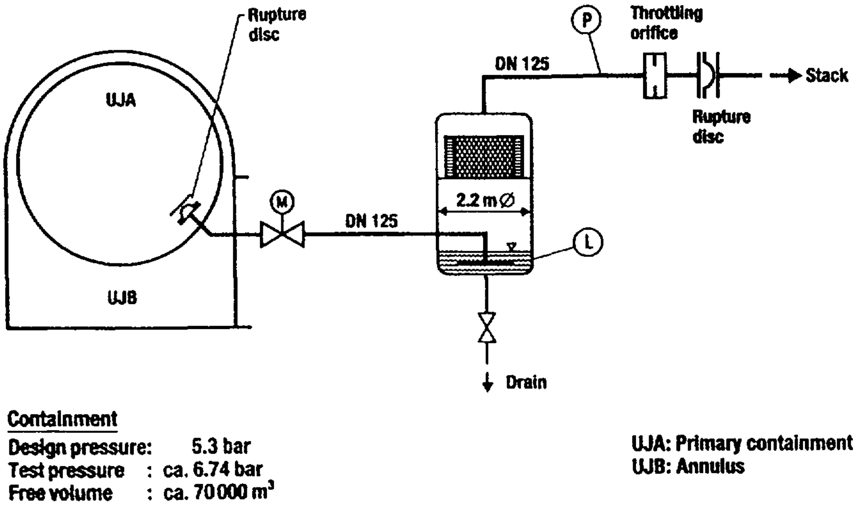


Fig. 8: Containment Venting
Flow Diagram and Arrangement

In the long-term phase following occurrence of a core melt accident the pressure would slowly rise from energy and mass released during the in-vessel phase and from corium concrete interaction up to the ultimate failue pressure of the containment Due to the large volume and structures in the containment it takes about 4 days to this pressure build up and more than 3 days to reach the test pressure In order to prevent an uncontrolled failure of the containment and to strongly reduce the consequences of potential radioactivity release to the environment, **a filtered containment venting** device is being installed in LWRs in the FRG One version, representing the Siemens type 'Sliding Pressure Venturi Scrubber', is shown in Fig 8
An existing containment penetration is used for the connection of the pressure relief line The containment atmosphere is discharged into the vent stack via the venting device The filter retains more than 99 % of the aerosols and more than 90 % of the iodine thus exceeding the required effectiveness markedly

This second mitigating AM measure reduces the activity releases caused by core melt sequences drastically to such an extent that offsite emergency response actions can be dispensed with and long-term land contamination can be ruled out.

Consideration has to be given also to the question of how the molten core material (corium), after RPV melt-through, would spread within the reactor building and erode the concrete basemat, although this path of activity release represents a lower risk to the environment than a release to the atmosphere.
The primary objective of an improved containment basemat design is to stabilize the corium and to maintain its coolability such that basemat penetration will be prevented.
This requirement will be met by one of the following two principal design approaches:

- Spreading the corium over a sufficiently large area such that the thickness of the melt layer is low enough to be coolable by direct water contact from above.
  Analysis shows that the required layer thickness is approximately 12 to 15 cm resulting in a melt lake area of roughly 200 m^2
  The decay heat is transferred to steam that is being condensed at the steel shell of the containment with the condensate drained back to the molten core material. Ultimate decay heat removal can be effected via the steel shell to an external water coolant spray or a convective air flow system.

- Alternatively, the corium can be controlled by a core retention device located in the lower part of the containment.
  Heat removal would be performed by a dedicated corium cooling system.

R & D efforts are underway to explore the different design options and to choose an optimized and balanced solution.

Striving for a containment design by which the most severe accidents theoretically conceivable could be deterministicly contained irrespective of their frequency of occurrence, i. e., large scale H_2 detonation, steam explosion and pressure vessel failure under high pressure core-melt condition would mean a departure from a balanced safety concept where safety is measured in terms of core damage frequency and corresponding probability for activity release to the environment.

Dealing deterministicly with very rare events whose frequency of occurrence is, e. g. less than 10^{-8}/year should be renounced according to the rules of practical good sense.
More generally, one should agree on an international basis that accident sequences leading to unacceptable radiological consequences with a frequency lower than a sufficiently small value to be agreed, e. g., $< 10^{-7}$/year, should be neglected; the reactor can and should be considered to be deterministicly safe with regard to such extremely rare event sequences.
In this sense, all conceivable accidents with potential catastrophic consequences to the environment should be deterministicly ruled out.

5. SIEMENS/KWU BOILING WATER REACTORS

The majority of the safety principles and accident management (AM) measures described in the previous chapters for the PWR can be analogously transferred and have been applied, respectively, to the BWR [12, 13].
E. g , probabilistic safety analyses (PSA) have been extensively performed for all classes of BWRs in operation in order to identify safety improvement needs.

- The computer aided process information system PRISCA™, after adaptation, is being implemented to the BWRs

- Both preventive and mitigative AM procedures to be initiated in beyond design events have been explored and elaborated, e g ,
  in case of a station blackout feedwater is injected into the RPV making use of the feedwater tank overpressure, and subsequently of fire protection systems with mobile energy supply
  following a core melt accident filtered containment venting will be performed using the Siemens sliding pressure venturi scrubber H_2 problems are avoided due to containment inertisation

The safety level achieved with the most recent BWR model 72 as realized in the two Gundremmingen NPPs KRB-B and -C is comparable to that of the corresponding PWR NPPs.

Many of the distinguishing features praised and strived for in advanced boiling water reactor (ABWR) development elsewhere have been anticipated in the KRB and even earlier NPPs already.
E. g.,

- Internal recirculation pumps integrated into the RPV thus eliminating the need for external recirculation piping have been in use since the Brunsbüttel NPP commissioned as early as 1977. By this means, and by implementation of an improved pressure suppression system within a cylindrical prestressed concrete reactor containment building a loss of coolant accident (LOCA) will be reduced to a comparably minor risk relevant accident.

- Fine motion control rod drives offering both good plant maneuverability and less pellet clad interaction (PCI) vulnerability of the fuel resulting from control rod movements.

6. CONCLUSIONS

Regain and reestablishment of public acceptance of large scale deployment of nuclear energy demand safety performance improvements appropriate to justify the expectation and conviction that the risk of occurrence of a severe accident will be further decreased and, in addition, that even an event exceeding the design basis and resulting in a core melt accident will not expose the environment to catastrophic radiological consequences.

For reactors to be built in the future safety improvements based on a combination of

- accident management procedures characterized by simplicity of operator actions to be taken, and
- passive safety systems to be explored and deployed

appear to hold promise of meeting this objective.

Agreement on an international basis should be strived for with the objective to improve the safety standard such that the probability of occurrence of an accident with unacceptable radiological consequences will be decreased to a value sufficiently low, e. g. < 10^{-7}/year, that, according to practical good sense, a reactor can be declared deterministicly safe with regard to such extremely rare events

In this sense all conceivable accidents with potential catastrophic consequences to the environment should be deterministicly ruled out on account of appropriate technical measures.

REFERENCES

[1] International Atomic Energy Agency, Vienna, 1988
Basic Safety Principles for Nuclear Power Plants, Safety Series No 75 - INSAG - 3

[2] Bürkle, W , Braun, W , Inherent Safety Features of Advanced Light Water Reactors
Proc of an IAEA Conference on Nuclear Power Performance and Safety, Vienna,
Sept 28 - Oct 2, 1987

[3] Gremm, O , The Role of Passive and Inherent Safety Properties in Siemens/KWU Nuclear Power Plants, Technical Committee Meeting on Passive Safety Features in Current Future Water Cooled Reactors, Moscow, USSR, 21 - 24 March, 1989

[4] Märkl, H , Inherent Safety of Advanced Nuclear Power Plants - Myth or Reality?
Lecture given to the Belgian Nuclear Society (BNS) Brussels, February 2, 1989

[5] Gesellschaft für Reaktorsicherheit (GRS) mbH,
Deutsche Risikostudie Phase B GRS-72 (Juni 1989)

[6] ALWR Requirements Document, Volume I, Electric Power Research Institute (1989)

[7] Feigel, A , Fabian H , Development of System Design in Recent Siemens/KWU PWR Influenced by PSA Results
PSA 89 International Topical Meeting Probability, Reliability and Safety Assessment
Pittsburgh, Pennsylvania, April 2 - 7, 1989

[8] Aleite, W , PRINS/PRISCA[R] Application, First Commissioning Tests and Experience Specialists Meeting on Man-Machine Communication for Emergency Operation in Nuclear Power Plants, Oct 18 - 20, 1988, Schliersee, FRG

[9] Hofmann, H., Jung, M., König, N., A New Digital Instrumentation and Control System for NPPs. To be published in Nuclear Engineering INTERNATIONAL, Oct 1989

[10] Fabian, H., Feigel, A., Actual Accident Management Measures in German Nuclear Power Plants Selected on Recent Results of PSA PSA 89 - International Topical Meeting Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, April 2 - 7, 1989

[11] Orth, K.-H., Safety Features of Next Generation KWU Pressurized Water Reactors ANS Topical Meeting on the Safety of Next Generation Power Reactors, May 1 - 5, 1988, Seattle, Washington, USA

[12] Fabian, H., Eyink, J., Assessment of Relevance and Consequences of Servere Accidents in Siemens/KWU BWRs IAEA Int. Symposium on Severe Accidents in NPP, Sorrento, 21th-25th April, 1988

[13] Albert, N., Bilger, H., Inerting System and Pressure Relief System with Filtered Venting in KWU BWRs. IAEA Int Symposium on Severe Accidents in NPP, Sorrento, 21th - 25th April, 1988

APPLICABILITY OF ADVANCED SAFETY SYSTEMS AND CONCEPTS TO LARGE-SIZED LIGHT WATER REACTORS

G. YAGAWA
University of Tokyo,
Tokyo, Japan

Abstract

NUPEC (Nuclear Power Engineering Test Center) with the sponsorship of MITI (Ministry of International Trade and Industry) started the investigation on advanced safety systems (related to the reactor shutdown, core cooling and fission product retention functions), using a passive system and /or a simplified system.

Major objective of this study is to seek the applicability of the advanced safety system concepts to large-sized LWRs of 800-1350 MWe.

This paper summarizes the preliminary result of this program consisting of the following

(a) Survey study
- Summarization of R&D activities for advanced safety systems in the world
- Assessment on the surveyed concepts

(b) Conceptual design
- Establishment of the conceptual design targets
- Designing and technical evaluation
- Reliability evaluation and compatibility evaluation with regulatory guide lines

(c) Extraction of developmental issues and overall assessment

---

1. INTRODUCTION

In the long run, the world electric power generation by nuclear plants has been steadily increased and especially the importance of LWRs has been recognized.

On the other hand, TMI accident and Chernobyl accident raised public concern to the safety of nuclear plants and public acceptance has become the most serious issue in the future nuclear plant development.

Under these circumstances, both efforts to improve the reliability and to improve the economy of LWRs are urgently required to keep the stable energy sourse.

It is the objective of this study to establish the advanced safety systems (related to the reactor shutdown, core cooling and fission product retention functions), using a passive system and/or a simplified system which have been or are being studied and developed in various countries for the purpose of improvement of reliabiilty and optimization of safety systems.

This study is focused upon the applicability of the advanced safety systems and concepts to large-sized LWRs of 800-1350 MWe.

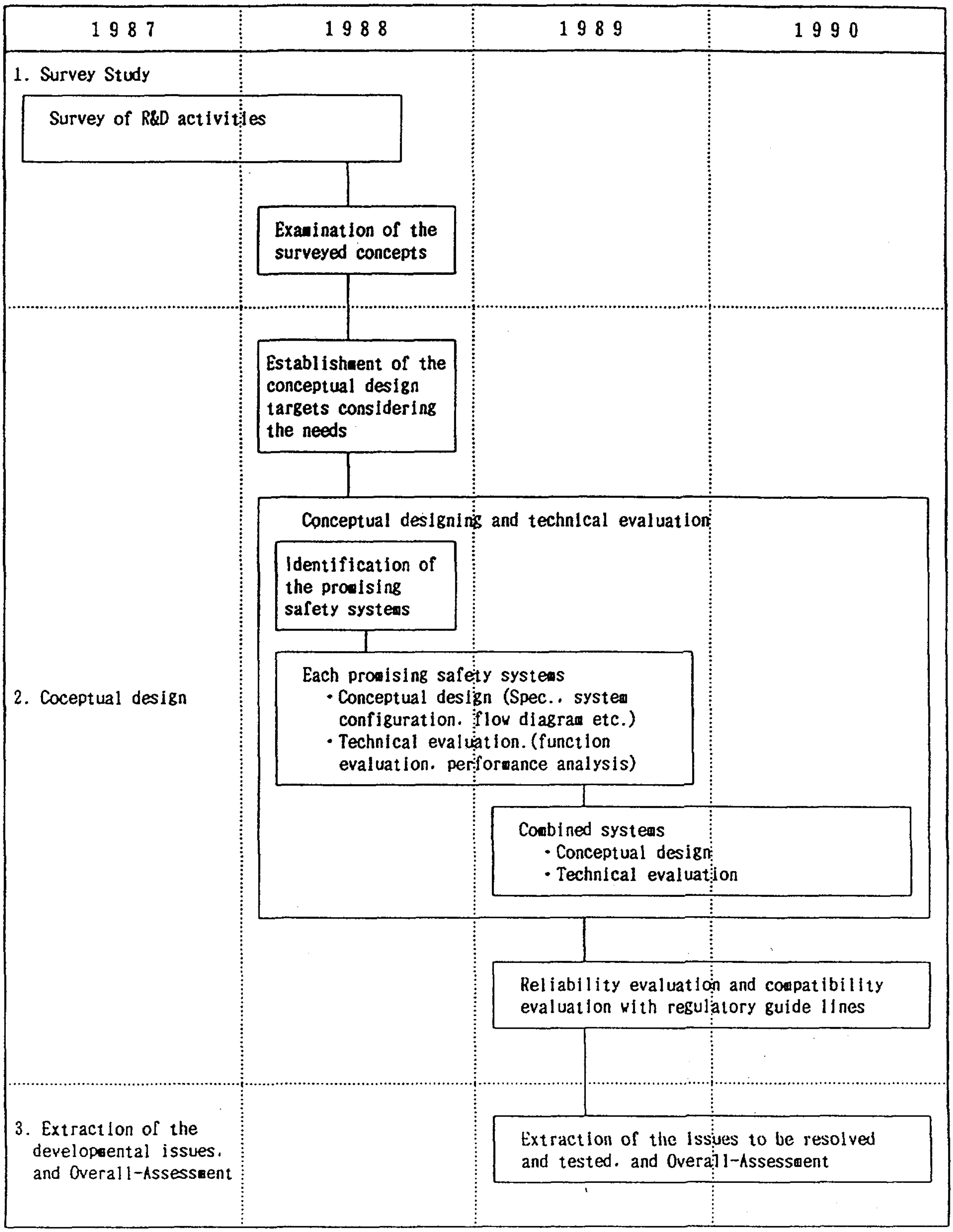
The investigation consists of three(3) steps described as follows and investigation period is four(4) years (see Table I).

(a) Survey study (1987-1988)

- Summarization of R&D activities for advanced safety systems in the world

- Assessment on the surveyed concepts

Table I Schedule of Investigation



(b) Conceptual design (1988-1990)

- Establishment of the conceptual design targets
- Designing and technical evaluation
- Reliability evaluation and compatibility evaluation with regulatory guide lines

(c) Extraction of developmental issues and overall assessment (1989-1990)

2. SURVEY STUDY

The survey study on the research activities is carried out.

According to surveyed results on the needs for advanced safety system developments in Canada and in Europe, it turns out that the common goals are to establish the sophisticated light water reactors which are modified and advanced based on the current proven LWRs.

Relating to the plants size, large-sized plants are required in Europe and small and medium-sized plants are required in USA. The needs of the next generation reactors in US manufactures (GE, WH) are the followings.

- Simplification
- Reduction of human-operation
- Improvement of system reliability
- More use of passive equipments
- Improvement of endurance in severe accident
- Improvement of ATWS capability

The research status on thirty-five (35) plants concepts in foreign manufacturers and research centers are surveyed for the purpose of searching new safety system seeds (concepts) in abroad. Then, the new engineering concepts on safety systems are examined and grouped into fifteen (15) seeds(concepts).

In addition, the design targets, design criteria, and design evaluations on the above concepts are surveyed.

From the Japanese researches on new engineering seeds, four(4) new engineering concepts which can be adopted as the advanced safety systems are selected.

2.1. Assessment of surveyed needs for advanced safety system

From the survey results on needs in Japan and in other countries, it is concluded that social needs for sophistcating safety systems in Japan and in foreign countries are almost the same.

The summary of the needs is as follows (see Table II for more details).

2.1.1. Improvement in economy

Improvement in economy of safety systems consists of the following.

- Reduction of construction cost
- Reduction of operation cost
- Shortening of construction period

Text continued on p. 230.

Table II Needs in Advanced Safety Systems

Needs	Specifications
Economical improvement	
Reduction of equipment cost	・Reduction of number of systems and trains ・Reduction of the dependency on supporting systems ・Reduction of number of active equipments inside CV
Reduction of operation and maitenance cost	・Simplification of equipment configuration ・Reduction of number of systems and trains
Shortening of construction period	・Reduction of pre-operation tests ・Shortening of CV construction period ・Reduction of number of systems and trains
Operability / maintenability improvement	
Simplification and reduction of periodic inspection	・Simplification of periodic inspection ・Reduction of periodic inspection items ・Reduction of number of active equipments
Simplification and reduction of maintenance work	・Simplification of equipment configurations ・Reduction of number of systems and trains ・Reduction of number of active equipments inside CV
Reduction of operator action after accident	・Reduction of operator action after accident ・Reduction of monitoring items during accident
Reliability improvement	
Improvement of system reliability	・Reduction of influence of common mode failures ・Reduction of dependency on supporting systems ・Simplification of equipment configurations ・Reduction of number of active equipments ・Reduction of equipment failure rate

Table Ⅲ Promising New Engineering Concepts

No.	New Engineering Concepts
1	Top-mounted hydraulic CRD
2	Accumulated standby liquid injection system
3	Gravity driven ECCS
4	Primary steam emergency (isolation) condenser
5	Steam injector
6	Natural heat removal for primary containment (water wall)
7	Secondary system natural circulation decay heat removal equipments
8	Natural ventilation cooling equipments
9	Accumulated / pressure-equalized ECCS
10	High-pressure RHR system
11	High-pressure natural circulation RHR system for primary system
12	Outer containment vessel spray equipments
13	Heat-pipe type decay heat removal system
14	Containment vessel with pin type fins
15	Static containment vessel spray equipments
16	Natural heat removal for containment vessel with outer pool
17	Steam driven emergency auxiliary equipments
18	External natural circulation cooling containment vessel
19	Buttery driven emergency auxiliary equipments

Table Ⅳ Application of New Engineering Concepts to BWR

Event \ Function		Reactor Shutdown: Short Term	Reactor Shutdown: Long Term	Core Cooling: Short Term Cooling	Core Cooling: Long Term Cooling: Core Cooling	Core Cooling: Long Term Cooling: Containment Cooling	Fission Product Retention
Accident	Large LOCA	① Top-mounted hydraulic CRD ② Accumulated standby liquid injection system ⑰ Steam driven emergency equipments ⑲ Buttery driven emergency equipments	① Top-mounted hydraulic CRD ② Accumulated standby liquid injection system	③ Gravity driven ECCS ⑨ Accumulated / pressure-equalized ECCS	③ Gravity driven ECCS	⑥Water wall ⑧ Natural ventilation cooling equipments ⑫ Outer CV spray equipments ⑬ Heat-pipe type decay heat removal system ⑭ CV with pin type fins ⑯ Natural heat removal for CV with outer pool ⑱ External circulation cooling CV	⑮ Static CV spray equipments
	Medium /Small LOCA	ditto	ditto	③ Gravity driven ECCS ⑤ Steam injector ⑨ Accumulated / pressure-equalized ECCS	③ Gravity driven ECCS ⑩ High-pressure RHR system ⑪ Primary system high-pressure natural circulation RHR system	ditto	ditto
Transient		ditto	ditto	④ Primary steam emergency (isolation) condenser ⑤ Steam injector	⑩ High-pressure RHR system ⑪ Primary system high-pressure natural circulation RHR system	—	—

Table V Application of New Engineering Concepts to PWR

Event \ Function		Reactor Shutdown		Core Cooling			Fission Product Retention
		Short Term	Long Term	Short Term Cooling	Long Term Cooling		
					Core Cooling	Containment Cooling	
Accident	Large LOCA	(Gravity driven CR)	(Gravity driven CR) ② Accumulated standby liquid injection system ③ Gravity driven ECCS ⑨ Accumulated / pressure-equalized ECCS	③ Gravity driven ECCS ⑨ Accumulated / pressure-equalized ECCS	③ Gravity driven ECCS (Core reflooding)	⑥ Water wall ⑧ Natural ventilation cooling equipments ⑫ Outer CV spray ⑭ CV with pin type fins ⑯ Natural heat removal for CV with outer pool ⑱ External circulation cooling CV	⑮ Static CV spray equipments
Accident	Medium /Small LOCA	ditto	ditto	③ Gravity driven ECCS ⑨ Accumulated / pressure-equalized ECCS	③ Gravity driven ECCS (Core reflooding) ⑦ Secondary system natural circulation decay heat removal equipments ⑩ High-pressure RHR system ⑪ Primary system high-pressure natural circulation RHR system	ditto	ditto
Accident	Main Steam Break	(Gravity driven CR) ② Accumulated standby liquid injection system ⑨ Accumulated / pressure-equalized ECCS	(Gravity driven CR) ② Accumulated standby liquid injection system ⑨ Accumulated / pressure-equalized ECCS	⑦ Secondary system natural circulation decay heat removal equipments ⑩ High-pressure RHR system ⑪ Primary system high-pressure natural circulation RHR system ⑤ Steam injector	⑦ Secondary system natural circulation decay heat removal equipments ⑩ High-pressure RHR system ⑪ Primary system high-pressure natural circulation RHR system	ditto (Break in CV)	—
Accident	F.W. Break	(Gravity driven CR)	ditto	ditto	ditto	—	—
Transient		ditto	ditto	ditto	ditto	—	—

Table VI Specified Needs and Conceptual Design Targets in Advanced Safety Systems

No	Specified Needs	Conceptual Design Targets
①	Reduction of number of systems and trains	I Number of systems and trains should be as lower as practicable But reliability of systems should be maintained.
②	Reduction of the dependency on supporting system (S/S)	II Dependency on supporting systems should be as lower as practicable.
③	Reduction of influences of common mode (C/M) failures	III The possibility of common mode failures should be removed as much as possible and the influences of common mode failures to the reliability of system should be as lower as practicable
④	Reduction of number of active equipments	IV Number of active equipments should be as lower as practicable. Attention should be paid to prevent economy from getting worse by increase of equipment cost and development cost, when new concepts are adopted to reduce number of active equipments. But relibility of systems should be maintained.
⑤	Reduction of number of active equipments inside containment vessel	
⑥	Simplification of equipment configurations	V The adopted equipment configurations should be as simple as practicable.
⑦	Reduction of equipment failure rates	VI The failure rate of adopted equipments should be reduced as low as practicable. But attention should be paid to prevent economy from getting worse by increase of equipment cost.
⑧	Reduction of periodic inspection	VII The sophisticated safety systems should be those in which needs of periodic inspection are reduced as much as practicable. In the case that the system needs periodic inspection, simplification of them should be required as much as possible. Attention should be paid to prevent economy from getting worse by increase of equipment cost.
⑨	Simplification of periodic inspection	
⑩	Reduction of pre-operation tests	VIII The sophisticated safety systems should be the system in which needs of pre-operation tests are reduced
⑪	Reduction of operator action after accident	IX The sophisticated safety systems should be those in which needs of operator action after accident are reduced as much as possible with the aim that there is no need of operator action. Pay attention to prevent economy from getting worse by increase of equipment cost.
⑫	Reduction of monitoring items during accident	X The sophisticated safety systems should be those in which monitoring items are reduced as much as possible during accident.
⑬	Shortening of CV construction period	XI The sophisticated safety systems should be those in which the CV construction period is shortened as much as possible.

Table Ⅶ Compatibility of the New Engineering Concepts to the Conceptual Design Targets

Conceptual Design Targets \ New Engineering Concepts	1 Top-mounted hydlaulic CRD	2 Accumulated standby liquid injection systems	3 Gravity driven ECCS	4 Primary steam emergency (isolation) condenser	5 Steam injector	6 Natural heat removal of CV -water wall-	7 Secondary system natural circulation decay heat removal equipments	8 Natural ventilation cooling equipments	9 Accumulated/ pressure -equalized ECCS	10 High-pressure RHR systems
Ⅰ. Reduction of number of systems /trains	—	○	○	—	—	○	○	○	○	○
Ⅱ. Reduction of the dependency on S/S	—	○	○	○	○	○	○	○	○	—
Ⅲ. Reduction of influences of C/M failures	—	○	○	○	○	○	○	○	○	—
Ⅳ. Reduction of number of active equipments	—	○	○	○	○	○	○	○	○	—
Ⅴ. Simplification of equipment configurations	×	○	○	○	○	○	○	○	○	—
Ⅵ. Reduction of equipment failure rates	—	○	○	○	○	○	○	○	○	—
Ⅶ. Simplification of periodic inspection	—	○	—	○	—	○	○	○	○	○
Ⅷ. Reduction of pre-operation tests	—	○	—	○	—	×	—	×	○	—
Ⅸ. Reduction of O/A after accident	○	○	○	—	—	○	○	○	○	—
Ⅹ. Reduction of M/I during accident	—	○	○	○	○	○	○	○	—	—
Ⅺ. Shortering of CV construction period	N/A	N/A	×	N/A	N/A	×	N/A	×	N/A	N/A

Conceptual Design Targets \ New Engineering Concepts	11 High-pressure natural circulation RHR system for primary steam	12 Outer CV spray equipments	13 Heat-pipe type decay heat removal system	14 CV with pin type fins	15 Static driven emergency auxiliary equipments	16 Natural heat removal of CV with outer pool around it	17 Steam driven emergency auxiliary equipments	18 External circulation cooling CV	19 Buttery driven emergency auxiliary equipments
Ⅰ. Reduction of number of systems /trains	○	○	○	○	—	○	—	○	—
Ⅱ. Reduction of the dependency on S/S	○	○	○	○	○	○	○	○	○
Ⅲ. Reduction of influences of C/M failures	○	○	○	○	○	○	○	○	○
Ⅳ. Reduction of number of active equipments	○	○	○	○	○	○	—	○	—
Ⅴ. Simplification of equipment configurations	○	○	×	×	○	○	—	○	—
Ⅵ. Reduction of equipment failure rates	○	○	○	○	○	○	—	○	—
Ⅶ. Simplification of periodic inspection	○	○	×	○	—	○	—	○	—
Ⅷ. Reduction of pre-operation tests	—	×	—	×	—	×	—	×	—
Ⅸ. Reduction of O/A after accident	○	○	○	○	—	○	—	○	—
Ⅹ. Reduction of M/I during accident	○	○	○	○	○	○	—	○	—
Ⅺ. Shortering of CV construction period	×	×	×	×	N/A	—	N/A	—	N/A

(NOTE)
○: Superior , —: Equal , ×: Inferior ,regarding capability compared to the current systems against the Conceptual Design Targets.

2.1.2. Improvement in maintenability / operability

Improvement in maintenability / operability is required both during normal operation condition and during accident condition as

- Simplification of inspection / test procedure
- Simplification of equipment repair / maintenance
- Automatic operation during accidents

2.1.3. Improvement in reliability

Required functions for improvement in reliabilities on safety systems are divided into two major functions. The one is to have safety equipments normal conditions without troubles during nomal operation, and the other is to achieve the healthy function of safety systems during accidents.

2.2. Assessment of surveyed seeds for advanced safety system

As a result of the research, nineteen(19) concepts selected as the promising new engineering concepts, which are shown in TableⅢ.

Analizing the new engineering seeds(concepts), the applicable areas of the new engineering concepts which can be replaced to the current safety systems are sought as shown in TableⅣ for BWR and TableⅤ for PWR, respectively.

These tables show how each new engineering concept is classified in terms of events and functions.

3. CONCEPTUAL DESIGN

Thirteen(13) specified needs are selected together with the conceptual design targets as shown in Table Ⅵ.

Then, the evaluation whether each new engineering concept of TableⅦ satisfies the conceptual design targets of TableⅥ is performed.

The compatibility of the new concepts to the conceptual design targets are shown in TableⅦ. As a result of this evaluation, it turns out that all the selected new engineering concepts satisfy at least one or more conceptual design targets.

Therefore, a preliminary conceptual designing is performed against all nineteen(19) concepts.

In result, the two new engineering concepts,(a) Top-mounted hydraulic CRD and (b) Containment vessel with pin type fin, are regarded as difficult concepts to apply to the current LWRs from the view point of performance and capability.

The reasons why the above two new concepts are not applicable are described as follows.

(a) Top-mounted hydraulic CRD
Top-mounted hydraulic CRD is not suitable to the high-power density core like large-sized LWRs, because SCRAM speed is lower than that of the current CRD.

(b) Containment vessel with pin type fin
Heat removal capability of pin type is worse than that of plate type fin.

In addition, the following concepts are required to be modified or to have some limitations.

(c) Heat-pipe type heat removal system
When "heat-pipe " is used in large-sized LWRs, large numbers of "heat-pipes" and penetrations through containment vessel are required.

Therefore, it is preferable to use "seperated type heat-pipe", called "Heat-pipe type heat removal system " that consists of evaporator, condenser, and connected pipes.

(d) Steam driven emergency auxiliary equipment
This concept requires high-pressure and high-temperature steam supply, and then is not compatible with the equipments/systems that require the function of operation in the condition of low-temperature and of long-term operation after accidents. This concepts could be applied only to standby liquid injection system in BWR.

(e) Buttery driven emergency auxiliary equipment
This concept is only applicable to the equipments/systems using the pump which has small capacity and operates only in short period.
This concept could be applied only to standby liquid injection system in BWR.

4. FUTURE PLAN

In the following two years, the conceptual designing such as development of P&ID (Piping and Instrumentation Diagram), technical evaluation of function and of performance, definition of power limit and justification of system capability will be performed in order to embody the advanced safety systems. Reliability evalutaion will also be performed.

Finally, the extraction of issues to be resolved and to be tested, and overall assessment of the advanced safety systems will be performed.

ACKNOWLEDGEMENTS

The auther would like to acknowledge the fruitful discussions of Prof. Y. Oka (Univ. of Tokyo), Prof. M. Aritomi (Tokyo Inst. Techn.), and other members of Steering Committee for Investigation on Advanced Safety Systems.

SAFETY ASPECTS OF ADVANCED LWR DESIGNS

F.R. ALLEN
AEA Technology,
Safety and Reliability Directorate,
United Kingdom Atomic Energy Authority,
Culcheth, Warrington, Cheshire,
United Kingdom

Abstract

Advanced reactor designs are now being actively pursued in many centres throughout the world for both economic and safety reasons. The Safety and Reliability Directorate of AEA Technology has reviewed these designs to see if they pose any new issues for safety analysis, which will require new methods or data to resolve. In order to identify potential accident sequences in new designs, a generic logical tool for accident sequence identification has been developed. Also, the safety of these designs has been found to rest more on analysis of such natural processes as natural convection. This may call for more detailed models and experimental verification. These apart, no fundamental difficulties have been found. Simplified designs should make it easier to demonstrate the required degree of safety more transparently, and many of the new designs can retain the benefit gained from operating experience with existing plant if the departures from current practice are not too radical.

1. INTRODUCTION

Advanced reactor designs are now being actively pursued in many centres across the world. These are being developed in response to pressures from a number of directions both to do with safety issues and also economic ones. Amongst these latter is the perceived need for smaller sized generating units, which can bring several economic benefits to set against its apparent loss of "economies of scale" in comparison to the current generation of power stations. However, this paper is concerned with safety aspects.

The new designs are based on gas-cooled and liquid metal cooled technologies as well as LWR technology, but the majority of those currently being developed are based on existing LWR technology, developed and extrapolated to a greater or lesser extent depending on the design concerned.

The Safety and Reliability Directorate of AEA Technology has recently been reviewing these designs with a particular brief. This is to see whether they pose any new issues for safety analysis, which will require new methods or new data to resolve. The purpose of this paper is to present the results of this in respect of LWR designs in general, and draw out generic points.

2. THE "INHERENT SAFETY" CONCEPT

Many advanced designs claim some degree of inherent safety. The concept of Inherent Safety has been with us for some time. [1] This is a concept which, though attractive, is susceptible to different interpretations and so a number of different kinds of "Inherent safety" can be identified and defined more rigorously:

> Intrinsic Safety: Safety provided by components of the design which are essential for the normal operation of the plant.
>
> Passive Safety: Safety provided by means of "natural" or "dissipative" physical processes. These may be provided through engineered systems specifically provided for that purpose but it is usually interpreted as only including engineered systems needing no external power source to operate them.
>
> Forgivingness: The extent to which a reactor design is tolerant of both maloperation and failure of engineered systems. This is usually held to embrace long time margins for operator response to serious faults and scope for successful mitigation and management of accidents.
>
> Ultimate Safety: The maximum possible consequences of an accident are within some specified acceptability criterion.

The main thrust of the remainder of this paper is to see what effect the incorporation of intrinsic or passive safety features into LWR designs affects the way in which their safety is analysed and assessed.

3. APPROACHES TO SAFETY ANALYSIS

Existing approaches to safety analysis of nuclear plant centre on two alternative methods - the "design basis (DB)" and "probabilistic safety analysis (PSA)" approaches. The DB method identifies a relatively small number of worst case scenarios and analyses the plant response in great detail to show that it conforms with specified criteria even under grossly pessimistic assumptions. The PSA approach tracks the possible responses of the plant to a large number of initiating events to produce an assessment of the overall safety of the plant. In addition, this enables the overall balance of the design to be evaluated and enables, in particular, potential weak points in the safety systems to be identified.

---

[1] See for example:

SPIEWAK, I (ed) "Forgiving or inherently safe reactors." (Proc. ANS Winter Meeting, Washington DC, November 1984) Trans.Am.Nucl.Soc. 47 (1984) 286-303.

LESTER, R K "Rethinking nuclear power". Scientific American 254 (March 1984) 23-31.

KLUEH, R "Future nuclear reactors - safety first?" New Scientist, 3 April 1986, pp 41-45.

Both of these methods rely to a greater or lesser extent on the existence of a list of initiating events to be considered. (In the PSA approach, it is possible to generate part of the list of initiating events by means of reliability studies on the plant as normally operated.) This is based in part on experience of operating similar plant, in part on previous analyses of similar plant and in part on regulatory requirements. In addition there is the problem of "completeness" - can we be sure that the list does not omit some significant initiating event, or even a whole group of such events? As it becomes necessary to analyse the safety of new designs, which extrapolate to a greater or lesser degree from our current experience base, there is a need to develop a more generic approach to this initial phase of the safety analysis.

To answer this need, an approach used in the past for LWR analysis has been developed by SRD to a generic tool for accident sequence identification. In addition to providing a more flexible approach capable of being applied to advanced designs; it also helps to answer the problem of 'completeness'. The new approach concentrates on safety functions and their preservation in generic transients and offers the possibility of a list of accident sequences which is complete at the generic level.

4. ACCIDENT SEQUENCE IDENTIFICATION METHOD

The generic accident sequence identification method concentrates on three key safety functions:

- Reactivity Control
- Heat Rejection
- Containment

and six generic transients:

- over power
- under power
- over cooling
- under cooling
- over pressure
- under pressure.

It looks at each of these in each phase of operation:

- Refuelling
- Cold Shutdown
- Startup
- Power Operation
- Hot Standby
- Cooldown.

This generates a list of 108 possible generic accident sequences which can then be developed in a plant specific context. In the initial phase the list is screened and then the analysis developed as in a conventional fault tree approach. Potential accident initiators specific to the plant are then identified and data obtained on them. This enables groups of initiators to be formed for subsequent transient analysis.

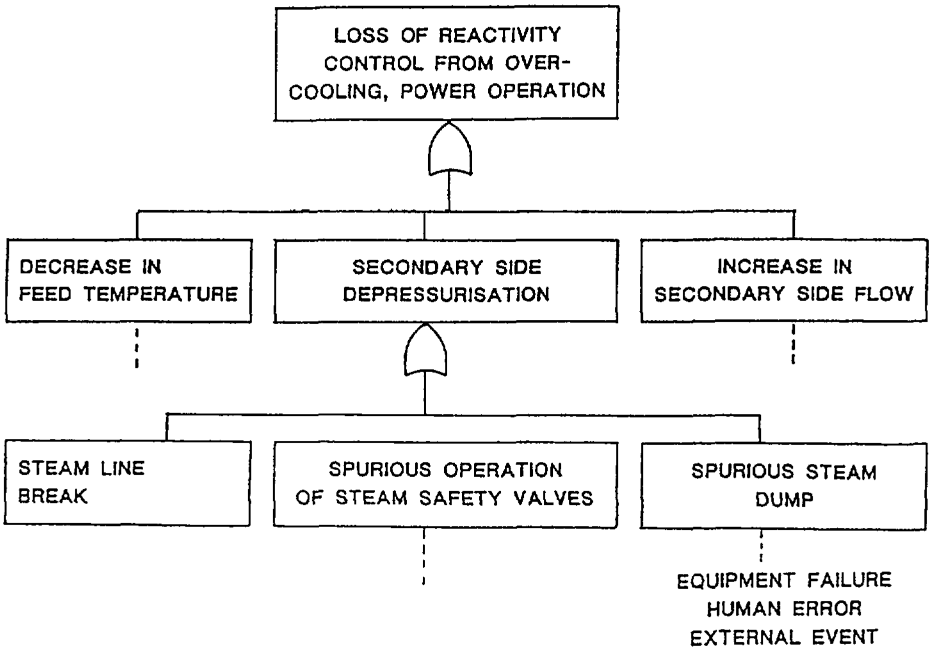


Fig 1

As a result of this logical analysis it is possible to generate a list of initiating events for a new system which does not rely on past experience and which can also be used to identify design basis accidents if need be.

Fig 1 shows an example of the method in operation.

5. APPLICATION TO ADVANCED DESIGNS

A large number of advanced LWR designs have now been proposed across the world and a sub-set of these have been reviewed by SRD. The approach outlined above was used to assess the general issues raised by these new advanced designs. This application was successful and leads us to believe that the method could readily be extended to a full scale study of a specific design. Not all of the new designs claim 'inherent safety' but most exhibit a move towards less reliance on active, engineered systems and more use of passive systems and natural processes. This trend is assisted by the parallel trend towards smaller core size which makes heat removal by natural processes easier.

Advanced LWR's offer advantages in this context. There are many safety advantages inherent in all LWR's, for example the well-established reactivity feedback mechanisms which can provide strong self-limiting capabilities in transients and which are exploited to good effect in many designs. In addition, advanced LWR's can draw upon the large body of experience gained with design and operation of existing plant; there is a very good basis in the fundamental technology on which to build provided the design is not too radical a departure.

With regard to the safety aspects of the new design features, the conclusions of the review, in general terms, are as follows. Firstly, so-called "inherent safety" is not the same thing as absolute safety as defined above. The designs reviewed relied on engineered provisions for their safety to some extent.

Most "inherently safe" designs incorporate passive safety devices or natural processes to ensure safety. This often results in significantly simpler designs, and it may well be easier to demonstrate the required degree of safety for these systems without complex analysis. Simpler designs, of course, may also be cheaper to construct. They may also ease such safety-related problems as quality assurance both through the simplification itself and by allowing a greater degree of shop fabrication.

However, the review found that all the designs still required some active engineered systems, the most common case being those to achieve cold shutdown, which cannot be achieved through temperature feedback alone.

6. IMPLICATIONS FOR SAFETY ANALYSIS

There are a number of well-known advantages and disadvantages to the shift to passive systems and natural processes. Advantages include the possibility that risk may be reduced or that a specified level of safety may be more 'transparently' demonstrated by less reliance on complex engineering systems. There is also the possibility that simplified designs will be cheaper to build. Against these advantages, there are several disadvantages such as the fact that such provisions may not be good for all faults and cannot be switched off. They cannot in general bring the plant to safe shutdown and can lead to operational difficulties. All these have been rehearsed before in sufficient detail for it not to be necessary to elaborate them here.

A more subtle difficulty has emerged from this study, however. In a conventional design of LWR, there are many engineering systems designed to keep the plant within its design basis. These may be redundant or diverse, depending on the reliability required. The basic safety of the plant rests largely on these systems and the calculated frequency of, for instance, core melt accident is generated largely by reliability analyses of engineering systems. The study of the reliability of such systems is now well established and a reasonable degree of certainty can be attached to the results. The physical phenomena concerned are often "analysed" using grossly pessimistic models with a wide safety margin. The certainty with which we can conduct this analysis is therefore quite high.

It is only when we step beyond the design basis into analysing core melt accidents that uncertainty associated with our understanding of physical processes becomes important. Probabilities of outcomes in this area (often called Level 2 PSA) depend not only on reliability of systems but also on the reliability of the analysis methods used for predicting the outcome of the physical processes.

In the new generation of advanced designs, however, the reliance on natural processes and passive systems to maintain the system within the design basis means that the reliability of these processes, and in particular the reliability of our analysis methods for these processes, becomes more significant. For example, suppose it is necessary to show compliance with a reliability target of 10^{-4} failures per demand for decay heat removal, and a naturally convecting system has been provided for this. It is necessary to show that the reliability or confidence in the analysis, which demonstrates that the natural convection loop will always start as intended, is good enough to support the required overall reliability. The physical processes typical of Level 2 PSA have in effect been brought into the Level 1 or the design basis areas. The situation is greatly simplified in that fixed-geometry as-designed systems are being considered so many of the more difficult aspects of the Level 2 analyses are absent. None-the-less it may well prove necessary to undertake further development of existing methods and/or experimental verification in order to provide the degree of certainty needed.

7. CONCLUSIONS

With advanced LWR's, there is a general trend towards smaller core power, simpler safety systems, and more reliance on passive systems and natural processes to maintain safety. The move towards these advanced designs can retain much of the benefit gained from operating experience with existing plant if the departures from current practice are not too radical.

One issue for new designs is the need to produce a list of initiating events on a logical basis without the benefit of operating experience for that particular design. SRD has developed a new approach to this which also helps answer the problem of completeness. This has been successfully applied in outline to a number of the advanced designs.

The review by SRD of a number of advanced designs shows that in general the simplification possible with these designs should make it easier to demonstrate the required degree of safety more transparently.

Another generic issue that emerges is that as the advanced designs rely more on passive systems and natural processes, the safety analysis becomes more reliant on our ability to analyse the behaviour of such systems. In particular the reliability of an engineered system in a conventional LWR analysis may be replaced by the reliability of the analysis of a natural-process system in an advanced LWR analysis. This may require further development of analysis methods and/or experimental verification to meet the required safety goals.

FUNDAMENTAL TRENDS IN AND TECHNICAL MEASURES FOR IMPROVING THE SAFETY OF OPERATING AND PLANNED VVERs

V.M. BERKOVICH
Atomehnergoproekt Institute,
USSR Ministry of Atomic Energy,
Moscow,
Union of Soviet Socialist Republics

Abstract

This report covers certain issues related to the improvements in safety of soviet NPPs with PWR reactors. The analysis is done for the modes of operation with significant deviation from normal operating conditions, such as blackout at NPPs; failure of all mechanical safety devices when they are required to function; significant leakages of primary circuit coolant into the secondary circuit; non-scheduled shutdown cooling of the reactor; loss of information about the state and condition of different components of the safety system.

Some recommendations and proposals are given for modification in the systems of the NPP, including passive devices, which permit to reduce probability of exceeding the related radioactivity release by two orders of magnitude.

List of Abbreviations

NPP - nuclear power plant
VVER - water-cooled and water-moderated reactor
RCPS - reactor control and protection system
PHRS - passive heat removal system
BIS - boron ejection system
SS - safety system
CCS - computer control system
PCP - primary coolant pump
FE - fuel element
FSDRASA - fast-acting steam dump (reducing) station -A
UCR - unit control room
BSC - back-up shutdown centre
QV - quick-closing valve
S - specifications
SG - steam generator
MSSSA - monitoring system for safety system availability

1. INTRODUCTION

The problem of ensuring the safety of nuclear power plants is presently acquiring special importance. The absence of any practical alternative to large-scale development of nuclear power makes designers attach much significance to the problem of safety particularly taking into account consequences of the accidents at Three Mile Island and Chernobyl nuclear power plants.

Recently a large number of safety analyses were conducted on VVER nuclear power plants which are currently operating worldwide and will continue to be the basic option at least up to 2000-2010. These analyses showed that modern VVER NPP had attained safety characteristics which can be considered adequate; on the other hand, there are ways of enhancing their reliability and safety.

Following the Three Mile Island accident particularly through safety analyses of VVER nuclear power plants were carried out in various countries. The accident alterted the international community and triggered an extensive development of research aimed at improving safety decisions.

Successful results have been achieved in this field, some of the technical decisions have already been introduced, this contributed to a higher safety level of modern NPP.

As a result of these studies methods of further safety improvement were developed.

Safety analyses of standard NPP with VVER-440 of second generation and VVER-1000 showed that their safety characteristics corresponded to the international standards. In some cases verification tests gave even more optimistic data than those that had been chosen as input criteria in the design. Analysis of Soviet VVER designs shows that reactor containment structures designed to withstand such accidents as 850 mm diameter pipe break do not fail even in case of circumferential reactor vessel rupture in the core region.

Although the present safety characteristics of modern VVER nuclear power plants can be considered satisfactory we adopted a decision to search ways of further improvements to ensure maximum reduction in risk resulting from operating plants and plants being planned. Safety approaches are illustrated in Table 1.

2. FUNDAMENTAL TRENDS IN VVER NPP SAFETY AND RELIABILITY IMPROVEMENT

Fundamental trends in further reducing risk from operation of NPP are outlined in "Basic safety principles for nuclear power plants" developed by the International Nuclear Safety Advisory Group (INSAG). They can be summarized as follows:

- defence in-depth
- accident management control
- parity of preventive and safety functions
- safety culture etc.

Implementation of these measures involves extensive research and development work.

For the purpose of developing most efficient measures which could be taken as soon as possible major events leading to significant fuel damage were analyzed, namely:

- accident development towards beyond-design basis
- size of accident exceeding that of a maximum design accident
- combination of above mentioned causes.

Table 1

Fundamental Trends in VVER NPP Reliability and Safety Improvement

Safety Objective	NPP Safety Improvment Methods	Practical Measures to Improve VVER NPP Safety
Accident prevention	Reactor inherent safety	Reactor physics improvement Improvement of reactor control and protection system Improvement of RCPS drive reliability
	Systems and equipment reliability improvement	Metal and equipment condition Equipment improvement
	Automatic process control system and information system improvement	In-core monitoring system Operator support systems in transient and non-stationary conditions
Safety in-depth of barriers	Localizing barrier improvement	Localization of leak from primary system within secondary system Hydrogen ignition system Pressure supression system and off-gas treatment system
	Operation of safety systems based upon passive principles of barrier protection	- Passive heat removal system - Boron injection system
	Improvement of CAD protection system and information system	Safety system availability

On the basis of this analysis major events initiating severe accidents were identified:

- long-term loss of power supply sources (with leakage or without it); failure of RCPS control elements
- major leak from the primary system to the secondary system leading to loss of core coolant.

Thus, we have been able to establish fundamental trends in improving the safety of VVER nuclear power plants and outline possible technical solutions.

3. PRACTICAL MEASURES OF IMPROVING VVER NPP SAFETY

3.1 REACTOR UPGRADING

Reactor upgrading is a question of particular interest; this paper briefly summarizes some aspects of reactor design development.

Reactor upgrading primarily implies improvement of nuclear/performance characteristics to enhance NPP safety.

To achieve this objective reactor upgrading would include the following:

3.1.1. Improving efficiency of the mechanical system of reactivity control by increasing the number if RCPS control element from 61 to 121 to ensure transfer of the reactor to a sub-critical state at a temperature of up to 100°C without extra additional absorber; it should be noted that according to requirements for reactivity control systems in Soviet reactors two systems are provided: a fast-acting mechanical system effective within the operating temperature zone and a fluid system effective within the whole temperature range. Necessity for operation of fluid reactivity control system imposes requirements on boron injection systems and makes safety systems more complicated. In order to increase realiability and safety requirements for mechanical reactivoty control system have been made to cover the whole temperature range.

Thus, nuclear hazardous regime can be avoided in non-stationary conditions associated with coolant temperature variations.

3.1.2 With the aim of achieving deep negative feedbacks over parameters concerning reactivity and, ultimately, to minimize fuel damage within the whole operating range modification of the reactor core was implemented:

- reduction in non-uniformity of reactor core power density due to increasing number of RCPS control elements and irradiated absorber rods

- in-core monitoring system improvement monitoring channels of new design were used to provide continuous control of neutron flux over the core volume during reactor operation and coolant temperature control at the fuel assembly inlet and outlet.

3.2 BORON INJECTION SYSTEM

System of boron injection into the primary circuit is designed to bring the reactor to a subcritical state by concentrated boric acid solution supply in case of RCPS failure.

The system consists of four independent channels connected to "cold" legs of main circulation circuit loops. Each channel incorporates an accumulator containing the concentrated boric acid solution; the accumulator is connected by pipelines to delivery and suction side of the primary coolant pump and provided with valves on these pipelines (figure 1). At the present time optimization of boron injection system characteristics is being carried out, for example, the following alternatives are considered:

- accumulator capacity 2,5 m^3
- boric acid concentration 160 g/l
- accumulator capacity 8 m^3
- boric acid concentration 40 g/l

Various valve designs and methods of maintaining an accumulator in operating condition are considered too.

In this paper primarily the concept of the system is formulated.

The boron injection system is at a disadvantage in relation to the mechanical reactivity control system as to response characteristics because of inability to reduce time of boric acid transport. However, performance characteristics of the boron injection system allow to considerably reduce reactivity effects and to avoid them in most cases during complete RCPS failure.

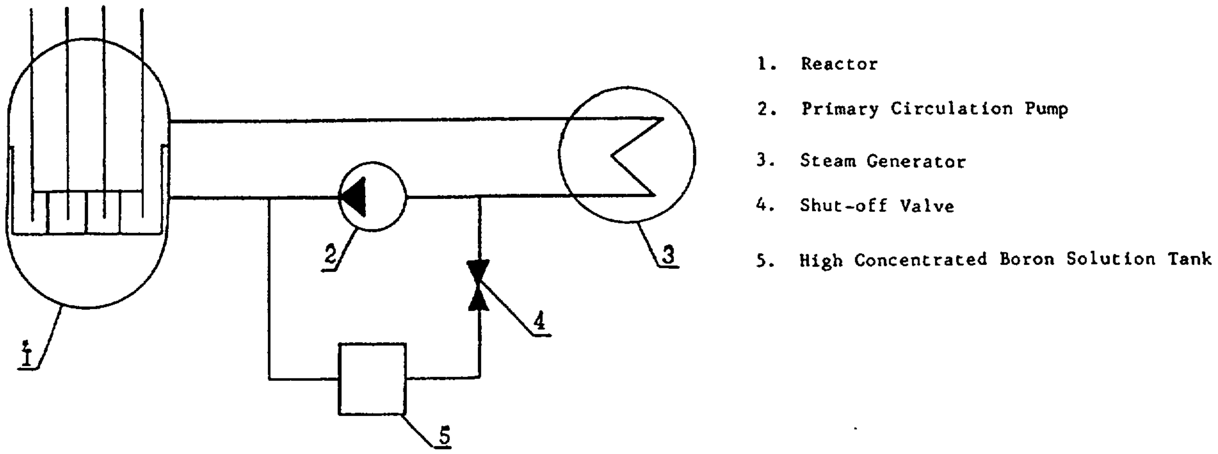


FIG. 1. Quick boron injection system.

The system operates in response to two signals:

- automatic protection signal
- signal indicating failure to reduce neutron flux within 2 sec. after automatic protection signal.

Command to start the system is executed by opening fast-acting valves on the primary coolant pump by-pass.

For a period of the primary coolant pump coastdown the high-concentrated boric acid solution is delivered to the circuit, in this way an introduction of liquid absorber is performed.

Thus, operation of the system is based on the passive principle (the inertia energy on the primary coolant pump coastdown). Power supply is needed only for generation of signal initiating the system operation.

3.3 PASSIVE HEAT REMOVAL SYSTEM WITH LOSS OF ALL POWER SUPPLY SOURCES

3.3.1 General Characteristics and Principles of Performance

The Passive Heat Removal System (PHRS) is intended for long-term removal of residual heat from reactor during loss of all power supply sources including emergency power sources with the primary and secondary systems being leaktight. PHRS is a closed system with natural circulation in the primary and secondary systems (figure 2). The heat is removed by ambient air at a temperature
$\pm$ 50^{o}C; the system heat exchangers are located in superstructures above the elevation of 45,6.

The system consists of four independent loops, each of them connected to an appropriate steam generator and loop of the main circulation of the reactor installation.

Reactor installation design may ensure a removal of residual heat by natural circulation at 10% of the reactor rated power. The natural circulation loop on the secondary system side has been designed to remove 80 MW of residual heat available in three loops (2,7% of rated power) at normal reactor operation.

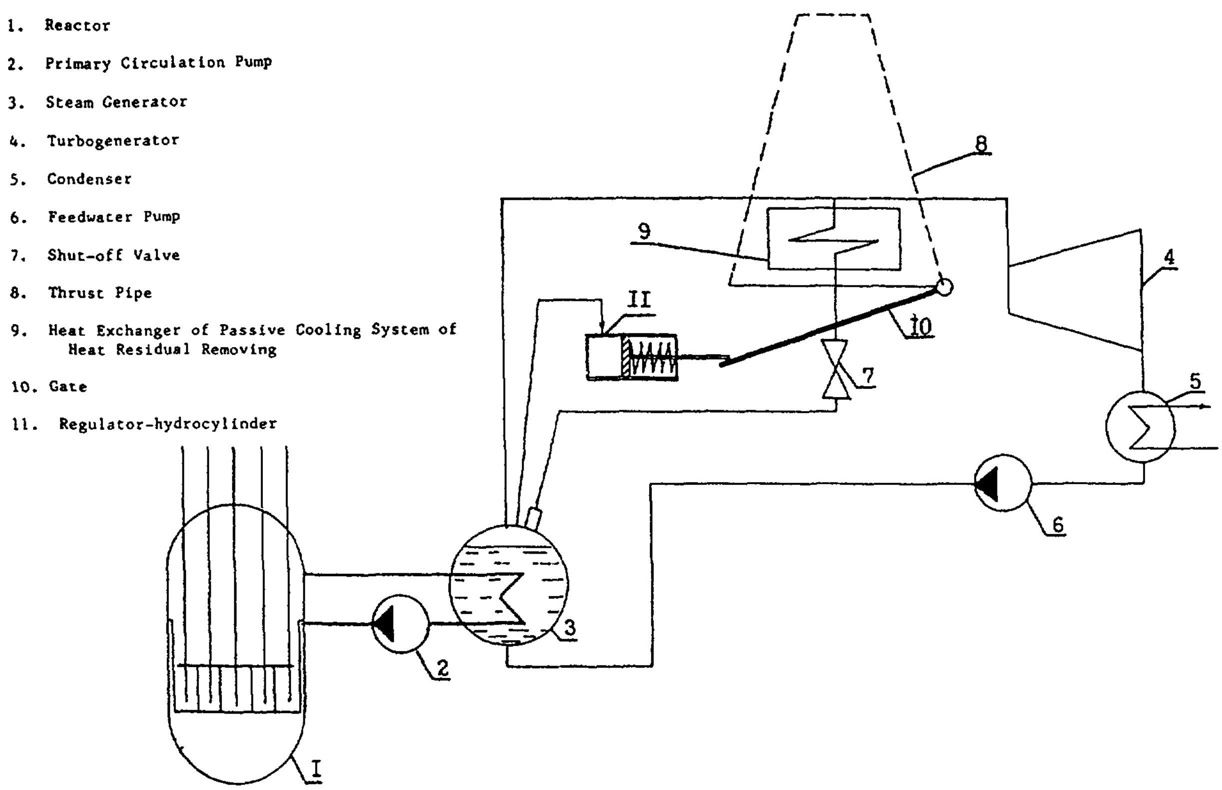


FIG. 2. Passive dissipation of heat.

In normal operating conditions the system is heated up which makes it possible in case of emergency to provide fast the design heat removal capacity.

These results have been confirmed experimentally, in fact it took the system less than 1 minute to reach the design capacity.

The heat removal system is passive. Its start-up and operation do not require any mechanisms or power sources. PHRS capacity is controlled through the air path by opening or closing a gate by the use of a passive direct-action controller actuated by the pressure of the secondary system.

In a steam generator the heat of the primary system is delivered to the secondary system; the resulting steam from the secondary system is fed to PHRS heat exchangers (the turbine path is cut off), where it is cooled by the ambient air, condensed and the condensate flows by gravity to the steam generator. To ensure the required cooling air flowrate a vent stack is provided at the bottom of which the system heat exchangers are located.

The heat exchanger room is provided with a gate which controls the opening for air passage. At normal power unit operation the gate is closed. During loss of a.c. power sources including the emergency power sources with increase in pressure within the secondary system the gate opens to provide the required passage of air. As the pressure in the steam generator decreases the gate closes thereby providing the passive control of air flowrate and, as a consequence, of fluid flowrate in the PHRS loop; and in this fashion PHRS capacity is regulated to match the variations of residual power of a reactor.

The use of PHRS is also possible without controlling its capacity which leads to reactor shutdown cooling.

The system is designed to remove decay heat with the main process loops being tight and it proves to be efficient in case of small and medium-size leaks in the primary system and the system retains its capabilities during boiling in the hot legs of the primary circuit as this takes place with the level decrease in the reactor vessel. When small and medium-size leaks are available including those resulting from 100 mm diameter pipe break the use of the PHRS makes it possible to considerably pro-long the period of the core dry-out.

The pressure drop in the primary system and as a result reduction in leak flow and better utilization of accumulator water as well as return of the condensate from the primary system to the core (which occurs as the level in the reactor vessel decreases) allow more efficient use of stored cooling fluid due to the PHRS operation.

For example, during 80 mm pipe break with simultaneous loss of all power supply sources without the use of the PHRS the fuel cladding may reach hazardous temperatures (temperature rise above 1200^{o}C) within less than an hour. The use of the PHRS might delay this process by 6 hours and more. Such a long-term gain in time offers more opportunities for adopting the appropriate measures to restore power supply and prevent severe damage of the core.

The passive heat removal system is highly efficient and reliable, its advantages are evident: its performance is based on passive principles, heat is removed directly to the ultimate sink - air, the high capacity of the system makes it possible to perform its function even in case of partial failures (e.g. failures of two loops).

It should be emphasized that the PHRS capabilities are not restricted to the features described. At present studies are carried out which would make it possible to reject an emergency feed pump system and a fast-acting steam dump reducing station -A due to the use of PHRS and possibilities of scheduled procedures for reactor shutdown cooling by means of PHRS are considered. Thus, PHRS is highly efficient system with multifunctional capabilities.

Adoption of this system will allow a considerable increase in NPP safety.

3.3.2 Analysis of a Possibility to Reject Emergency Feed Pump and Fast-Acting Steam Dump Reducing Station-A in Reactor Installations Provided with PHRS

Functional requirements for emergency feed pump (EFP) and fast-acting steam dump reducing station -A (FSDRS-A).

EFP and FSDRS-A perform the following safety functions:

- protection of the secondary system against the excess pressure (FSDRS-A) in case of rapid decrease in vapor energy removal
- reactor shutdown cooling in case of FSDRS-K and auxiliary feed motor pump failure (FSDRS-A, AFMP)
- reactor shutdown cooling in emergency conditions with high pressure in the primary system (FSDRS-A, EFP)

Requirements for FSDRS -A

FSDRS-A operation is required in the following situations:

- closing of turbine stop valves
- turbine generator load reduction by more than 50%
- complete de-energizing of NPP accompanied by closing of the turbine stop valves and feed water delivery to the steam generator being stopped
- it is assumed that under the given conditions FSDRS-K would not operate.

Requirements for EFP

The EFP operation is needed in the following situations leading to reduction in the steam generator water level below the permissible limit:

- interruption of feed water delivery to the steam generator
- complete de-energizing

It is assumed in these cases that both main turbine pumps and auxiliary motor pumps are not operable.

The operation of EFP is required to restore the steam generator water being lost in the process of decay heat removal.

With PHRS being available reactor shutdown cooling is possible without FSDRS-A and EFP, but for a number of regimes (for example, failure to close safety valves of the steam generator) and feed pipe break in the other steam generator to meet safety criteria the optimization of equipment characteristics is required, e.g. design pressure of the secondary system (figure 3).

Change of reactor installation parameters during complete de-energizing and cooldown by means of PHRS

Input data for calculations of reactor shutdown cooling by means of PHRS.

Data presented in Table 2 are assumed as input data for VVER-100 primary circuit geometry and performance characteristics of primary circuit systems.

In modelling power density it was assumed that:

(1) the most important group of RCPS elements failed during protection system-1 operation
(2) time delay 0 in protection system operation during complete de-energizing is assumed 1,7 s
(3) initial power of reactor installation is 3200 MW(t)
(4) steam generators are designed to be filled with coolant, so each of them contains 47700 kg of water

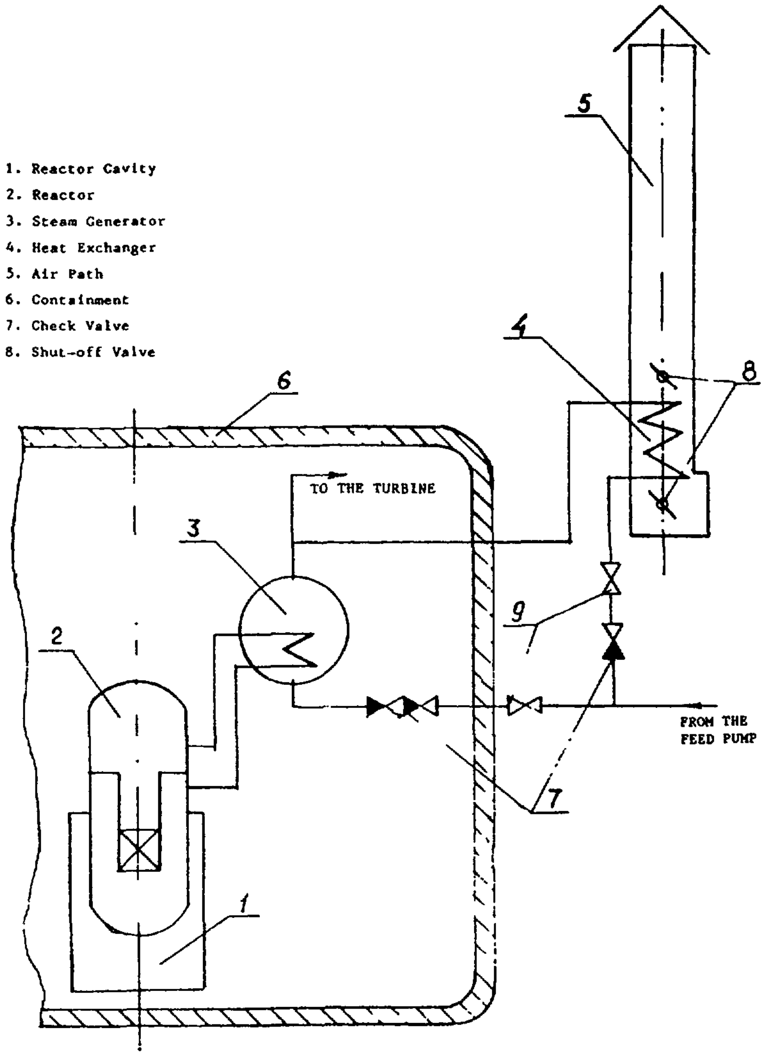


FIG. 3. Connection of the passive heat removal system to a steam generator.

TABLE 2. PHRS Characteristics

N	Denomination	Value
1.	Thermal rated power, MW	80,8
2.	Number of channels (subsystems) prcs	4
3.	Number of heat exchangers, pcs	16
4.	Absolute operating pressure of coolant (vapor) at system inlet, MPa	6,27
5.	Temperature of coolant (vapor) at heat exchanger inlet, C^{o}	278,5
6.	Coolant temperature at heat exchanger outlet, C^{o}	278,5
7.	Vapor humidity at heat exchanger inlet, %	0,5
8.	Fluid at heatexchanger outlet	condensate
9.	Air flowrate, kg/s	4x 118,8
10.	Absolute operating air pressure, MPa	0,098
11.	Maximum air temperature at system outlet, C^{o}	217,8
12.	Hydraulic resistance of steam-water path, kPa	95,5
13.	Aerodynamic resistance of air path, Pa	67,8
14.	Design operating pressure, MPa	7,84
15.	Design temperature, C^{o}	300
16.	Air temperature at system inlet, C^{o}	50

Estimation of PHRS dynamic characteristics showed that with nominal steam pressure and instantaneous opening of valves (on steam line) and gates (on air line) PHRS reached the rated power for not more than 60 s. However, as characteristics of valves and gates are not yet specified now, the dynamic characteristics of PHRS is assumed more conservative in design; it is assumed to reach the rated power for 150 s. (Table 3).

TABLE 3. PHRS Dyanmic Characteristics

T (s)	0	5	15	30	50	100	150	200	250	1000
	0	0,006	0,08	0,17	0,32	0,69	1,05	1,02	1,0	1,0

Results of calculations of reactor shutdown cooling parameters in actuating four channels of PHRS and fail-safe operation of impulse safety devices are presented in Fig. 4.

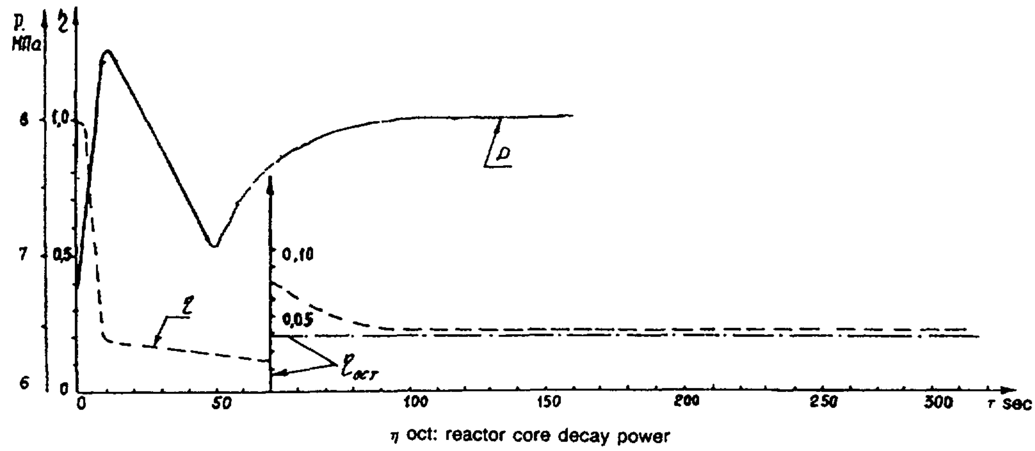


FIG. 4. Curves of decay $\eta(\tau)$ and pressure in the SG-P(τ) with PHRS operating and loss of all power supply sources.

PHRS is designed to operate at 2,7% of the rated load; reduction in the decay power of a reactor to this value occurs in 375 s, following the protection system operation, excess of the reactor decay power in respect of PHRS capacity leads to single operation of impulse safety devices for 10 s, after pressure drop to 6,9 MPa (set point for closing impulse safety devices) the steam generator valves will close and the further development of the process proves the PHRS capabilities to cool down the reactor installation. At present investigations of dynamics of a reactor provided with PHRS without operation of emergency feed motor pump and fast-acting steam dump (reducing) station -A are still in progress; the preliminary conclusions are as follows:

(1) During operation of four PHRS channels at power 2,7 of the reactor rated power and fail-safe operation of impulse safety devices (IS) a single opening of ISD takes place for 10s with the discharge of a portion of steam, after that ISD close for 50s and PHRS provides reactor cooldown

(2) If impulse safety devices on a steam generator fail to close (following first opening of ISD on all steam generators) PHRS provides reactor shutdown cooling but reopening of ISD on three steam generators does not take place

(3) If one PHRS channel fails to be actuated cyclic opening of ISD on the steam generator with failed channel will occur, however, the function of reactor shutdown cooling is performed. Evidently, provision of a nuclear power plant by PHRS would increase safety of NPP operation. However, decision of excluding operation of emergency feed motor pump and fast-acting steam dump (reducing) station-A should be taken on the basis of comparison of safety indexes characteristic for each alternative.

3.4 MONITORING SYSTEM FOR SAFETY SYSTEM AVAILABILITY

This system is intended for continuous monitoring of discrete position of safety system elements with display of a combined signal on the control board.

In normal operating conditions safety system channels are maintained in the following modes:

- waiting mode
- test-run mode
- under repair (for 2 shifts, maximum, afterwards the unit must be shut down).

When safety system channel is expected to be repaired two other channels should be tested to detect latent failures.

The monitoring system for safety system availability operates with the aid of the computer control system (CCS) according to two programmes: for waiting mode and test-run mode. In case of non-stationary position of a safety system element its location is detected by the computer, the cause of its unavailability is established and appropriate measures are taken to eliminate it.

The use of the monitoring system for safety system availability permits to:

- minimize inadvertent errors of personnel
- have continuous data flow displayed on the control board concerning the availability of each of the three safety system channels and their ability to perform their functions
- control and eliminate in due time unavailability of safety system elements.

Thus, adoption of the monitoring system for safety system availability makes a considerable contribution to reducing the probability of accident development into beyond design basis.

3.5 SYSTEM FOR PRESSURE SUPRESSION AND CLEAN-UP OF ACCIDENTAL RELEASES

System for pressure supression and clean-up of accidental releases from the containment is designed to prevent excess pressure rise above the permissible level which may be the case in the event of a beyond design basis accident and result in the loss by the containment of its functional features.

Design filter capacity should correspond to maximum values of activity resulting from the core melt-down.

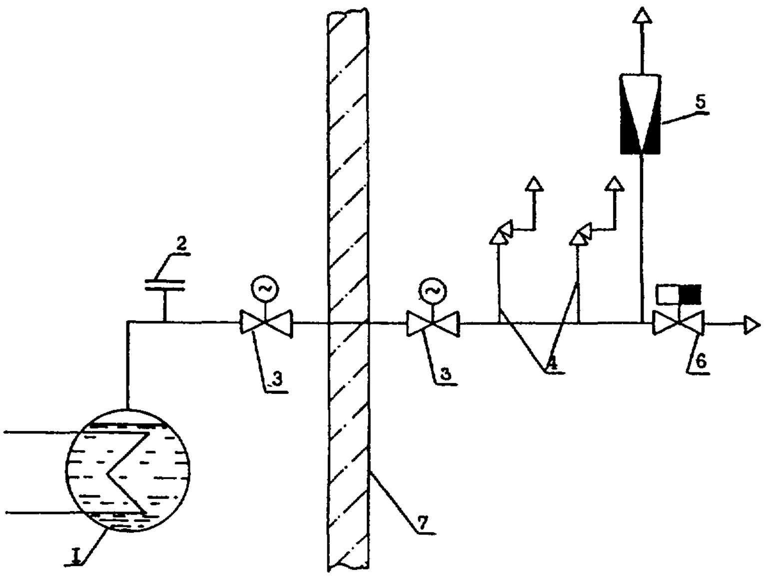
TABLE 4. Possible Redundancy of Functions Performed by Active and Passive Systems for Alternative 1

1	Functions 2	Operation of passive systems only 3	Operation of active systems 4
1	Primary core flooding	Accumulator of 1 stage	Accumulator of 1 stage
2	Complete core flooding	Accumulator of 2 stage (a)	Accumulator of 2 stage (a) or pump with a capacity of 600-700 m^3/h
3	Core make-up feed	Accumulator of 2 stage (b)	Safety injection pump
4	Heat removal from secondary system	PHRS	Auxiliary feed motor pump + turbine condenser
5	Core make-up feed after evacuation of accumulator of 2 stage	PHRS condensation	Auxiliary feed motor pump + turbine condenser or safety injection pump
6	Protection of primary containment from excess pressure	Filter venting from primary containment	Filter venting from primary containment
7	Limitation of leaks through containment	Double containment with filter venting from the annulus	Double containment with active ventilation in the annulus
8	Preparation of the power unit for adopting appropriate measures as a consequence of loss of coolant accident		- pump with a capacity of 600 m^3/h (coolant pump for scheduled operation of cooling pond pump operating in the sump) - sprinkler pump - active ventilation of containment and annulus and cleaning effluents
9	Residual heat removal during deenergizing	PHRS (without cooldown or to 110°C)	Auxiliary feed motor pump + turbine condenser (without cooldown or with cooldown to 110°C)
10	Bringing the unit to a cold condition	PHRS (to 110°C)	Auxiliary feed motor pump + turbine condenser (to 110°C) - coolant pump for scheduled operation (to 70°C)

3.6 LOCALIZATION OF LEAK FROM PRIMARY SYSTEM WITHIN SECONDARY SYSTEM (STEAM GENERATORS)

The system is designed to prevent releases of radioactive materials into the atmosphere in case of heat exchanger tube rupture or steam generator header leak of considerable size in the primary circuit.

Should the considerable leak be detected from the primary system into the secondary system the localization system is actuated and the active fluid returns to the containment (figure 5).



1. Steam Generator
2. Membrane
3. Quick-operating Valves
4. Impulse-safety Devices
5. Quick-operating Reducing Plant
6. Quick-operating Shut-off Valves
7. Containment

FIG. 5. Leakage from circuit I into circuit II.

3.7 SYSTEM FOR CONTAINING AND COOL-DOWN OF MELT CORE OUTSIDE THE REACTOR VESSEL (CORE CATCHER)

In the process of implementation of research and development work in the Soviet Union the alternative designs for containing melt core debris outside the reactor vessel are considered in spite of the low probability of melt core outcome of the pressure vessel. Presently in the Soviet Union and majority of other countries developing the nuclear power industry various designs of equipment and technology capable of confining the melt core are being studied along with other similar problems. By this time the research has not been completed and therefore none of the existing core catcher designs can be recommended for use.

As results have shown the system for containing the melt core is not adequate as to contribution to increasing safety. However, modification of system for localizing core melt accident and preventing it from further development needs thorough consideration.

Introduction of the localizing system of this kind would make it possible to prevent releases of radioactive materials into the environment in case of maximum fuel damage and thus ensure high level of nuclear power plant safety inspite of the very low probability of such accident. Therefore in this country the study is still in progress and the Government encourages efforts in this field participating in various international programmes devoted to this subject.

In case of obtaining successful results of the investigations that is adequately justified and acceptable engineering solution, the system for containing the melt core outside the reactor vessel will be incorporated into the design.

4. CONCLUSION

To estimate the efficiency of the proposed systems the probabilistic safety analysis of VVER-100 design was conducted without taking into consideration the above mentioned measures and including them.

The probability of the occurrence of the core melt-down and excess of the individual dose regulated by the standards were chosen as probabilistic indexes.

In estimating probabilistic safety indexes of NPP input data on frequency of the occurrence of initiating events and component failures were assumed on the basis of statistics and equipment specifications.

It should be noted that input data are sufficiently conservative and margin on an absolute probability value may be quite large.

However, this does not have an effect on a relative value of increase in safety level.

Estimation of effect of various initiating events on safety indexes allowed to distinguish among them a group of critical initiating events the contribution of which to the probability of core melt and excess of the reference dose amounts to 98-99 per cent.

The include:

- failure of heat removal in the secondary system
- de-energizing
- leak from the primary system into the secondary system
- small-size and medium-size leaks.

Evaluation of effect of additional safety measures adopted on the basis of present proposals (not taking into account the above mentioned measures) on the critical group of initiating events and as a consequence - on the probabilistic NPP safety indexes as a whole shows that:

(1) On probabilistic index of core melt safety level increase by a factor of 40
(2) On probabilistic index of individual dose exceeding the reference dose safety level increases by a factor of 100
(3) Above mentioned results of estimation of gain in safety indexes are appropriate and should be verified at the stage of project development. At the same time on the basis of these results it would be possible to estimate the efficiency of additional systems and develop methods of further NPP safety increase, particularly, probabilistic assessments of critical initiating events showed that for further safety improvement (below 10^{-6}) per year) modification of equipment would be necessary (for example, improvement of reliability of steam dump systems, primary coolant pump seals), as well as development of special diagnostics.

Thus, the probabilistic safety analysis methods prove high efficiency of the above mentioned measures.

Such measures as:

- reactor upgrading
- passive heat removal system
- system for localizing leaks from the primary system within the secondary system etc. are major contributors to enhancing safety.

It should be noted that technical solutions considered are suitable for existing NPP and those under construction. Thus, adoption of the above mentioned measures would permit increasing significantly overall safety of nuclear power industry on the whole.

SAFETY ASPECTS OF U.S.-SPONSORED ALWR NUCLEAR POWER PLANT DESIGNS

J.J. TAYLOR
Nuclear Power Division,
Electric Power Research Institute,
Palo Alto, California,
United States of America

Abstract

The safety objectives of the Advanced Light Water Reactor (ALWR) Program, sponsored jointly by the Electric Power Research Institute and the U.S. Department of Energy, are defined so as to achieve a factor of 10 improvement in safety over present LWR reactors. The embodiment of this objective in a passively stable 600 MWe pressurized water reactor (PWR) and a boiling water reactor (BWR) designs is summarized. Both these systems utilize passive cooling mechanisms for emergency core cooling and containment cooling rather than active equipment. Some of the key safety features for the passive BWR are: natural circulation at full power, with free surface steam separation; isolation condenser for passive heat removal from RCS and containment; gravity drain emergency cooling; and steam injector. Some of the key safety features for the passive PWR are: natural circulation decay heat removal; gravity-driven ECCS with full-pressure tanks, depressurization, and low-pressure tank; and passive containment cooling. Limitations in measuring the safety of the design and of the plant in operation are associated with common-mode failure, external events, and human reliability inputs. Because of such limitations, claims for significantly greater safety than set by these objectives for the ALWR or any other concept cannot be accurately verified. Utilizing the industrial safety record as a measure is helpful but not adequate. The means of achieving safety at this level and measuring it are sound and consist of probabilistic safety assessment, industrial/regulatory standards, and the "drive for excellence. Even though human reliability cannot be accurately predicted, the strong emphasis in advanced reactor design on human factors and the reduced requirements for rapid operator response in the passively stable reactors significantly reduces the consequences of human error.

---

1. INTRODUCTION

EPRI has spent the last five years defining and shaping the safety requirements of the next generation of advanced light water reactors (ALWRs). [1] This work has been accomplished with key and highly experienced personnel of EPRI's member utility companies, with the reactor manufacturers and architect/engineers, and with the joint support of the U.S. Department of Energy (DOE) and is presently under review by the U.S. Nuclear Regulatory Commission (NRC). Two broad convictions come from that experience which will be discussed in this paper. First, we can define systems which are significantly safer, by a factor of about 10, than those that are operating today. Public and political acceptance as well as financial prudence demand such increased safety, regardless of the excellent safety record achieved to date with the present systems. Second, we must humbly admit that we do not yet have fully satisfactory methods of measuring safety improvement much beyond that factor of 10.

2. IMPROVED SAFETY OBJECTIVES

In the EPRI/DOE ALWR Program, a set of key technical principles has been established to guide the design:

- Highest attention to nuclear safety.
- Simplicity--to enhance safety, constructibility, operations and maintenance.
- Margin--a rugged, forgiving plant.
- Proven technology--reliance on demonstrated success paths.
- Human factors--attention to man-machine interface in every aspect of the design.

A quantitative overall safety objective has been established that core melt probability will be no greater than 10^{-5} per reactor year and the chance will be no greater than 10^{-6} per reactor year that a release of radioactivity from containment would result in a radiation dose greater than 25 rem at the site boundary. This objective is about a factor of 10 more stringent than has been achieved to date on typical U.S. plants as estimated by probabilistic safety assessment (PSA) methodology. As important as that objective is, it is not sufficient in itself, and so a detailed set of safety requirements for future light water reactors has been defined as part of the ALWR Utility Requirements Document developed by the program. Those total requirements are defined in depth in two volumes, which are in the final stage of preparation. Volume I contains top-tier requirements and includes general design requirements, design basis events, structural design bases, materials, reliability and availability, constructibility, operability and maintainability, quality assurance and licensing. Volume II consists of 13 chapters covering specific performance and design requirements for the entire nuclear plant from reactor core to the switchyard. The safety requirements are contained in Volume I and in Chapter 5 of Volume II.

These requirements are applicable to future light water reactors which utilize the same fundamental design concept as the present generation light water reactors. We term them "evolutionary" designs for that reason. It is through a large number of design improvements that the significantly greater degree of safety can be achieved over the present designs.

But another approach to safety has evolved in the ALWR Program. It has come from the effort to develop conceptual designs for light water systems in the range of 600 MWe unit output as compared to the 1000 to 1300 MWe plants which have emerged in the latter years of the present generation. In seeking to compensate for the loss of economy of scale with the smaller units, conceptual designs have emerged which take advantage of the small size to substitute passive for active systems for emergency cooling functions, achieving a substantial degree of simplicity which could then be reflected in reduced equipment and construction costs. These systems will meet the same quantitative overall safety objectives and the pertinent detailed ones defined in the Utility Requirements Document. Supplemental safety requirements are presently being formulated to reflect the significant changes in systems design, in particular the introduction of passive cooling and the elimination of active emergency cooling equipment.

3. PASSIVELY SAFE DESIGNS

The specific characteristics of these so-called "passively stable" designs have been presented in other papers (2-6), but I will take a moment to summarize briefly their passive cooling features. Conceptual designs have been developed for both a BWR, called SBWR by General Electric, the principal designer, and a PWR, called AP-600 by Westinghouse, its principal designer.

A schematic of the SBWR, which operates under natural circulation at full power, is shown in Figure 1. To achieve passive cooling capability, the suppression pool has been located above the reactor core so that the emergency core cooling water is provided by gravity. A containment heat removal system cools the suppression pool wall by naturally circulating water and has the capacity to cool the containment building passively for a period of three days. An isolation condenser, located in the suppression pool, transfers reactor and containment heat to the pool and is used to control reactor pressure passively without the need to remove fluid from the reactor vessel. Safety-relief valves are, therefore, not required to discharge steam to the suppression pool. Major reductions have been achieved in the amount of mechanical and electrical equipment and safety-grade systems in this design as compared to conventional BWRs, resulting in lower maintenance and surveillance test time and costs.

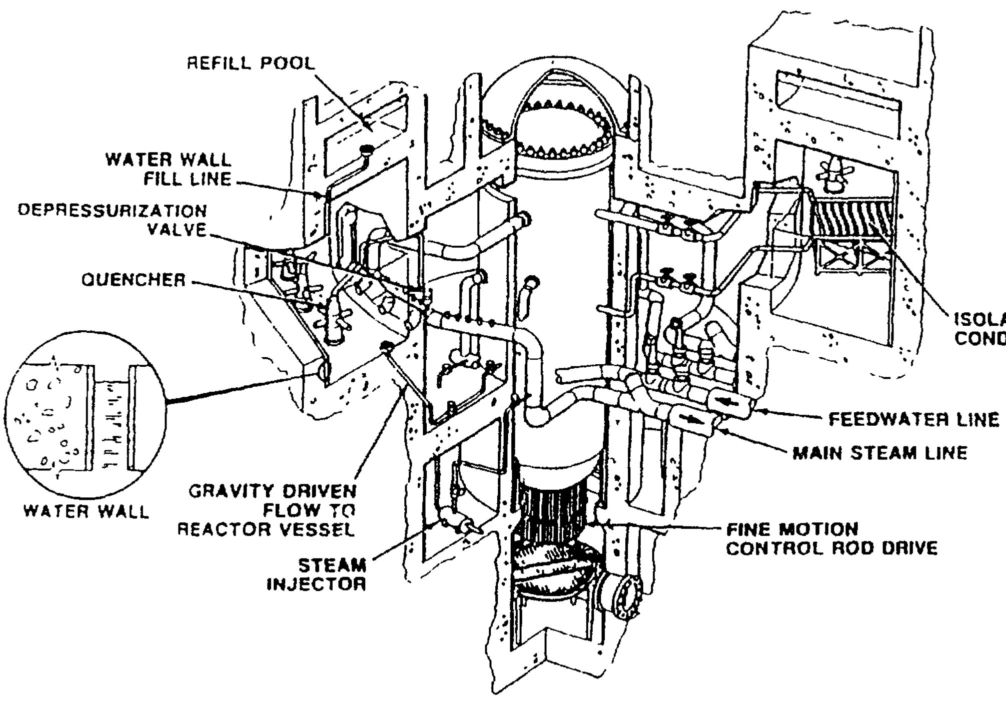


Figure 1. SBWR Features

Emergency cooling in the AP-600 is provided by a passive emergency core cooling system (ECCS) and a passive containment cooling system. The ECCS shown in Figure 2 consists of a combination of cooling water sources: gravity drain of water (from two core makeup tanks and a large refueling water storage tank suspended above the level of the core) and water ejected from two accumulator tanks under nitrogen pressure. Core decay heat can be removed through the steam generators or through a passive residual heat exchanger located in the refueling water storage tank. This heat exchanger transfers core decay heat to the refueling water by natural circulation.

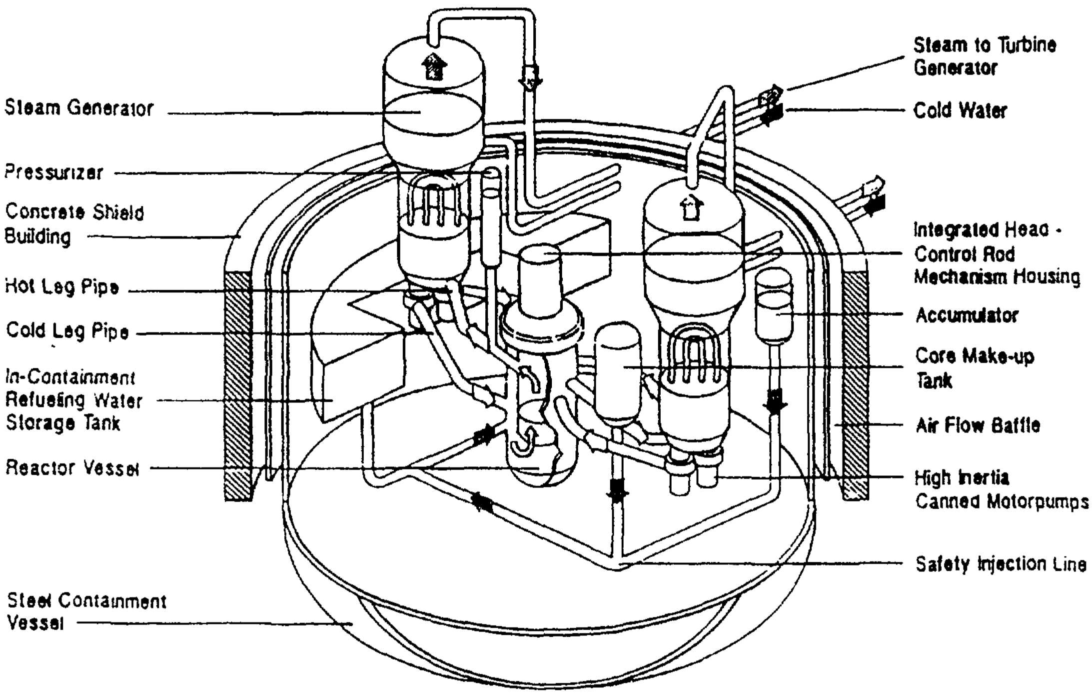


Figure 2. Advanced Passive PWR

The containment shell is passively cooled by evaporating water that is gravity fed from a large tank located above the containment. The heat is ultimately removed to the atmosphere by a natural circulation air system as shown in Figure 3). Only automatic valve operations (no operator action and no pump, diesel, or fan operations) are required to provide emergency core cooling and containment cooling for three days after a major maximum loss-of-coolant accident has occurred.

The use of passive cooling features has effected a substantial simplification of the AP-600. By comparison with a conventional 600-MWE PWR, bulk commodities of a passively stable PWR are reduced sharply: valves by 80%, large pumps by 65%, piping by 60%, heat exchangers by 50%, ducting by 35%, and control cables by 80%. Because no on-site emergency ac power is needed, many safety-grade active components have been eliminated, and the volume of buildings designed to nuclear-grade seismic requirements is reduced by 40%.

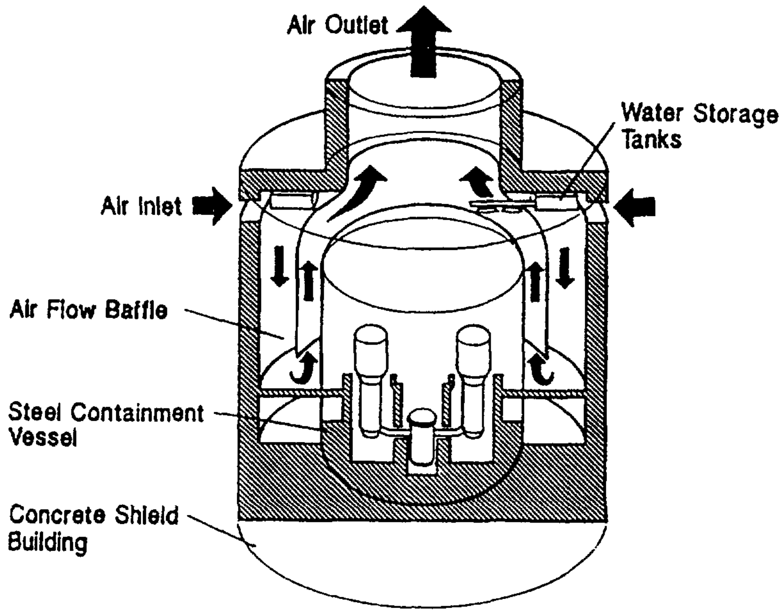


Figure 3. Passive Containment Cooling System

If these simplifications and passive cooling capabilities are confirmed in the detailed design and test verification phases of the program, major economies can be achieved which can be further enhanced by shipyard- and factory-based modular construction bringing construction times back to a manageable four-year time frame.

A more recent 340-MWe PWR design, called the SIR by its designers, Combustion Engineering and the UKAEA, shows similar passive cooling features and simplifications. If one looks out to even more advanced systems, passive cooling is also a primary feature: the high-temperature gas-cooled reactor (MHTGR) being developed by GA/Bechtel/Siemens, the sodium-cooled reactor (PRISM) being developed by GE/Argonne National Laboratory, and the PIUS design being developed by ABB Atom.

A broader aspect of the safety approach in the ALWR Program has been the creation of substantial international participation which enhances the input of safety experience and safety standards from utilities around the world. Cooperative agreements for participation in the ALWR Program are in place with:

- Taiwan Power Company
- Korea Electric Power Corporation
- Kansai Electric Power Company, Japan
- KEMA, The Netherlands
- ENEL, Italy
- EdF, France
- CRIEPI, Japan

4. MEASURING SAFETY

I've outlined with pride the promising prospects for improved safety in future light water reactors. But now I'll turn with humility to the problem of measuring that safety.

Would that one could dispose of the issue by claiming that the design is inherently safe or absolutely safe, but those of us who engineer and operate industrial machinery know that there is no such thing. And if we thought there was, the public would not believe it. Let us say rather that we've moved closer to that ideal through the increased utilization of inherent or passive features.

The primary overall level of safety measurement is to utilize PSA methodology to estimate and to assess these designs against the overall safety objectives set for them. But this is not fully satisfactory because of two limitations in the PSA methodology: the treatment of common-mode failure and human reliability input.

EPRI has done substantial work in defining and assessing common-mode failure treatment in probabilistic safety assessment. [7] In broad terms, this work indicates that common-mode failure plays an increasingly large role as the probability of core melt gets below 10^{-5} per reactor year. This finding combined with evaluations that show that external events, much less dependent on the differences in reactor concept, also begin to dominate risk potential as the core melt probability gets below 10^{-5} and as the overall probability of hazardous radioactive release gets below 10^{-6} per reactor year. This combination of the increased dominance of common-mode failure and failure through external events has led us to the conclusion that these probabilities are the lowest practicable in terms of confident measurement by existing methodology.

The other limitation in probabilistic safety assessment is the accuracy of the human reliability input. Experience and intuition indicate that reduction of human error is the most important potential way of improving safety, and yet our ability to measure this element of safety is still elementary. Present methods do not distinguish between the TMI-1 and TMI-2 control rooms, yet simple observation strongly suggests that the TMI-1 control room, because of its greater simplicity and greater visibility, fosters greater human reliability than the more complex control room of TMI-2.

EPRI has initiated a program to develop statistical data on the response of operators, in simulation training, to a wide variety of accidents. Commonwealth Edison and the Electricite de France both are contributing substantial amounts of data to this pool which in time, I believe, will provide a quantitative input to the PSA. Data at this time strongly suggests that our present human reliability input is substantially conservative.

The Severe Accident Management Program [8] which has recently been launched in the United States is an attempt to reduce the residual public risk from an accident through additional mitigation actions. The objective of the program is to familiarize the operators with recovery approaches which could be employed after a degraded core condition has occurred. Here again, ability is needed to assess the effectiveness of such approaches and reflect them in subsequent PSAs. With present methodology, we have limited accuracy in assessing the actual improvement in mitigation potential.

A final limitation in the use of PSA methodology to assess safety is a nontechnical one. The utility and the regulator can effectively utilize the results of such assessments since they are in probabilistic form. They are inscrutable to the layman and, therefore, not very useful in public communication.

One might ask why does not the nuclear industry depend on the time-honored method of measuring safety used today in essentially all other industries--the industrial safety record. By this approach, safety is measured by the length of accident-free experience to date. By that standard, the nuclear industry is substantially safer than any other industry operating today in the world. But as tempting as it might be to use that method, the TMI-2 accident showed the commercial nuclear industry that something more was needed.

And if there was any remaining doubt, the recent events at the Savannah River Laboratory should dispel them completely. The DuPont Company relied primarily on the outstanding industrial safety record at Savannah River to assess the safety of operations. That record was outstanding: the best in DuPont worldwide operations, which have a justified reputation for safety first. But that approach led to complacency which caused Savannah River to lag behind the steady nuclear safety improvement in commercial nuclear power plants in the post-TMI era. As a result, the Savannah River reactors are shut down. There has never been an injury related to a nuclear incident at Savannah River, and one of the three reactors completed 35 years of operation representing millions of man-hours of effort without one lost day of work due to an accident. It is clear that an outstanding industrial record, as important as it is, is not sufficient for nuclear safety.

So we are limited in our measurement of safety at this stage:

(a) to the use of PSA with its limitations;

(b) to adherence to the industrial and regulatory standards as a fundamental base which assures safe design, fabrication/construction, operation, and maintenance; and

(c) to the "drive for excellence" to prevent the onset of complacency.

Such a constraining position is not a poor one and is probably the best safety methodology that exists in any industry today. But if an improved quantification of human response could be developed, PSA could be used to assess quantitatively the benefit of simplification and improved human factors. More importantly, we would have a more cost-effective tool to detect, and correct for, the complacency that can lead to human error with serious consequences.

It is this higher level of safety which the passive plant designs are pursuing in the ALWR Program as well as in the advanced liquid-metal and high-temperature gas-cooled reactor development programs. Although we are depending upon engineering judgment more than on quantitative measurement, these passive designs and the simplification which they permit are expected to reduce substantially the concern about human error in future nuclear power plant operation.

REFERENCES

[1] TAYLOR, J.J., STAHLKOPF, K.E., NOBLE, D.M., DAU, G.J., Nucl. Eng. Des. 108, 19 (September-October 1988).

[2] DUNCAN, J.D., McCANDLESS, paper presented at American Nuclear Society (ANS) Topical Meeting on Safety of Next Generation Power Reactors, Seattle, WA, May 1-5, 1988.

[3] WOLFE, B., WILKINS, D.R., ibid.

[4] Nucl. Eng. Int. 32, 19 (November 1987).

[5] CONWAY, L.E., paper presented at ANS Topical Meeting on Safety of Next Generation Power Reactors, Seattle, WA, May 1-5, 1988.

[6] VIJUK, R., BRUSCHI, H., Nucl. Eng. Int. 33, 23 (November 1988).

[7] Benchmark of Systematic Human Action Reliability Procedure (SHARP), NUS Corporation/EPRI, EPRI Report NP-5546, December 1987.

Procedures for Treating Common Cause Failures in Safety and Reliability Studies, Pickard, Lowe & Garrick, Inc./EPRI, EPRI Report NP-5613, Vol. 1, February 1988, and Vol. 2, to be published.

[8] Staff Plans for Accident Management Regulatory and Research Programs, U.S. NRC SECY-89-012, January 18, 1989.

SPECIAL INVITED PRESENTATION

A PROCESS FOR RESOLVING SAFETY AND INSTITUTIONAL ISSUES OF ADVANCED REACTORS: REPLACING PUBLIC CONCERN WITH CONFIDENCE

K.C. Rogers

United States Nuclear Regulatory Commission
Washington, D.C.
United States of America

1. INTRODUCTION

Good evening, ladies and gentlemen. I am delighted to be with you this evening to participate in this important International Atomic Energy Agency (IAEA) and Argonne National Laboratory (ANL) international workshop on the Safety of Nuclear Installations of the Next Generation and Beyond. I wish to share with you this evening my perspectives on the potential for changes in the international community's perception of the safety of commercial nuclear activities, particularly, advanced reactors of the next generation. It is particularly appropriate that the Argonne National Laboratory, which is widely recognized for its expertise and programs in advanced reactor and fuel cycle technologies, is cohosting this international workshop with the IAEA. I also wish to acknowledge the International Atomic Energy Agency's active role in increasing the international community's awareness - that of the Member States, their governing bodies and responsible agencies - of the increase in global atmospheric CO_2 levels and acidification from the increased use of fossil fuels for electricity production and various process industry applications. The Director General, Dr. Hans Blix, and the Assistant Deputy Director, Dr. Morris Rosen, are to be commended for their concerns over these trends and their far-sighted view of the need to address the institutional issues of public acceptance of nuclear power as an option to ameliorate the increasing atmospheric concentrations of "greenhouse gases" and future climatic effects.

In this regard, however, I would like to offer a few caveats and suggestions on coupling the future potential of nuclear energy to the easing of greenhouse problems. In my opinion, the international nuclear community should steer a course that avoids either overemphasizing or minimizing the importance of the nuclear option in mitigating global greenhouse effects. Neither the collective actions of any single country nor the aggregate world-wide applications of a single technology can offer more than a partial solution to greenhouse problems.[1] Timely actions by all nations in adopting measures that are technologically, economically, and politically feasible will make a worthwhile contribution to at least delaying and mitigating the potential consequences of climate changes and sea level rises resulting from global warming.

Although there appears to be a rather strong scientific consensus that greenhouse effects are real and are already upon us, quantitative estimates in apportioning manmade causes and the costs and the effectiveness of these measures to reduce their impact are accompanied by large uncertainties and considerable controversy.[2] Nevertheless, in my view we cannot afford to await robust scientific confirmation of the accuracy of such estimates since this may be considerably delayed, if indeed ever realized. On the other hand, the societal consequences, should we guess wrongly on these matters, could be so momentous and adverse that a defensive strategy of remedial actions appears clearly justified on the grounds of prudency alone.

In this regard, increased worldwide investments in the nuclear energy option could make a useful, if modest, contribution to an "insurance philosophy" needed to garner international political support for a set of preventative and mitigative measures to alleviate the consequences of global warming. The challenge to the international nuclear community, then, is how to improve the technological, economic, and political feasibility of the nuclear option in all countries so that nuclear power can achieve a useful contribution in reducing greenhouse problems.

My topic for this evening is the constructive role the regulator can provide in helping resolve the safety and regulatory institutional issues involved in the introduction of advanced reactors. Before turning to that topic, let me briefly cite the findings of two recent U.S. Environmental Protection Agency reports to the U.S. Congress.[1,3]

As you know, many greenhouse gases are presently accumulating in the atmosphere, and the most important of these is carbon dioxide (CO_2), followed by methane (CH_4), chlorofluorocarbons (CFCs), and nitrous oxide (N_2O). The problem, according to the U.S. Environmental Protection Agency (EPA) experts is that at current emission levels, greenhouse gases are being released into the atmosphere faster than they are being removed. Once emitted, these gases remain in the atmosphere for decades to centuries. As a result, even if emissions remained constant at, say, 1985 levels, the greenhouse effect would continue to increase for more than a century. The EPA projects that carbon dioxide concentrations would reach 440-500 parts per million (ppm) by the year 2100, compared to about 350 ppm today, and about 290 ppm a century ago. Drastic reductions in human-caused emissions, of the order of 50 to 80 percent of CO_2 emissions alone would be required to stabilize atmospheric concentrations at current levels.[1] Even if all manmade emissions of these gases were eliminated, their concentration would remain high for decades.

The EPA believes that it would take as long as a century and possibly more for the oceans to absorb enough carbon dioxide to reduce atmospheric concentrations of CO_2 toward its preindustrial value. It would take at least half a century before the concentrations of CFCs and N_2O declined by half after all manmade emissions were eliminated. While uncertainties about the diverse effects of greenhouse gas buildup on global climate abound, these uncertainties are not about whether the greenhouse effect is real or whether increased greenhouse gas concentrations will raise global temperatures. Rather, the uncertainties lie in the timing and magnitude of global warming and its implications for our planet's climate, ecology, and economies.

Thus, mankind's challenge is to establish credible strategies for the twenty-first century to reduce manmade emissions of the greenhouse gases, particularly CO_2. Accelerated substitution of nuclear fission energy on an international scale in the next century could help achieve at least the reductions in CO_2 needed to stabilize atmospheric concentrations. According to an EPA scenario of a Slowly Changing World with Stabilizing (greenhouse) Policies,[1] nuclear energy could increase its present 5 percent contribution to the world's primary energy supplies to 14 percent by the end of 21st century, or with a scenario of a Rapidly Changing World with Stabilizing Policies, to 20 percent by this time. A subsidiary question then, and a worthy task of this workshop, is a definition of the principal institutional and other impediments to take acceptance of nuclear energy and how to reduce them. Tonight I will address one of them - public concern about the safety of commercial nuclear power, and how improved nuclear regulation might help reduce these concerns.

Many observers see the root cause of anti-nuclear sentiment as a "distrust of the technology itself, distrust of the entities controlling the technology, the conviction that safe use of the technology would require unreasonable expenditures or police-state measures, and plain fear of the devastation a nuclear accident can wreak".[4] I would add to this list two others: a deep-rooted concern about the effect of radiation on biological processes and the health of human and other ecological species, as well as a concern about final disposal of radioactive waste and decommissioning of radioactively-contaminated plants and facilities.

I believe the real test of public acceptance will come in the next decade or two as national decisions have to be made on replacement of electrical capacity including nuclear plants, environmental effects and the independence of energy supply are debated, and related national security and economic issues are considered. What is the proper role of nuclear regulators in the debate? I am inclined to share the belief of Michael Laverie of the French Service Central deSurete des Installations Nucleairs (SCSIN) that an enlightened public is the best guarantor for the future of nuclear power. A public that is well-informed about measures taken to ensure the safety of nuclear installations can reduce the likelihood of dramatic shifts of public opinion regarding nuclear power technology.

The U.S. Nuclear Regulatory Commission has issued over the past several years four major Commission policy statements which address the U.S. regulatory approach to existing and advanced reactors for enhanced safety. These actions should help to foster a greater level of public acceptance. They are the Severe Accident Policy Statement of August 1985, the Advanced Reactor Policy Statement of July 1986, the Safety Goal Policy Statement of August 1986, and the Standardization Policy Statement of September 1987. The Severe Accident Policy focused on criteria and procedures the Commission would use to increase severe accident margins in both existing and future plants and to certify future designs. It concluded that for existing plants a need existed for a systematic examination of each plant based on probabilistic assessment techniques to assure that there were no unrecognized outstanding vulnerabilities to severe accidents. This program, known as the Individual Plant Examination Program, or IPE, is presently in its early implementation phases by plant licensees.

The Advanced Reactor Policy has as its central purpose, improvement of the licensing environment for advanced nuclear power reactors by encouraging early discussions between the NRC staff and advanced reactor designers in order to permit timely Commission consideration of the new design safety characteristics, and of the regulatory implications of these new improved designs. The statement also put industry on notice by expressing the Commission's expectation that advanced reactors were to provide additional safety margins by utilizing simplified, passive, inherent, or other innovative features to accomplish reliably their safety functions.

The Safety Goal Policy, the most significant of the four in setting forth quantitative safety norms, established two qualitative safety goals and two quantitative objectives which together broadly defined an acceptable level of radiological risk to the public.

The fourth, the Standardization Policy, encouraged standardization of the entire power plant and certification of future plant designs. Its intent was to improve the licensing process by reducing the complexity and uncertainty of the regulatory licensing process for standardized plants. As you may know, elements of this policy have since been codified in the new Part 52 rulemaking, which establishes an improved regulatory framework for the licensing, construction, and operation of the next generation of U.S. reactors.

Implementation strategies developed for these policies are in what I would call an interpretative phase at present. The Standardization issues are primarily procedural in nature and are being addressed by Industry and the NRC's Office of General Counsel. The Safety Goal, Severe Accident, and Advanced Reactor issues on the other hand, are less procedural and involve substantive technical safety matters.

The final rulemaking to establish the new Part 52 to Title 10 of the Code of Federal Regulations became effective in May 1989. It provides for early site permits (prior to plant license application), standard plant design certifications, and combined construction and operating licenses. The new rule implements the Commission's earlier Standardization Policy Statement and embodies as much of the Commission's earlier proposed Standardization and Licensing Act of 1987 as our current legislative authority permits. The criteria in the new rule apply to both evolutionary LWRs and advanced reactor designs of both LWR and non-LWR technologies. Criteria to assess advanced reactor designs include scope of design to be standardized, level of detail to be standardized, plant options to be standardized, and requirements for prototype testing. The Commission believes the new Part 52 will constitute a major step in simplification of the licensing process, increase the scope and level of design detail necessary for licensing, provide greater public confidence in the technology, and reduce other institutional impediments to an option of nuclear power such as investment uncertainty.

The Safety Goal policy interpretation and implementation should provide overarching guidance for the Severe Accident and Advanced Reactor policies, since it contains the following four principal elements: establishment of a hierarchy of safety objectives; conduct and review of plant probabilistic risk assessments (PRAs); integration of risk reduction efforts; and identification of subsidiary quantitative safety targets.

The plan for implementing the Severe Accident policy for existing plants contains the following elements: examination and rectification of severe accident vulnerabilities in existing plants, development of generic containment performance improvements with respect to loadings from severe accidents, upgrading staff and industry training to improve plant operations, performance of a severe accident research program (SARP), assessment of vulnerabilities to severe accidents from external events; and development of a severe accident management program. The last three elements and the containment performance improvement element will likely affect future plant designs.

Severe Accident policy implementation and standardization for future plants applies to evolutionary LWRs, advanced LWR, and non-LWR reactors. The evolutionary LWR designs incorporate current state of art design for large 1200 to 1350 MW pressurized and boiling water reactors such as General Electric's Advanced Boiling Water Reactor, Combustion Engineering's System 80 Plus Advanced Pressurized Water Reactor, and Westinghouse's RESAR SP/90 Advanced Pressurized Water Reactor. Atomic Energy of Canada's small modular CANDU 3 pressurized heavy water reactor builds upon three decades of successful experience with the Canadian deuterium natural uranium (CANDU) concept, and may at a future date be added to the list of evolutionary water reactor plants available to be licensed in the U.S. These designs all appear to incorporate significant engineering refinements and advanced plant control systems over the respective predecessors for which there is an extensive engineering and operational base of experience.

The evolutionary LWRs all retain active engineered safety systems which appear to meet and exceed current NRC General Design Criteria. Current NRC licensing schedules call for completion of the ABWR review and issuance of a Safety Evaluation Report (SER) in mid 1990; completion and issuance of the Combustion Engineering System 80 Plus APWR in mid 1991; and completion and issuance of the SER for Westinghouse RESAR SP/90 Preliminary Design Approval by the end of this year. In a number of respects the evolutionary LWRs appear to exceed current NRC regulations; examples include greater core thermal margin, improved reactor vessel fabrication, designed-in bleed/feed cooling, capability for cavity/drywell flooding, and alternate AC power supply for emergency purposes. The evolutionary plants are expected to achieve a mean annual Core Damage Frequency or Core Melt Probability equal to or less than 10^{-5}, which is generally believed to be a factor of 5 to 10 better than what is typical of most current licensed plants. Moreover, these new designs also expected to exceed current licensing basis design requirements by reducing the site boundary (0.5 mile) whole body dose to less than 25 Rem for accident sequences whose cumulative frequency exceeds 10^{-6} per reactor year. This is a very demanding objective and one that is much more stringent than the current Safety Goal policy by several orders of magnitude, but it is a target for safety that appears worth aiming at given the public acceptance improvements that may be derived.

Demonstrable improvements in plant design in terms of markedly reduced potential for severe accidents and greatly reduced off-site consequences should lessen current public safety acceptance concerns, particularly with regard to emergency response. To convince the public that nuclear power is dependable and an environmentally preferable energy source, the steadily improving industry safety record will have to be continually demonstrated and documented over a long period of time.

I must say in all candor that the Commission and the industry are not yet in agreement on all evolutionary plant issues. The principal technical issues currently under debate for severe accidents include:

1. Timing of fission product release from fuel
2. Fraction of fission products released from the core
3. Chemical form of iodine and fraction released to and suspended in the containment atmosphere
4. Fission product aerosol removal from containment atmosphere
5. Amount of hydrogen generation (fuel clad oxidation extent and ex-vessel core-concrete interaction)
6. Hydrogen concentration criteria to prevent detonation
7. Containment overpressure protection

While the present technical debate is ongoing, I believe that ultimate resolution of these matters will reflect the achievement of a broad consensus within the U.S. scientific and technical community. Ultimately benefits will flow to the public and investors alike through safer plants which will reassure the public and result in greater investment protection.

What about the Severe Accident policy for the more advanced modular passive LWR reactors such as the Westinghouse AP-600, General Electric SBWR, Combustion Engineering's SIR, and possibly the Swedish ABB-Atom PIUS conceptual designs? For these advanced plants, the Commission expects to take the same basic approach as it is presently following for evolutionary plants. The passive plants depart more significantly from existing regulations than do the evolutionary plants. As you know, they rely on natural circulation both in water systems and in air systems for decay heat cooling under severe accident conditions.

Elevation differences are required to establish the necessary thermal heads from fluid density differences to establish natural driving forces. The NRC will require that these elevation differences be conservatively calculated to assure sufficient natural circulation.

Larger elevation distances may mean taller containment structures which would increase costs. Engineering a passively-safe plant is much more difficult than engineering an actively-safe or combined actively- and passively-safe plant! I would expect that extensive testing of engineering mockups of important passive engineered safeguards systems of these plants will be required to demonstrate with reasonable assurance the functionality and operability of these essential systems under adverse environmental conditions.

While industry naturally seeks a cost-optimized passively-safe LWR that is modular, smaller, easier to construct, and less costly, NRC's independent review which is rooted in obtaining a high degree of assurance of safety may require design changes beyond the cost-optimized level to provide additional safety assurance. Licensing review schedules for the four passive plant draft SERs are presently less certain than for the evolutionary plants: Final Design Approvals are presently estimated in the period from 1993 to 1995 with design certifications completed in the 1995 to 1997 period.

For the three Department of Energy advanced reactor designs, the modular high temperature gas-cooled reactor and two modular liquid metal fast neutron spectrum reactors, a general conceptual approach and specific criteria have been established. For these systems which incorporate "inherent" safety features, the key issues appear to be the following:

1. What range of accidents must be considered for design, siting, and emergency planning? What is the Complementary Cumulative Damage Frequency (CCDF) "risk curve" for each design?

2. How should siting source terms be calculated and used for designs which are significantly different from current generation LWRs? Is more research needed to support present assumptions?

3. How should the need for or adequacy of a containment building be evaluated? Can the functional equivalent of containment be provided in the fuel form, such as the MHTGR fuel microspheres, or is the time-tested defense-in-depth concept an argument for a conventional containment or a confinement structure?

4. How should the need for or adequacy of offsite emergency evacuations, sheltering, and drills be evaluated?

I consider these questions worthy topics for this Workshop to debate.

The Commission has or will shortly issue draft Safety Evaluation Reports on the MHTGR and the PRISM and SAFR LMRs.

There are a number of open issues pertaining to each concept, and further discussion between NRC and the Department of Energy on certain design bases for these advanced plants is in progress. The Advisory Committee on Reactor Safety has advised the Commission on the adequacy of design safety and enhanced margins of safety on all three designs, as well as the evolutionary and passive light water plants. For certain features, such as the lack of conventional containment, the ACRS has exhibited a degree of skepticism given the present stage of design effort.

I have not mentioned one other on-going review: the DOE and EPRI/Industry ALWR Requirements Document. The Requirements Document is a top down specification guide for the basic design features that the next generation of evolutionary and passive plants should offer. It reflects the operational features and capabilities the people who have operated the current generation of these plants for 20 years want and their insights as to design robustness and safety protection that is required. For the EPRI work, the line of safety protection is as I described earlier, commensurate with the core melt frequency goal of $\leq 10^{-5}$ per reactor year and 25 rem exposure of $\leq 10^{-6}$ per reactor year at the site boundary which readily achieves, with margin, the Commission's safety goals. A benefit of the Requirements Document is the establishing of utility requirements and NRC approval before the detailed final design of the advanced passive plants has significantly begun.

As a general requirement or early design scoping document for advanced PWRs and BWRs, the Commission has to strive for consistency in developing technical positions on generic safety issues in the EPRI Requirements Document on the one hand and design-specific issues in actual vendor designs on the other. We are finding that this is not always an easy task. Nevertheless, the draft Safety Evaluation Report for Parts I and II of the Evolutionary LWR Requirements Documents is scheduled for completion in May 1990; the schedule for review of Part III, the Advanced Passive LWRs, is presently under discussion with EPRI. Once the staff review of the EPRI requirements document is completed, a question remains about the legal standing of the Requirements Document and whether this should be ultimately codified into NRC's regulations, perhaps as an acceptable content and format document for an applicant to use.

What benefits, then, flow from independent regulatory review of these reactors of the next generation, and how will this activity help contribute to public understanding? I think there are several:

1. Independent scrutiny of complex designs by a regulatory agency first of all provides a check on the completeness, technical accuracy, and systems integration of the design. Independent review by a competent regulator with a non-vested interest should be reassuring to the public.

2. Publication of the Safety Evaluation Report for public information and comment, and the Design Certification hearing process itself, permits public participation in the resolution of key safety or environmental issues <u>prior</u> to actual design certification and subsequent

construction. This "up front" disclosure should minimize the level of disagreement on specific design issues and about the level of safety, thereby reducing public concerns.

3. The review process itself challenges designer and regulator alike to intensify efforts to enhance safety features; the Level 3 PRA requirement of Part 52 for example should help assure that there are no overlooked vulnerabilities to severe accidents, and provide a quantitative framework for design and possibly operational improvements which enhance safety.

4. Requiring essentially a full scope of design for the certification of the water moderated designs should offer both a safety and operational benefit, since experience has shown that the balance-of-plant can challenge the safety of the plant and contribute to reduced availability.

5. The requirement for construction and testing of a full-scale prototype of the advanced designs which incorporate inherent safety features is a prudent defense against unforseen systems integration problems for design concepts lacking maturity, assuming their maturity cannot be demonstrated in some other way. Successful prototype operation should develop investor, regulator, and public confidence in advanced plants.

6. The process of a structured review of new designs by a single agency can yield synergistic effects; safety insights developed from design solutions for a particular system in one plant may apply to another.

7. Finally, public confidence in advanced plants should increase since licensing authorities in several countries have concluded they can be safer than the current generation of plants.

I believe all these benefits, which stem from public confidence in an effective regulatory process, will help create an international atmosphere necessary to permit greater reliance on commercial nuclear energy in the future, and thereby help stabilize future emissions of carbon dioxide with its adverse environmental consequences.

In the interest of professional responsibility however, we must make clear the fact that nuclear energy will not constitute an absolute remedy for reducing <u>all</u> greenhouse gases and related climatic changes, but that it can contribute to this reduction, as well as provide additional time for further study of the climatic effects. Both are important benefits.

2. CONCLUSIONS

In conclusion, let me summarize the main points I have made:

1. Advanced reactors clearly have the potential to provide substantially greater safety than current generation reactors; this fact should ease public acceptance of nuclear power.

2. An improved regulatory process such as the provisions the new Part 52 to Title 10 of the Code of Federal Regulations can improve the safety of advanced designs and assure their safe operation, thereby increasing public confidence. In addition, Part 52 has been designed to provide stability to the licensing process.

3. Increased public confidence in the product and in the process should reduce the present major impediment to the expansion of nuclear power--public concerns about safety. Attendant improvements in the nuclear fuel cycle and successful demonstration of disposition of high level waste, which I have not talked about this evening, should help reduce public apprehension concerning radioactive wastes.

4. The international sharing of experience in design, development and research of the next generation of reactors and improvements in the fuel cycle will enable each nation to internalize that which is applicable to its own institutional structure and reactor technology experience. This sharing of experience will also upgrade international safety levels to which the domestic programs and safety standards of each country may be compared. There is much to be gained by international cooperation; ideas and concepts can be debated, promising developments can be jointly pursued, and various institutional solutions common to industry can be exchanged.

5. The drastic reductions required in carbon dioxide emissions alone in the 21st century in order to stabilize atmospheric concentrations of this major constituent of the greenhouse gases by the 22nd century could in principle be approached with an increase from nuclear energy's current approximate 5 percent contribution to a 14 to 20 percent contribution by the beginning of the 22nd century.[1] Historically, technical and economic substitutions of other fuels have been accomplished within such a time frame.

6. Converting public concern to confidence about the long term safety, economy, and environmental benefits of nuclear energy is probably necessary to permit a displacement or substitution of this magnitude in the century ahead.

Thus, the objectives of this Workshop are of the utmost importance. Since the effects you seek may well take a century or more to achieve, it is all the more essential that you begin this grand assignment immediately! Thank you for your attenticn this evening, and may I offer you my best wishes for continued progress in these efforts on your return to your respective homes.

REFERENCES

1 Policy Options for Stabilizing Global Climate, Draft Report to Congress, U.S. Environmental Protection Agency, Office of Policy, Planning, and Evaluation, February 1989.

2 "Scientific Perspectives on the Greenhouse Problem, Executive Summary," The George C. Marshall Institute, Washington, D.C., 1989.

3 The Potential Effects of Global Climate Change on the United States, Report to Congress, June 1989.

4 "Outlook on Public Acceptance," McGraw Hill Special Report, June 1989.

SAFETY ASPECTS OF NEW DESIGNS AND CONCEPTS FOR NUCLEAR POWER PLANTS

(Session VI)

Chairmen

G. PETRANGELI
Italy

S. ROSEN
United States of America

SAFETY ASPECTS OF NEW LMFBR DESIGNS IN EUROPE

P. BACHER
Direction de l'équipement,
Electricité de France,
Paris

G. HUBERT
Service Etudes et projets thermiques et nucléaires,
Electricité de France,
Lyon

France

Abstract

The licensing and start up of the Creys Malville 1200 MWe LMFBR (SPX1) and the safety analysis performed on the other european projects (SPX2, SNR2, CDFR) form a sound basis for the safety approach of the new European Fast Reactor (EFR) project. Prevention of whole core accidents, development of passive safety features taking benefits of the specific characteristics of pool type LMFBR, consistency in the containment strength to avoid weak point and cliff edge effects, allowance for adaptation to different national licensing procedures without major design differences in the NSSS, are some of the main safety orientations of the EFR project. Further studies will allow to precise some options, for example concerning the containment (e. g. hung or anchored safety vessel) or the decay heat removal systems (probabilistic assessment). However, previous studies give assurance that, in all case, design solutions already developped or under development, are able to satisfy stringent safety requirements.

1. INTRODUCTION

In 1988 some major utilities in Europe (in particular CEGB, RWE/SBK, EDF...) agreed to act jointly within the framework of the European Fast Reactor Utility Group (EFRUG) for studies of an European Fast Reactor (EFR). Major european D and C Co decided to answer to this initiative by forming the EFR Associates (EFRA), which became then the industrial partner of EFRUG.

Experience gained from safety studies, licensing and start up of the Creys Malville 1200 MWe power station (SPX1) is of course of major importance for the definition of the safety approach of future european LMFBR. In addition safety trends applied already to other european projects (such as CDFR in UK, SNR2 in FRG, SPX2 in France) form a basis for a common safety aproach. In this field, a particular attention must be paid to the recommandations and positive advice formulated in december 1988 by the french "Groupe Permanent chargé des réacteurs nucléaires" (french safety authorities technical experts) on the RNR 1500 (SPX2) safety report, and to the statement made by the ad hoc committee appointed by the German Federal Ministry of the Interior on the SNR2 concept. Among the common and innovative safety tendancies of european projects which will be foreseen for EFR, special emphasis can be made on:

- feed back of experience from Creys Malville,
- design approach and development of passive safety features taking benefits of the inherent characteristics of pool type LMFBR,
- prevention of whole core accidents which allows not considering them in the design,
- research of consistency and coherency in the containment strength to avoid weak point and cliff edge effects.

2. DESIGN APPROACH

The general design approach may be characterized for all european projects as a "defense in depth" approach, particularly applied to each of the barriers between active source and environment.

Taking benefit of the safety studies on previous projects, a list of design faults has been drawn up for EFR. The design of the reactor is largely based on analysis of these faults, which are expected to be representative of the most severe events of a given range of frequencies.

Table 1 shows the design criteria proposed for EFR design faults according to a classification of their estimated frequencies. It can be noted that these criteria are such that the higher the predicted frequency of a fault the lower the consequences must be. The design criteria for clad and fuel are voluntarily severe : if fuel melting cannot be avoided, as a limiting case in the design, it must not lead to a subassembly melting and any predicted fuel ejection must be strictly limited.

Although the rules of analysis are mainly deterministic (consideration of uncertainties, combination with aggravating failure and loss of off site power, etc.), complementary probabilistic approaches may also be used. The general aim is to assure that the probability of escalation of any particular family of events over design limits is less than 10^{-7} / year.

Such complementary aspects of deterministic and probabilistic analysis, combined with the feed back of experience from Phenix, PFR and Creys Malville, provide consistency of the design, insuring that no particular sequence of events could be a weak point in the overall safety approach. It gives also the possibility for the safety cases to fit each particular national requirements (the usual UK approach, for example, being more probabilistic oriented than the current french approach).

In the design approach due consideration is also given to internal and external hazards. Among the latter, earthquakes have a particular importance in LMFBR design. Combinations of faults with seismic loadings have to be taken into account because an earthquake, which affects the whole plant, could lead to failure of any non seismic qualified equipment, loss of off site power, etc.

TABLE 1. DESIGN CONDITIONS CLASSIFICATION AND LIMITING PLANT CRITERIA

Frequency : Reactor/yr (Guidelines)	Category	Plant Limits: RCC-MR (minimum requirements)	Dose target to: public (whole body dose) (1)	Fuel limits	Fuels Pin Clad limits	Plant Criteria
1	Normal Operation	A	50 µSv/year	No melting	No open clad failures	
10^{-2}	2	A	50 µSv/event	No melting	No clad failures except due to random defects	Plant should be able to return to full power in short term after fault rectifi-cations
10^{-4}	3	C	1mSv/event	No melting	Temp. limits not to lead to sys-tematic (i.e. large numbers of) pin failures	Plant should return to full load after rectification and inspection
	4	D	50mSv/event	Any predicted limited melting to be acceptable	No clad melting	Plant may not be economically recoverable

Design probabilistic limits : the consequences of a design condition, representative of a family event, must not exceed 4th category limits with a propability > 10^{-7}/yr.

(1) These targets must be considered as indicative limits. ALARA principle have to be used.

Among the design objectives for EFR, the trends for a more "forgiving" concept lead to minimize calls for operator actions (no requirement for operator action in the design analysis before 30 mn) and to developp passive features, such as possibility to remove residual heat by generalized natural convection.

The possibility of such generalized natural convection, in case of total loss of electrical supplies, has been taken into account in SPX1 and SPX2, on the basis of analytical codes, scale models and tests, notably on the Phenix reactor. A low power test will be also performed on SPX1. Nevertheless this event has been considered for SPX1 as a limiting case for the design and it was not foreseen to demonstrate the possibility to restart the plant after such an event.

One of the main aim of the EFR studies on this aspect is to improve the knowledge about natural convection in order to postpone as long as possible the need for energy supply. In case of positive results, it is foreseen to accept loss of electrical supplies as a more frequent situation, which would reduce safety requirements on diesel generators. Such an option has of course other implications than for the reactor block and sodium circuits ; consequences of loss of system such as cooling systems of the roof slab and the reactor pit, ventilation, handling devices, etc. have also to be investigated.

3. PREVENTION OF WHOLE CORE ACCIDENTS

To reach the main general safety objective for EFR, which is to keep a safety level no less stringent than a modern thermal reactor design, the consideration to give to HCDA prevention is of course of major importance. The orientation for EFR is to exclude whole core accident sequences from the design.

A large benefit can be taken in this field from the numerous studies which have been made on SPX1 accidental sequences, which concluded notably that the possibility of unprotected transients is not credible because of their low probabilities. The CABRI 1 experiments, carried out in an international environment and recently completed, strongly substantiate this conclusion since they show the absence of "cliff edge" effects. However, for each potential initiator of a core melt, systematic analysis have to be made for any new project, taking into consideration its own characteristics.

A first step, according to the defense in depth concept, is to avoid any escalation of design faults.

More specific developements are given below for some of the main initiators, taking into account safety features foreseen in EFR project.

3.1. Unprotected transients

The general probabilistic target for shutdown systems reliability is that their failure frequency must be less than 10^{-7}/year.

This requirement implies :

- 2 independant shutdown systems, each of them able to accomodate an additional single failure and made up of a trip system and an associated absober rod group,

- diversity between trip systems, rods and mechanisms,

- initiation, as far as possible, by 2 different physical parameters of the 2 shutdown systems for design events leading potentially to unacceptable conditions in the core,

- absorber rods efficiencies which guarantee that, even in case of single failure, the most penalizing reactivity insertion considered in the design is compensated by shutdown system insertion.

In terms of diversification it must be particularly underlined that, as in SPX1 and SPX2 options, trip of one group of rods is initiated by the cut-off of the supply to the electromagnetic couplings above the roof of the reactor, while for the other group, electromagnets are in sodium, and thus insensitive to relative deplacement of the core and the structures above the core.

Given this adequate design of the shutdown systems, an other requirement foreseen for the EFR safety analysis to reject unprotected event in the residual risk, is to show an additional line of defense in case of untripped condition (LOF, LOHS and TOP).

This additional line of defense can be :

- protective measures reducing the probability of a fault development,

- a grace delay before irreversible consequences which allow active counter measure (e.g. operator trip action),

- or an additional feature which insures rod insertion in case of trip failure.

This requirement of an additional line of defense, which has been also fullfiled for SPX2 and SNR2 ("third shutdown level"), leads to design additional features such as the "SADE" system, which insures direct scram magnet deenergization in case of loss of electrical supplies to the primary pump.

3.2. Decay heat removal

Loss of DHR leading to unacceptable consequences must be less than 10^{-7}/year. The design foreseen for EFR DHR systems is :

- the use of main heat transport system (steam generators) after trip under normal operation,

- the use of redundant safety graded Direct Reactor Cooling Systems consisting in sodium heat exchangers (DHX), intermediate loops and air heat exchangers (AHX).

The number, and eventual need of diversity, of these DRC systems has to be decided on the basis of a probabilistic study. The study which has been performed on the SPX2 DHR systems, which was very similar to the EFR design, gave the following orientations :

- the main initiator to consider is a loss of one of the DRC loop ; the most penalizing failure being a DHX leakage because of the long repair time,

- the question of need of diversity is very dependant on the type of common mode failure which has to be considered.

Because of the possibility of natural convection the active components failures have small consequences on the DHR reliability. If it is considered that simultaneous common mode failure of redundant passive components, protected against internal and external hazards, is not credible, the only real problem to deal with is the risk of successive failures of identical components. Therefore, the need for diversity of such components depends on the possibility of repair of the first failure before the next one occurs, in case of successive, but not simultaneous, common mode failures.

In other words, increased redundancy and short repair time of DRC passive components could be an alternative to a diverse design.

Nevertheless all types of common mode failures have to be assessed (risks of sodium freezing, dampers seizing, etc...) and this probabilistic approach is not yet finalized for EFR. Further studies and considerations are needed to precise the design of DRC loops. Several design solutions give assurance that, in all cases, the safety target can be satisfied.

3.3 Core support structures

Core support structure design shall be such that failures leading to unacceptable insertion of reactivity can be excluded and classified in the residual risk.

The relevant demonstration is achieved through :

- high quality levels during design and fabrication,

- adequate safety margins on loads,

- fail safe or fault tolerant design (strongback, diagrid),

- in service inspection and use of leak before break approach (primary vessel).

EFR design will take benefits from existing european designs (suspended main vessel, transition weld, strongback, diagrid), and the particular safety analysis which have been performed on this subject for former projects.

For example, the SPX2 analysis was the following :

Starting with a given core support structure design, the areas where the margins are least, with respect to stress limits, are determined.

In most cases, the assesment is made for a weld area, where the characteristics of the material are less favorable. The propagation of postulated defects located in these areas, during the plant lifetime, is studied. The postulated defects taken into account correspond to the maximum defects liable to exist after manufacture and inspection. Moreover, such defects are presumed to be perpendicular to the most severe main stress direction. These defects, as they appear at end of life (EOL), are then compared with the critical defects, under the most pessimistic design basis loading, which is generally the SSE. If the margin between the EOL defect and the critical defect is adequate, the objective set has been achieved and the risk of rapid core support failure is sufficiently low.

Should this not be the case, and if the ISI procedures available prove inadequate to detect the defect before it becomes critical, the designer must modify the structure. In this way, either a sufficient margin is obtained between the EOL defect and the critical defect, or it must be shown that the EOL defect will be detected before becoming critical (either directly or by its global effects). ISI devices are already available or are to be developped.

3.4. Containment

Among the potential initiators which have to be considered, a possible leak of the main reactor vessel is taken into account in all project designs. To avoid uncovering of the core and to ensure decay heat removal, two main types of designs have been developped : a hung safety vessel, as the Creys Malville one, or a safety vessel anchored to the reactor pit, as developped for SPX2.

According to the defense in depth concept, both designs must be able to cope with a beyond design scenario of a leak of the safety vessel following a leak from the main vessel. A specific procedure has been developped and implemented on Creys Malville, which allows the reactor pit to be protected and leaktight in case of sodium leak. For SPX2, a sodium resistant concrete behind the anchored safety vessel has been developped.

As both design are able to satisfy safety requirements, both are studied for EFR and the final decision will take into account other parameters such as cost, accomodation for implementation, etc...

Another item of consideration is to eliminate weak points in the primary containment and to achieve an homogeneous level of strength and leaktighness. In this way, the roof slab must have a resistance to static and dynamic loads consistent with the main vessel.

Following Safety Authorities request, such a study have been made for SPX2. To check the consistency of the primary containment strength, including a sodium wave impact under the roof slab, a dynamic energy of 150 MJ has been postulated. The study has shown the necessity, and the possibility, to improve the roof slab resistance.

Leaktighness resquirements for the secondary containment, consistent with the primary containment behaviour in case of unexpected contamination of the reactor cover gas, were also defined for SPX2.

4. SEVERE ACCIDENTS

The above design approach reduces the probability of severe accidents to a very low level. However, in line with the defense in depth concept, it is felt necessary in some countries to supplement this safety design approach by making allowance for events not considered plausible but representative of the risk to be considered in drawing up the emergency off-site plans. In this category the events foreseen for EFR, which have been also considered for SPX2 are :

- a complete melting of a fuel assembly for which, the total instantaneous blockage of one subassembly, is the reference scenario ; full benefit of the SPX2 studies and SCARABEE experiments will be obtained for the EFR case, the objective being to show that such a fuel melt cannot degrade into a large coremelt,
- a large sodium water reaction in a steam generator,
- a leak from the safety vessel following a leak from the main vessel (as seen above),
- a secondary sodium fire on the reactor slab (inside the secondary containment).

5. CONCLUSIONS

Based on the experience gained from former projects in Europe, including the Creys Malville start up, analysis of the SPX2 safety report by the French Safety Authorities and of the SNR2 options by a German BMI group of experts, a coherent and comprehensive safety approach is being elaborated for EFR.

Due to different national licensing procedures, some national tuning in the safety cases under consideration are to be expected, but would not lead to major design differences in the Nuclear Steam Supply System.

Therefore the common agreed concept should allow adaptation to national site specific requirements, without major changes.

SAFETY ASPECTS OF THE U.S. ADVANCED LMR DESIGN

D.R. PEDERSEN*, G.L. GYOREY**,
J.F. MARCHATERRE*, S. ROSEN***

*Argonne National Laboratory,
Argonne, Illinois

**General Electric Company,
San Jose, California

***Office of Nuclear Energy,
United States Department of Energy,
Washington, D.C.

United States of America

Abstract

The cornerstones of the United States Advanced Liquid Metal Cooled Reactor (ALMR) program sponsored by the Department of Energy are: the plant design program at General Electric based on the PRISM (Power Reactor Innovative Small Module) concept, and the Integral Fast Reactor program (IFR) at Argonne National Laboratory (ANL). The goal of the U.S. program is to produce a standard, commercial ALMR, including the associated fuel cycle. This paper discusses the (1) U. S. regulatory framework for design of an ALMR, (2) safety aspects of the IFR program at ANL, (3) the IFR fuel cycle and actinide recycle, and (4) the ALMR plant design program at GE.

---

1. INTRODUCTION

The Integral Fast Reactor (IFR) program at ANL is responsible for the irradiation performance, advanced core design methodology, safety, and the fuel cycle (including the fuel cycle facility) for metal fuel for the ALMR. An engineering-scale fuel cycle facility is being designed by ANL for installation in the Hot Fuel Examination Facility-South (HFEF/S) adjacent to EBR-II scheduled for hot operation in fall 1990. General Electric is responsible for managing the reactor plant design involving wide participation by U. S. industry, National Laboratories, and international participation. The work is in the advanced conceptual design phase, and key development and testing tasks are proceeding in parallel.

The design for the ALMR is based on the PRISM (Power Reactor Innovative Small Module) concept originated by General Electric (Ref. 1) and on the IFR (Integral Fast Reactor) metal fuel concept developed by ANL (Ref. 2). The basic elements of the concept are: (1) metallic fuel, (2) liquid sodium cooling, (3) modular, pool-type reactor configuration, (4) an integral fuel cycle, based upon pyro-metallurgical processing and injection-cast fuel fabrication, with the fuel cycle facility collocated if so desired. The ALMR concept is particularly responsive to long-term energy supply needs by nature of metal fuel's high breeding capability and to the need for a secure fuel cycle with actinide recycling to ease the long-term waste disposal task.

In the ALMR concept, the liquid sodium coolant operates at atmospheric pressure, and maintains a design point margin to boiling greater than 400K (700°F). This eliminates the need for a pressurized primary system and thick-walled pressure vessels. With its high thermal conductivity and specific heat capacity, liquid metal cooling enables the ALMR to operate at decay heat levels in natural circulation, without the need for forced flow. Liquid metal cooling permits a compact core configuration that complements the neutronic advantages of metal fuel and an enhanced fast neutron energy spectrum.

2. REGULATORY FRAMEWORK

The ALMR Program is carried out taking into account continuing changes in the regulatory environment; changes which aim at achieving both improved safety and simpler, more predictable licensing of nuclear power plants. Key aspects are discussed below.

Advanced Nuclear Power Plant Policy

The U.S. Nuclear Regulatory Commission (NRC) established a policy on Advanced Nuclear Power Plants. This policy encourages interaction between the designers of advanced concepts and the NRC at early stages of the design process. The policy states that advanced reactors should provide at least the same degree of protection of the public and the environment as is required for current reactors, and that advanced reactors are expected to provide enhanced margins of safety. The following desirable characteristics are suggested in the policy for advanced reactors.

- Highly reliable, less complex shutdown and decay heat removal systems; use of inherent or passive means are encouraged.
- Longer time constants to allow more time before reaching safety system activation.
- Simplified safety systems, reduced requirements for operator actions.
- Reduced potential for severe accidents and consequences by inherent safety, reliability, redundancy, diversity, and independence in safety systems.
- Reliable equipment in the balance of plant, or safety system independence from the balance of plant, to reduce challenges to the safety system.
- Easily maintainable equipment and components.
- Reduced radiation exposure to plant personnel.
- Defense in depth by multiple barriers to radiation release and by reducing the potential for and consequences of severe accidents.
- Features that are based on existing technology or which can be established by development programs.

Safety Goal Policy

A policy on Safety Goals has also been established by the NRC. The central principle of this policy is that the risk posed by nuclear power plants to the neighboring population should not exceed one-tenth of one percent of the accidental fatality and cancer risk resulting from all other causes, and thus represent not a significant additional risk. The specific implementation of this policy has not yet been established by the NRC; however, the Advisory Committee for Reactor Safeguards (ACRS) has made its recommendations on this subject. The ACRS recommends as a general guideline that the likelihood of a large radiation release be less than 10^{-6} per reactor year. The ACRS also recommends separate guidelines for prevention of severe core damage and for mitigation, implying that some mitigative capability be required even if the safety goal is shown to be met by preventive means alone. The recommended guideline for mitigation is a minimum of less than one chance in ten for a large radiation release for the entire family of core melt scenarios.

Standardization

In view of the serious difficulties and delays experienced in the nuclear power plant licensing process, there has been a general agreement that the U.S. licensing process requires reform and that a key ingredient is the certification of standard plant designs. The NRC has recently completed a new regulation titled Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants (Code of Federal Regulations Title 10, Part 52). This regulation establishes the process for standard plant design certification. For new designs, which differ significantly from the established light water cooled reactor technologies, it calls for operation of a full-size prototype. The first commercial plant, licensed through the conventional licensing process, could serve the role of the prototype.

Evacuation Planning

A major contributor to regulatory delays in the U.S. has been emergency planning. Particularly troublesome aspects have been the detailed off-site evacuation plans and exercises, involving numerous local agencies, and the provisions for rapidly alerting the neighboring population to prepare for evacuation. It is generally agreed that on-site emergency planning is prudent, and also that provisions for off-site actions, such as communication links with certain local agencies are reasonable. However, the situation could be much simplified if requirements for detailed off-site evacuation plans and exercises and provisions for early warnings, such as sirens, could be eliminated. While the NRC has not reached a formal position on this subject, the NRC staff has proposed to consider eliminating the troublesome aspects mentioned above if the plant meets certain criteria. The NRC Staff proposes that these criteria be that the probability be less than 10^{-6} per year that the lower level Protective Action Guidelines (1 REM whole body,5 REM thyroid) are exceeded at the site boundary for 36 hours after an accident, considering all accident events.

3. INTEGRAL FAST REACTOR PROGRAM AT ANL

The two major goals of the IFR development effort are improved economics and enhanced safety. The enhanced safety goal has focused on designing for reliance on inherent processes to provide neutronic shutdown and reactor cooling in response to accident initiators. While they are not considered to be part of the reactor design basis, the consequences of unprotected (i.e., without scram) accidents have traditionally played a significant role in the evaluation of safety performance and the determination of containment requirements for licensability of liquid metal-cooled reactors.

The essence of the passive safety is to provide for intrinsic LMR performance characteristics that maintain the balance between reactor cooling capability and power production and prevent core disruption in instances when engineered safety systems have failed. These response characteristics are achieved by use of inherent mechanisms, hydraulic, and neutronic reactor system properties, which are determined by the choice and arrangement of reactor materials.

However, the most significant safety aspects of the IFR program result from its unique fuel design. A ternary alloy of uranium, plutonium, and zirconium, developed at Argonne, based on experience gained through more than 20 years operation of the EBR-II reactor with a uranium alloy metallic fuel. In the IFR concept, the ternary fuel is injection cast as cylindrical slugs and placed inside the cladding. Liquid sodium bond in the fuel-cladding gap provides an efficient heat transfer medium that, along with the high fuel thermal conductivity, maintains low fuel operating temperatures. The fuel-cladding gap is sized for a low smear density (typically 75%) to accommodate irradiation-induced fuel swelling to permit high burnup. Fuel elements of U-19Pu-10Zr in HT9 (Martensitic) and D9 clad have been irradiated in EBR-II to 14.4 at.% and 18.4 at.% burnup, respectively as of June 1989.

IFR Fuel Thermal Performance

Many of the superior safety performance characteristics of the IFR ternary alloy fuel design can be traced to its thermal and mechanical properties. The low temperature gradient across the fuel gives a correspondingly small zero power-to-full power Doppler reactivity swing, resulting in reduced control reactivity requirements and less external reactivity available for accidental insertion. The low operating temperature also yields a smaller positive Doppler reactivity input in unprotected transients on power reduction. This permits other reactivity feedbacks such as axial and radial core thermal expansion, to overcome the small positive Doppler input associated with power reduction, resulting in self-adjustment of the reactor core power to equal available decay heat removal capacity in loss-of-heat-sink (LOHS) and loss-of-flow transients (LOF).

Under accident conditions, transient heating of metallic fuel produces cladding loading dominated by the plenum pressure. The similarity of the fuel and the cladding thermal expansion and the compliance of the porous fuel lead to negligible Fuel-Cladding Mechanical Interaction (FCMI) cladding damage. Fuel melting in a metallic fuel element does not result in a significant clad loading because of the available porosity and small fuel density decrease on melting. The high thermal conductivity of metal fuel results in the hottest fuel being located near the core exit. Six experiments M2 to M7 have been performed in the TREAT transient reactor to determine margins to fuel pin failure, failure location, associated mechanisms and consequences and to characterize pre- and post-failure fuel relocation. A full range of fuel burnup and fuel and clad compositions are to be investigated. Tests M2, M3, and M4 were carried out using EBR-II driver fuel pins with U-5 Fissium fuel. Nine such pins were tested under slow overpower transients, with burnup and peak heating conditions being the key test parameters. Three of the pins were tested to cladding breach.

Three similar transient overpower tests (M5, M6, and M7) have been performed, using five D9-clad U-19 Pu-10Zr fuel pins with burnups up to 10 at.% and one low-burnup HT9-clad U-10Zr fuel pin. Two of the ternary fuel pins were tested to failure. Posttest analyses and examinations of the test pins from those tests have been completed. Additional TREAT tests will be performed to expand the database for IFR reference fuels to higher burnups, HT9-cladding, and to evaluate the impact of high Pu fuel.

The general results of the tests are that metal fuel has a large margin to pin failure (about 4 times nominal power in an 8 second period overpower transient), and significant molten fuel extrusion into the plenum region. In the experiments where pin failure occurred, considerable sweepout and dispersal fuel was observed without blockage formation. Fuel extrusion can provide a significant source of negative reactivity feedback in preventing severe core melt accidents (Ref. 3).

Metallic fuels interact metallurgically with iron-based cladding materials. During normal operation, the rate of solid-state interdiffusion is no greater than the wastage in ceramic pins due to fission product attack of the inner cladding wall. During transient heating, cladding penetration by liquid fuel-cladding eutectic can contribute to cladding failure; however, the effect appears to weaken the cladding only by thinning the wall. Two major out-of-pile test programs on irradiated fuel are underway at ANL to investigate the impact of fuel-clad eutectics. They are the Fuel Behavior Test Apparatus (FBTA) and the Whole Pin Furnace (WPF) Tests. The FBTA apparatus tests a short segment (~ 1 cm) of an irradiated element to determine the cladding penetration by the fuel clad eutectic. The WPF program can test the combined effects of clad thinning, eutectic penetration, and fission gas loading upon clad integrity.

IFR Fuel Neutronic Performance

The metallic fuel form also offers favorable neutronics properties. Specifically, the absence of low mass moderating atoms in the fuel leads to a hard neutron spectrum, increasing the neutron production per neutron absorbed in the pin. This occurs both because of the higher η value for Pu^{239} with the harder neutron spectrum and because of the enhanced fast fission in U^{238}. The combined effect increases the number of neutrons available for breeding and parasitic losses (η_{eff}-1) from about 1.65 for oxide systems to about 1.95. Moreover, the effective heavy metal density is increased by use of the metallic fuel relative to the traditional oxide fuel form. Both of these characteristics can be used to increase core internal conversion ratio to a point where zero burnup reactivity swing is achievable in a three or four batch core with 12 to 20 month refueling interval.

The harder neutron spectrum attendant the metallic fuel form has two important effects on reactivity feedback coefficients. The negative Doppler reactivity coefficient, T dk/dT, is reduced by about a third relative to oxide systems. The positive sodium density coefficient becomes more positive by about 1/3. The net effect of the lower temperature rise across the pin radius and the shifts in reactivity coefficients is to make the coolant temperature rise component of the power coefficient larger than that which is vested in the fuel temperature rise. This partitioning of the power coefficient components (which is opposite to that of oxide fuel) is the key to favorable passive reactivity shutdown response attainable in the IFR.

IFR Fuel Local Faults Tolerance

Loss of cladding integrity of a fuel element during normal steady-state full power operation should not occur during the design lifetime of the fuel because of the margins included in the design of the fuel and cladding. However, stochastic fuel element failure must be anticipated, due to a random cladding defect which goes undetected during manufacture and inspection or due to random localized thermal, hydraulic or mechanical conditions within the fuel assembly.

Metallic fuel elements have a range of features that enhance their tolerance to local fuel failure events. These features include:

a. Fuel compatibility with sodium - no chemical reaction products.
b. High thermal conductivity of metal fuel - This results in very low fuel centerline temperatures, and reduced hot-spot temperatures for distorted geometries.
c. Low fuel clad mechanical interactions - reduction in clad loading.
d. Easy to fabricate fuel-allows easy attainment of high quality reprocessed fuel.

The major fraction of the original EBR-II experience was with uranium-fissium alloy. Recent experiments with ternary alloy fuel are confirming the anticipated excellent performance. Six Run Beyond Clad Breach (RBCB) experiments with predefected metal fuel have been completed with breach time of up to 223 days without observable fuel loss or opening of the breach site.

Anticipated Transients Without Scram

In the full spectrum of unprotected accidents, three specific initiators have emerged to serve as quantifiers of safety margins. They are: (1) the loss-of-flow (LOF) accident, in which power to the coolant pumps is lost, (2) the transient overpower (TOP) accident, in which one or more inserted control rods are withdrawn, and (3) the loss-of-heat-sink (LOHS) accident, in which feedwater supply to the steam generators is lost. For all three initiators, it is also assumed that the plant protection system fails to insert the shutdown control rods. These events are generally classed as anticipated transients without scram (ATWS). The key to successful prevention of core disruption under these conditions is the provision in the design for reactor performance characteristics that: (1) limit mechanisms leading to reactor damage, and (2) promote mechanisms responding to the upset condition and acting to restore the balance between reactor power production and cooling. An example of the first is the minimumization of the control rod TOP accident. This is achieved by maximizing the breeding potential and conversion of fertile uranium into fissile plutonium. This reduces the total burnup reactivity swing, the control reactivity requirement, and thus the available insertion reactivity.

Avoidance of both short- and long-term core disruption in ATWS events depends on (1) providing sufficient negative reactivity feedback to overcome the power-to-cooling mismatch and return the system to equilibrium at slightly elevated system temperatures, or alternately, (2) reducing the positive reactivity feedback components acting to resist the transition to system equilibrium. In this second respect, metallic fuel provides superior inherent safety performance in ATWS events, due to the reduced positive Doppler reactivity feedback associated with the small radial temperature gradient in the fuel (high thermal conductivity).

Full scale unprotected LOF and LOHS transients have been carried out in EBR-II (Ref. 4). These tests have confirmed the capability of the metal fueled IFR concept to respond to unscrammed accidents without core (coolant boiling or fuel failures) or system damage.

Severe Accidents

The probability of core meltdown is exceedingly remote; however, despite all possible design measures taken, a theoretical possibility of core meltdown (e.g., from complete and sudden loss of flow without scram or from complete, long-term loss of all decay heat removal systems) remains. Work to date has revealed three characteristics of particular importance to reduction of risk for these extreme scenarios: (1) the adiabatic Doppler feedback rate for metal fuel is equal or greater (more negative) than for oxide fuel, and (2) metallic fuel disperses upon melting giving rise to a powerful reactivity shutdown mechanism, and (3) resolidified molten metal fuel debris beds are highly porous and are coolable.

4. IFR FUEL CYCLE - ACTINIDE RECYCLE

The waste management potential of the IFR concept is promising but has yet to be demonstrated. The key technical elements of the IFR fuel cycle technology are based on metallic fuel and pyroprocessing. Pyroprocessing is radically different from the conventional PUREX reprocessing developed for the LWR oxide fuel. Chemical feasibility of pyroprocessing has been demonstrated. The next major step in the IFR development program will be the full-scale pyroprocessing demonstration to be carried out in conjunction with EBR-II. IFR fuel cycle closure based on pyroprocessing can also have a dramatic impact on the waste management options, and, in particular, on the actinide recycling.

For discussion of high-level waste management, it is convenient to categorize the nuclear waste constituents into two parts: fission products comprised of hundreds of various isotopes, and actinides comprised of uranium and the transuranic elements--neptunium, plutonium, americium, curium, etc.

The relative radiological risk factors for the fission products and actinides contained in the LWR once-through spent fuel waste are plotted in Fig. 1 as a function of time after discharge from the reactor. The radiological risk factor of the spent fuel is normalized to the cancer

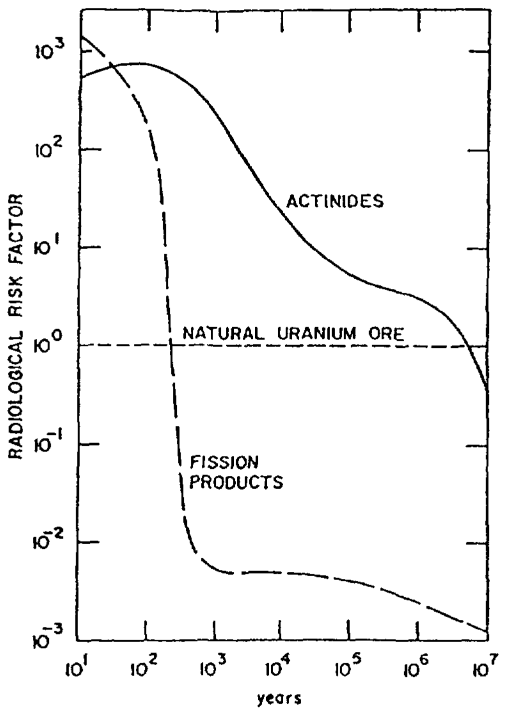


Figure 1. Radioactive Decay of High Level Reactor Waste

risk associated with the original natural uranium ore. Figure 1 illustrates the dominance of the long-term radiological risk of actinides over all other fission products. In a time span of the order of 200 years, the fission products decay to a sufficiently low level that their radiological risk factor drops below the cancer risk level of their original uranium ore. Actinides, on the other hand, have long half-lives and their radiological risk factor remains orders of magnitude higher than that due to fission products for tens or hundreds of thousands of years. From this point of view, therefore, there is a strong incentive to separate actinides and recycle them back into the reactor for in-situ burning.

The benefit is in the fact that the effective lifetime of the nuclear waste is reduced from millions of years to about 200 years. This would have an enormous impact on assuring the integrity of high-level waste for its lifetime and ultimately on the public acceptance of the nuclear power. But even if the actinides are removed and the lifetime of the high-level waste is reduced to hundreds of years, the need will remain for a geological repository.

IFR pyroprocessing makes actinide separation practical. In the IFR process, most of the actinide elements accompany the plutonium product stream. Those that do not, initially stay with the rare earths. But pyrochemical processes can separate rare earths from actinides remarkably well, in contrast to the difficulty of these separations in the PUREX process. The hardened IFR neutron spectrum is better for the actinide burning than that of any other reactor type. Thus the potential of the IFR concept to achieve the actinide recycling is very promising, although further research and development work is needed to fully establish its feasibility.

Material Control

The ALMR concept with the Integral Metal Fuel cycle is also responsive to concerns over the control of plutonium, the so-called "nonproliferation issue." In this fuel cycle, the plutonium is never completely separated from uranium, nor from much of the fission products, so that it remains in a diluted and highly radioactive form, making diversion extremely difficult, and requiring extensive processing to separate the plutonium. The plant layout also incorporates an optional on-site fuel cycle facility. With this option, fuel transport and the attendant diversion concerns can be even further reduced.

5. ALMR PLANT DESIGN AT GE

Safety Approach

The overall objective of the ALMR program is to develop a system with improved safety and competitive economics for the long term. The design is to

- be responsive to long term resource, waste, and security requirements,
- be responsive to the new directions in regulatory requirements, and
- incorporate lessons learned from past practices where certain design characteristics caused problems in licensing, public acceptance, and economic viability.

Examples of design characteristics found in the past to be troublesome in the licensing area are as follows.

- Reliance on multiple active systems to maintain a safe state.
- Resultant vulnerability to loss of electrical power and questions of reliability, especially that of decay heat removal.
- Reliance on operator actions to perform safety functions.
- Vulnerability to operator errors, especially in interfering with automatic safety actions.
- Difficulty in meeting anticipated transient without scram (ATWS) requirements.
- Vulnerability to large seismic events causing multiple failures.
- Vulnerability of the reactor system to faults in the balance of plant.

The safety goals and requirements established for the ALMR program include the conventional ones established in the past for nuclear power plants, and for sodium cooled power plants in particular, such as leak protection, fire mitigation, protection from natural phenomena, etc. However, in response to the recently evolving regulatory framework in the U.S. and the lessons learned from past experience, a number of additional safety goals were established for the ALMR program which may not have been used, or at least not emphasized, in the past. The most important of these are listed below.

- Passive decay heat removal, not vulnerable to operator errors.
- Strong inherent negative reactivity feedback for core reactivity control to maintain a safe state in the event of anticipated transients without scram (ATWS).
- Reactor protection (scram) system, well separated from the plant control system, with failure to shutdown to be less than 10^{-6} per demand.
- No operator action required to reach and remain in a safe state.
- Operator action cannot inhibit or override safety actions.
- High margins in ultimate seismic capability.
- Very low core damage probability, below 10^{-6} per year.
- Accidental radiation release probabilities and characteristics such that detailed off-site evacuation planning, exercises, and early warning will not be required.
- Passive and other innovative safety characteristics to be demonstrable in a prototype without damaging the plant.

<u>Innovative Plant and Safety Features</u>

Modular Reactor in Underground Silo

The ALMR plant layout is shown in Fig. 2. It consists of three identical power blocks of 465 MWe, for a total plant net electrical rating of 1395 MWe. Each power block consists of three reactor modules with individual thermal ratings of 471 MWt, each reactor module has its own steam generator which jointly supply steam to a single turbine generator. The reactor modules and the intermediate heat transport systems are underground, providing improved protection from tornadoes, missiles, and sabotage. The small thermal ratings of the individual reactor modules ease the task of decay heat removal, and reduce the potential consequences of a core damaging accident.

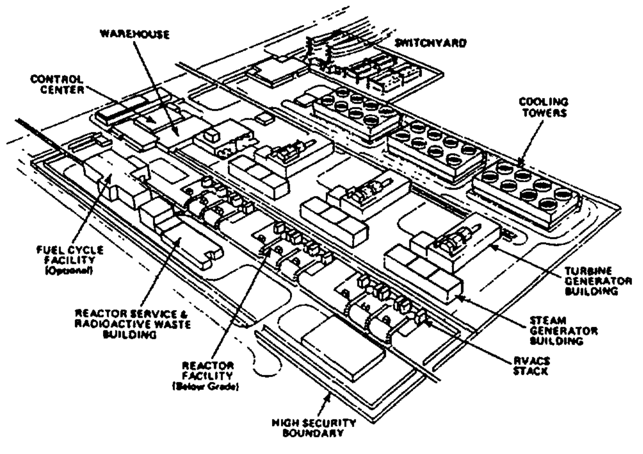


Figure 2. PRISM ALMR Power Plant-1395 MWe

Seismic Isolation

The reactor module with all the safety related systems rests on 20 seismic isolators (Fig. 3). The isolators essentially decouple the system from horizontal accelerations in the high frequency range which are of greatest importance in establishing design margins. Work is in progress to determine the cost of raising the safe shutdown earthquake capability from the original 0.3 g requirement to the range 0.5 to 0.75 g. The primary sodium circulation pumps are electromagnetic, with synchronous machines providing backup power for flow coastdown in the event that normal power to the pumps is lost. The synchronous machines are on the seismically isolated platform, and thus the potential for a seismic event degrading the flow coastdown capability is minimized.

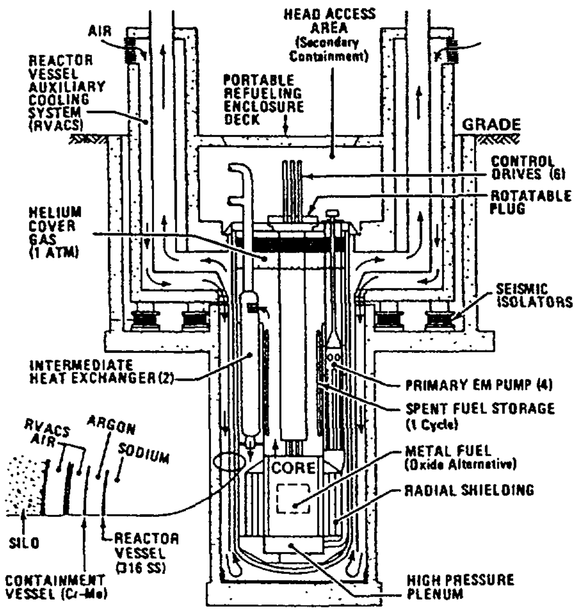


Figure 3. Reactor Module in Below-Grade Silo

Passive Decay Heat Removal

Normal decay heat removal is done by passing steam from the steam generator to the condenser. Two passive backups are provided. The first of these is natural circulation of the intermediate heat transport system and natural circulation atmospheric air flow through a shroud surrounding the steam generator. The ultimate decay heat removal is by the reactor vessel auxiliary cooling system: atmospheric air, naturally circulating around the containment vessel in the underground reactor silo, as indicated in Fig. 3. This system is always in operation, and is highly immune to human interference and to structural failure. Because of the large and multiple air passages, a 90% blockage can be tolerated with temperatures remaining below ASME level D limits (700C, 1300F).

Limited 1E Power Requirements

Because of the passive characteristics of the design, the requirement for Class 1E power are low, approximately 50 kilowatts for a nine module plant, and can be supplied entirely from batteries. Continuous power is required only for the reactor protection system sensors, electronics, and monitoring displays, together with basic lighting and ventilation for the operators.

Reactivity Shutdown and Control

The reactivity shutdown system consists of six control rods, associated drives and electronics. The requirement established for the system is that the probability of failure to shut down be less than 10^{-6} per demand. The insertion of any one of the six rods will bring the core to cold shutdown conditions. Each rod can be inserted into the core three different ways: rod run-in by the plant control system, fast run-in initiated by the reactor protection system, and gravity drop also initiated by the protection system. The reactor protection system is safety grade, automatic, well separated from the nonsafety grade plant control system, and located entirely in the reactor module vaults, away from the control room.

A key requirement placed on the ALMR design is that it maintain a safe state, through passive means, for anticipated transient without scram (ATWS) events involving loss of primary flow, loss of heat sink, and control rod runout. This is achieved through strong negative temperature coefficients, conservative power rating, and a core design with low excess reactivity. A key contributor to these characteristics is the metal fuel. The metal fuel has excellent negative feedback characteristics and furthermore, it provides superior neutron economy, so that the core can be designed for very low reactivity swing during the refueling cycle, and thus, with very low excess reactivity held down by control rods.

Figure 4 shows the reactor behavior under a combined condition of loss of forced primary flow and loss of heat removal by the intermediate heat transport system at full power and without scram. Through the inherent reactivity feedbacks and the passive air flow heat removal, the core outlet sodium temperature settles below the established temperature limit of 700C (1300F) and high margin to sodium boiling is maintained.

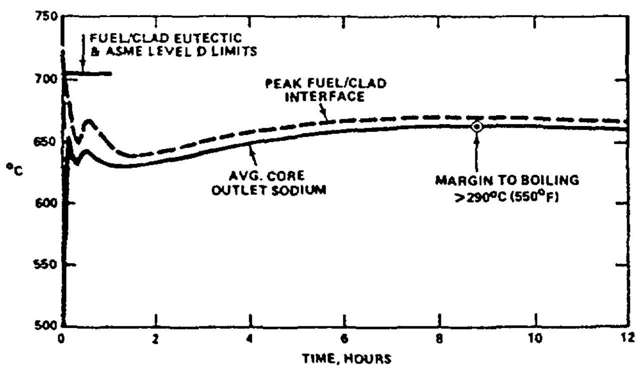


Figure 4. Sodium and Fuel Temperatures After Loss of Primary Forced Flow and Loss of Cooling by the Intermediate Heat Transport System at Full Power and With Failure to Scram

While the fuel-clad interface temperature exceeds the limit for several minutes, no fuel failures are expected.

Figure 5 shows the reactor behavior under an accidental rod withdrawal at full power without scram, adding 40 cents reactivity at the maximum capability of the control system, 2 cents per second. The power peaks at about 170% and settles at about 135% of rated. The sodium and fuel temperatures again settle out below the 700C (1300F) limit, and no fuel failures are expected. Various options are under considerations for limiting the anticipated inadvertent rod withdrawal to about 40 cents. The ideal situation would be if the total core excess reactivity at full power and with all rods withdrawn to their mechanical limits, could be limited to this figure. In the event that this proves to not be possible, because of core reactivity changes during the refueling cycle and because of uncertainties, other options are under consideration to limit reactivity addition by inadvertent rod withdrawal.

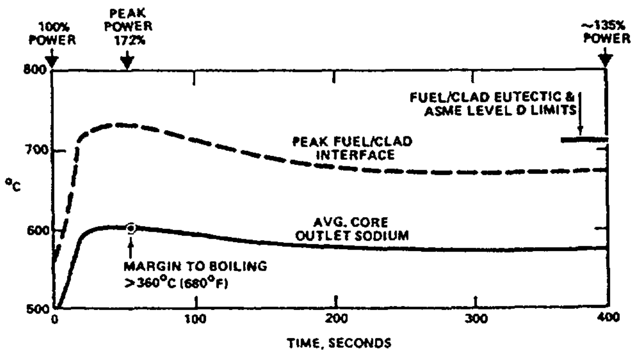


Figure 5. Sodium and Fuel Temperatures Resulting from Withdrawal of Control Rods at Full Power and With Failure to Scram (40¢ Reactivity Insertion at 2¢/Second)

Prototype Test

The ALMR effort includes the planning and design of a prototype plant test program to demonstrate the passive reactivity control and decay heat removal features, even under failure to scram conditions, and to provide a basis for standard design certification. While the exact route to the prototype test can remain flexible in response to possible changes in the need for the ALMR, the current judgement is that the lowest cost and risk approach is the building of a single reactor module, preferably on a U.S. Government site, for the purposes of the prototype test. This could be done in two phases: building only the reactor module and intermediate heat transport system for a safety test phase, and then adding the turbine-generator for a power operation phase. Alternately, the prototype testing could be performed on the first commercial power producing plant consisting of a single power block.

NRC Regulatory Review of the ALMR

Both the ALMR design team and the NRC recognize the desirability of interaction with each other during the design process to assure regulatory approval of the final product. Such interaction has been an integral part of the ALMR program plan in the form of regulatory review cycles, starting at the conceptual design stage. The first review cycle was accomplished during 1987 and 1988. A second review cycle is planned for the advanced conceptual design phase during the next three years. More formal regulatory review will begin with the preliminary design phase leading to preliminary design approval, and will continue during the final design phase, leading to final design approval and the licensing of the prototype plant. Finally, for the completion of the safety testing in the prototype, standard design certification will be obtained, opening the door to commercialization. The current reference schedule reaches certification about the year 2003; however, the schedule is flexible and can be adjusted to meet changing requirements.

A Preliminary Safety Information Document (PSID) was submitted to the NRC for review in November 1986. This document is similar to a Preliminary Safety Analysis Report (PSAR), but with less detail because of the conceptual nature of the design. During 1987 and 1988, numerous meetings and discussions were held among the design team, the NRC Staff, and the Advisory Committee for Reactor Safeguards (ACRS) in the course of the review. The results of the review are the draft Safety Evaluation Report (SER) prepared by the NRC Staff (Ref. 5) and the review letter by the ACRS (Ref. 6) reporting the findings.

The safety evaluations by the NRC Staff and by the ACRS are generally favorable. Overall, they find that the design is responsive to the NRC's Advanced Reactor Policy, namely, that the design has the potential for a level of safety at least equivalent to current plants, and that the design provides several passive and other desirable features enhancing the safety of the power plant. The passive reactivity feedback and decay heat removal features are recognized and credited by the reviewers, as are the long response time and low risk of core damage under many severe challenges to the plant, and the reduced dependence on and vulnerability to human actions and errors. The NRC recommendation was that the design and development continue.

As expected from any safety evaluation, and particularly from a preliminary, first-round evaluation, a number of issues and concerns were identified by the reviewers. Most of these are of a nature such that they can be addressed and satisfied as the design work progresses and more information and detail become available. Examples are the role and protection of the operators, sabotage resistance, sodium fire protection, and shutdown system diversity.

The issues raised in the review which have the potential for significant impact on the design and the overall approach are severe accidents and containment. That these major issues would be raised was not completely unexpected. The submittal for the first round of NRC review emphasized core damage prevention. The analyses show that the inherent reactivity effects and the passive decay heat removal reduce the probability of sodium boiling and fuel melting to a level sufficiently low to meet the NRC safety goal by means of core damage prevention alone, namely, that the probability of a significant radiological release is less than 10^{-6} per year. Nevertheless, analyses of radiological release were made to show compliance with regulatory site limits. The analyses conservatively assume that the containment boundary, which is completely sealed during operation, leaks directly to the atmosphere at a rate of 0.1% per day, and that all the fuel cladding has failed. The results show that with 100% of the noble fission gases, 0.1% of the other fission products, and 0.01% of the actinides released at the rate of 0.1% per day, the regulatory limits of 25 REM whole body and 300 REM thyroid dose are met for 2 hours at 0.5 mile and for 30 days at 2 miles. The results also show that with a still conservative but reduced release fraction of solid fission products and fuel materials, the 1 REM whole body and 5 REM thyroid Protective Action Guideline doses are met for 36 hours at the site boundary.

The submittal for the first round of NRC review was made before the ACRS made the recommendation that in meeting the safety goal, a mitigation capability of at least a factor of 10 be required for the entire family of core melt scenarios. In the first submittal, specific analyses were not made of potential impact on the containment boundaries by core energetic events or molten fuel movement. Such severe events were considered only in the probabilistic risk assessment and only in a simplified manner.

Both the ACRS and the NRC Staff have expressed concern about the unconventional containment concept used in the design, that is, the absence of a separate strong, pressure and temperature resistant containment structure completely surrounding the primary system, as additional protection for very low probability and unforeseen accidents. In the current design, the containment boundary is the reactor vessel head and the containment vessel (often called guard vessel) which completely surrounds the primary reactor vessel. The vessel head boundary is backed up by the head access area at a secondary confinement boundary. Concerns were also expressed about the positive sodium void effect and the possibility of fuel failure propagation in the event of fuel assembly blockage, however low the probability of such events may be.

Future Regulatory Review

The current phase of the ALMR effort, the advanced conceptual design, will lead to the next round of regulatory review by the NRC and the ACRS. For this phase of the work, the safety approach and goals of the ALMR program described earlier are retained, but are augmented in response to the evaluation received in the first round of regulatory review.

The goal of very low core damage probability through passive means is retained. In addition, very low probability events which could lead to severe core damage will be explicitly considered and their potential impact on the system boundaries will be analyzed to investigate the capabilities of the design to limit radiation releases. Various alternative containment concepts with additional or improved barriers to radiation release will be considered and evaluated, while retaining the highly reliable and passive decay heat removal system. The advanced conceptual design phase also includes numerous tasks which are responsive to other issues raised in the regulatory review and which aim to reduce the cost and improve the commercial aspects of the design.

ACKNOWLEDGEMENTS

This work was performed under the auspices of the U. S. Department of Energy, under contracts W-31-109-Eng-38 and DE-AC03-89SF17445.

REFERENCES

1. CRAIG, E.R., and BLUMBERG, B., Jr., Modular Nuclear Reactor for a Land Based Power Plant and Method for Fabrication, Installation, and Operation Thereof, U. S. Patent 45088677 (April 1985).

2. TILL, C.E., and CHANG, Y.I., "The Integral Fast Reactor," (Advances in Nuclear Science and Technology), Vol. 20 (1988).

3. BAUER, R.H., WRIGHT, A.E., ROBINSON, W.R., KLICKMAN, A.E., HOLLAND, J.W., "Behavior of metallic fuel in TREAT transient overpower tests," (Proc. ANS Topical Meeting on Safety of Next Generation Power Reactors), Seattle, Washington (May 1-8, 1988).

4. PLANCHON, H.P. et al., "Implications of the EBR-2 inherent safety demonstration test," (Nuclear Engineering and Design), Vol. 101, pp. 75-90, North Holland-Amsterdam (1987).

5. LANDRY, R.R., KING, T.L., WILSON, J.N., Draft Preapplication Safety Evaluation Report for the PRISM Liquid Metal Reactor, U.S. Nuclear Regulatory Commission, NUREG-1368 (June 1989).

6. Safety Evaluation Report for the Power Reactor Inherently Safety Module (PRISM) Design, letter by F. J. Remick, Acting Chairman, ACRS to L. W. Zech, Jr., Chairman USNRC (November 22, 1988).

SOME ASPECTS OF NEXT-GENERATION FAST REACTOR SAFETY

Yu.E. BAGDASAROV
Safety Division,
Physics and Power Engineerig Institute,
Obninsk,
Union of Soviet Socialist Republics

Abstract

In the paper variation in general approaches to validation of nuclear power plant (NPP) safety in the USSR in the last few years is followed. On the basis of this analysis and present-day knowledge a concept of fast reactor units of increased and feasibly attainable safety is proposed taking into account the elements of both deterministic and probabilistic approaches.

The results of the BN-800 power unit evaluation from the viewpoint of this concept requirements are presented.

INTRODUCTION

Prior to the accidents at the TMI and ChNPP (Chernobyl Nuclear Power Plant) there had been a sufficiently loyal attitude of governments and population to the development of nuclear power practically in all countries. This was favoured by a new technology, relatively more rigid requirements to NPPs design, construction and operation, acceptable levels of their environmental impact under normal operating conditions. The main deterrent factors were capabilities of industry and economic competitiveness. The above accidents revealed inadequacy of the measures taken to ensure NPP safety, potential hazards of severe accidents to personnel and population, possible large-scale ecological and economic losses as a result of them. This caused a sharp reduction (and in some countries total cancellation) of NPP construction and a transformation in approaches to NPP safety validation.

Until the ChNPP accident the NPP safety in the USSR was specified by the regulation codes having been in force at that time, including the ОПБ-82 and ПБЯ-04-74 codes.

After the accident at the ChNPP numerous organizational and technical activities were carried out on reinforcement of safety requirements to the NPPs under construction, to the analysis and increase of the operating power units safety, to the promotion of work on the issue of new regulation codes and up-dating of those currently available.

Further on, we shall dwell only upon those changes in approaches which pertain to the development of next-generation fast reactor designs and, in particular, of the BN-800 reactor.

The most important of them are:

- Postulation of specifications on taking into account the shock-wave impacts from explosible objects located in the vicinity of an NPP;
- The development of specifications on NPP siting with indicating the maximum permissible irradiation dose for

population at the 25 km-zone boundary under beyond-design accidents ("for NPPs and nuclear electricity- and -heat generating plants the human external radiation dose should not exceed 10 rem during the first post-accident year and the children thyroid internal radiation dose due to inhalation should not exceed 30 rem at a distance of 25 km from the plants");

- The necessity for the beyond-design accidents analysis at the NPP design stage with the demonstration of fulfilling the requirements to NPP siting under these accidents;

- Introduction into a new version under development now, of some probabilistic-analysis elements; in particular, limiting the permissible probability of severe accidents followed by exceeding the population irradiation indices at the 25 km-zone boundary by a value of 10^{-7}/(reactor year).

Of the whole complex of the NPP safety assurance problems (external impacts, accidents due to common causes, quality assurance during designing, construction and operation, training of personnel, etc) the greatest attention is being recently given by specialists to inherent safety properties of the reactor plant itself and to their improvement, to the advancement of the known reactor types and their systems and to the development of new ones. In so doing, primary emphasis is placed on the use of natural factors, self-protection, passive principles in safety systems.

In the same manner the safety problem is also being considered in the present paper.

In published papers and reports by some authors there are ideas of creating absolute safe power units. It seems to us that a more correct term would be a power unit of feasibly attainable safety.

In 1987, at I.V. Kurchatov Nuclear Power Institute a group of specialists representing various trends in nuclear power engineering were working. They considered necessary to pose a problem of step-by-step improvement of the NPP power unit safety characteristics: in the nearest 10-15 years to create and construct nuclear power units of increased safety, in the period after 2000-power units of feasibly attainable safety.

The recommendations of this group have not yet obtained a status of regulation codes.

Based on the work of this group, on new specification requirements to NPP siting in the USSR, as well as general trends in the world practice, the following concepts of fast reactor power units of increased safety and feasibility attainable safety are proposed below.

In the process an attempt to combine probabilistic and postulated safety requirements has been made.

1. CONCEPTS OF FAST REACTOR POWER UNITS WITH INCREASED SAFETY AND FEASIBLY ATTAINABLE SAFETY

1.1 Definitions of an Increased Safety Nuclear Power Unit and of That with Feasibly Attainable Safety

A. An increased safety power unit is the unit that provides as follows:

A1. No excess of the permissible levels of population irradiation and environment contamination at external emergency events characteristic of this area.

A2. No core rupture beyond the second limit of the nuclear fuel damage under all internal initial emergency events except those of low engineering probability.

Notes to A2: By "low-probability events" including personnel malfunction it is understood a set of internal emergency initial events with a total probability that does not exceed:

- 10^{-7}/(reactor year) for accidents resulting in a radioactivity release outside the outer protection barrier with an excess of the population irradiation and environment contamination levels;

- 10^{-5}/(reactor year) for accidents resulting in a reactor core failure beyond the second limit of nuclear fuel damage with radioactivity localization.

B. A power unit with feasibly attainable safety is the unit that ensures as follows:

B1. No excess of the permissible levels of population irradiation and environment contamination at external emergency events characteristic of the given area;

B2. No core damage beyond the second limit of a nuclear fuel failure under all internal emergency events, except those of low engineering probability, due to reactor plant inherent safety properties.

Note to p. B2: by the "low engineering probability events" including personnel malfunction, it is understood a set of initial internal emergency events resulting in a core failure beyond the second nuclear fuel damage limit with a total probability not higher than 10^{-7}/(reactor year).

General note to Part 1.1 By "the second limit of a nuclear fuel failure it is understood a failure and melting-down of some fuel in a group of 7 core subassemblies.

1.2 Radiation Release Criteria at Design and Beyond-Design Accidents

Radioactive products released from the primary circuit, NPP personnel and population radiation doses, conditions for introduction of emergency plans for various types of accidents and their probabilities of realization are determined by the diagram.

1.3 Inherent Safety Requirements

In order to achieve the characteristics of nuclear power units with increased safety and feasibly attainable safety it is necessary to make the most use of the fast reactor inherent safety properties and of safety systems based on passive principles, in particular:

- large accumulating capacity of sodium circuits that provides a time reserve for operators' intervention into beyond-design accident control with the aim to restrict its consequences;

- natural circulation of sodium through the primary and secondary circuits;

- negative power and temperature coefficients of reactivity over the whole range up to the design limits of safety system operation;

Diagram showing the relationship between characteristics determining nuclear power plant safety.

	Radiation effects; permissible doses according to p.3.17 СП АЭС-79	Ultimate doses according to p.1.3 of "requirements to NPP Siting"	Intoduction of emergency plans zone of residual risk
Modern NPPs and requirements put to them	Design accidents, DBA, postulated external events (without account for accident probability)	Beyond-design accidents (without account for accident probability)	Hypothetical accidents (without account for accident probability)
NPP units with increased safety and requirements placed on them	Design accidents, postulated external events characteristic of the location site (without account for accident probability). Core failure below the second limit of nuclear fuel damage under all internal initial events with radioactivity containment within the outer protection barrier at the total accident probability higher than $10^{-5} \frac{1}{\text{reactor.year}}$	Core damage beyond the second limit of nuclear fuel failure under beyond-design accidents due to internal events with radioactivity release outside the outer protection barrier and an excess of the permissible level of population irradiation and environment contamination by the СПАЭС code at a total accident probability higher than $10^{-7} \frac{1}{\text{reactor.year}}$	Core damage due to internal events with radioactivity release outside the external protection barrier and an excess of ultimate doses for population irradiation and environment contamination in accordancewith requirements to NPP location at a total accident probability lower than $10^{-7} \frac{1}{\text{reactor.year}}$
Power units with feasibly attainable safety and requirements placed on them	Design accidents, postulated external events characteristic of a location site (without account for accident probability). Core damage below the second limit of nuclear fuel failure at internal initial events with radioactivity localization within the outer protection barrier due to inherent safety properties at the total accident probality higher than $10^{-7} - \frac{1}{\text{reactor.year}}$	A core damage beyond the second limit of nuclear fuel failure at beyond-design accidents due to internal events with radioactivity release outside the external protection barrier and an excess of permissible by СПАЭС population irradiation and environment contamination level at a total accident probability higher than $10^{-7} - \frac{1}{\text{reactor.year}}$	A core damage due to internal events with radioactivity release outside the external protection barrier and an excess of ultimate doses of population irradiation and environment contamination in accordancewith requirements to NPP siting at a total accident probability lower than $10^{-7} - \frac{1}{\text{reactor.year}}$

- elimination of the possibility of coolant loss at losses of piping and reactor vessel tightness;

- neutron field stability;

- capability of sodium and primary circuit special equipment to retain and accumulate radioactive fission product;

- passive fire-extinguishing systems;

- passive principles of negative reactivity insertion in case of emergency conditions arising due to modification of external core structural elements (control and safety rods, the reactor vessel, etc.);

1.4 Minimum List of Beyond-Design Accidents

Increased and feasibly attainable safety properties of the power unit should be demonstrated for the following situations:

- a total (partial) loss of primary circuit tightness over gas and sodium;

- total loss of power of a plant for a prolonged period of time: a loss of electric power system supply for a time period up to 24 hours and a failure of the reliable alternating-current supply (a failure in starting diesel generators) for a time period of up to 3 hours;

- unsanctioned insertion of available excess reactivity;

- a loss of forced cooling of a shut-down reactor;

- loss of system electric power and a failure to drop of safety rods actuated by the control signal;

- a local accident with fuel melting down in a single fuel subassembly;

- total long-term loss of normal heat removal.

1.5 Additional Postulated Requirements to the Power Unit of Feasibly Attainable Safety

- In case of a total failure of the normal heat-removal system and of all the active decay heat-removal systems and means it is necessary to provide, by using passive principles, a decay heat removal precluding sodium boiling in the core and primary circuit loss of tightness;

- Inside the reactor vessel a "trap" based upon passive principles should be provided for molten fuel collection and cooling-down;

- A value of maximum possible non-sanctioned positive reactivity insertion by shim rods should not exceed the total negative reactivity value spontaneously inserted due to reverse effects and passively acting systems at stabilization of the maximum coolant temperature in the core below the boiling point.

1.6 General Requirements

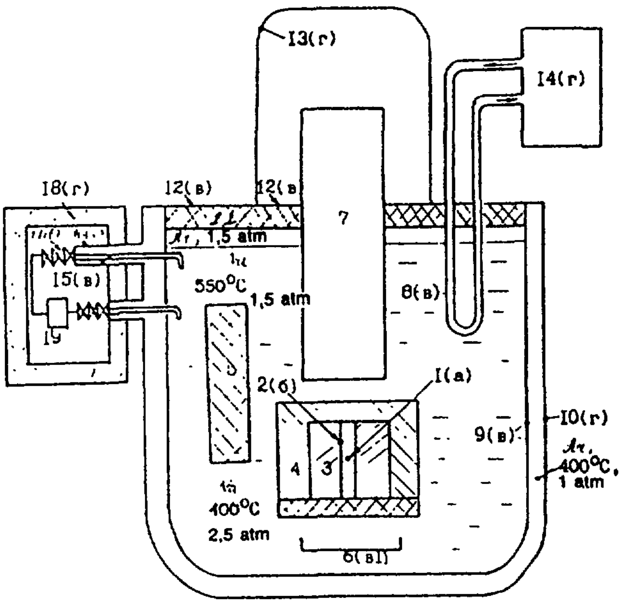
To compensate for potential human errors or for safety system failures a concept of defence-in-depth should be used based upon safety levels and including a number of successive barriers placed on the path of radioactive materials released into the environment, in conformity with the IAEA Safety Series No. 75 INSAG-3 requirements.

2. The BN-800 Power Unit Safety

A detailed description of features and advantages of fast reactors, the BN-350 and BN-600 operating experience and BN-800 unit characteristics are covered earlier.

The BN-800 power unit was developed in conformity with the presently acting regulation codes on NPPs safety.

Four barriers are provided on the way of the radioactivity released from fuel to attended rooms of the power unit in all possible directions (see a scheme presented in Fig. 1. As in all reactor types, as the first, second and third barriers are considered the fuel matrix, the stainless-steel tight



Safety barriers on the path of radioactivity propagation:

the first barrier - a
the second barrier - б
the third barrier - в
the fourth barrier - г

1. fuel
2. fuel elements cladding (tight and strong)
3. core
4. screens and storage around the core
5. saturation with stainless-steel structures around the core
6. the tray for molten fuel collection and cooling
7. the central column with control and safety system drives
8. the heat-transfer tube wall of the heat exchanger between the I and II sodium circuits (tight and strong)
9. reactor vessel (tight and strong)
10. guard vessel around the reactor vessel (tight and strong)
11. "sandwich" top roof (massive and strong) of the reactor
12. metal welded structure (tight and strong)
13. metallic "dome" above control and safety rod drives and rotating plugs (tight and strong)
14. intermediate non-radioactive sodium circuit (tight and strong)
15. piping wall
16. guard vessel (strong and tight)
17. cut-off valves (triple redundancy with independent power supply systems)
18. I-circuit cell walls (strong with a preset degree of tightness)
19. I-circuit auxiliary systems

FIG. 1. Arrangement of BN-800 power unit protection barriers.

and strong fuel-element cladding and the reactor vessel. The characteristic features of the third barrier (the reactor vessel) function and operating conditions are:

- practically total integration of the whole primary-circuit equipment within its boundaries;
- negligible pressure (about 0.5 atm.gauge, in the gas volume and 1.5 atm. gauge in the lower part);
- the vessel temperature being maintained at a low (for stainless steels) temperature of about 400^{o};
- negligible (practically no) neutron radiation damage.

The third safety barrier is extended by the reactor roof; by heat transfer tubes of the intermediate heat exchangers; the guard vessel for auxiliary piping going out of the reactor; cut-off valves (three in succession at the inlet and outlet).

The most important fourth barrier is the reactor containment vessel equal in strength with the main one. On the path of radioactivity propagation in the direction of an open steam-water circuit the fourth barrier is the non-radioactive sodium circuit and its strong and tight structural elements (piping and equipment walls). For the localization of a potential radioactive products release through the recharging-system rotating plug seals the fourth barrier in the form of a strong metallic dome is provided; for the localization of sodium leak consequences at a loss of tightness of the external auxiliary primary sodium piping (the fourth barrier) the tight and strong primary-circuit cells are provided. The results of analysis of some most severe beyond-design accidents and their probability estimate are presented in Table 1.

In item 8.2 of Table 1, at considering a beyond-design accident, a spontaneous operation of hydraulically suspended safety rods is taken into account. At present, this additional system is under development in the BN-800 project. A concept and performance of such a rod was realized and experimentally tested at the BR-10 reactor. The results are extremely good; the rod is put to endurance testing.

TABLE 1. CONSEQUENCES AND PROBABILITY EVALUATION OF SOME SEVERE BEYOND-DESIGN ACCIDENTS

N	Initial situation	Consequences (final state)	Probability 1/year
1	2	3	4
1.	Complete (partial) loss of tightness of the I circuit		
1.1	Reactor vessel loss of tightness	Core parameters do not depart from the nominal values. No radioactivity release outside the I circuit boundaries	$10^{-5} \div 10^{-6}$
1.2	Loss of tightness of external piping and a failure of all safety systems	Core parameters do not depart from the nominal values. Radioactivity releases are below the requirements on NPP location	10^{-8}
2.	Complete long-term loss of power of the plant: loss of power grid and reliable redundant electric power supply (diesel generator starting failure)	During 1 day situation at the plant does not interfere with personnel actions on returning to service of the systems and diesel generator starting. The I circuit and the vessel remain tight. The maximum sodium temperature without personnel interference can reach a steady-state condition (800°C) in 3 days. No sodium boiling.	$10^{-7} \div 10^{-8}$
3.	Unauthorized insertion of available excess reactivity	For a dangerous state to be achieved it is required a multiple (up to 30) mechanical and erroneous operator interference, a failure of all available safety system channels (3 systems, 9 channels) and a failure to press a scram system button	10^{-7}
4.	Complete long-term loss of normal heat removal	Power unit parameters are maintained at a design level due to heat removal through the decay heat removal system of the air heat exchanger	
5.	Loss of forced cooling of shut-down reactor	Safe decay heat removal is carried out by means of natural circulation in the I circuit and air heat exchanger decay heat removal loops	
6.	Local fuel subassembly failure	The instantaneous dangerous flow rate reduction being excluded by design means, all conceivable scenarios leading to sodium boiling and fuel melting down are extended for hours and realized at multiple errors and failures; sodium boiling and fuel melting down in a single fuel subassembly;	10^{-5}
		accident propagation to adjacent fuel subassemblies.	10^{-8}

1	2	3	4
7.	Loss of power grid supply and a failure to drop of all safety rods	Shim rods or continuously operating automatic control rods come into operation. Reactor is cooled through the air heat exchanger decay heat removal system. A short-term cladding temperature increase in some most stressed fuel elements up to 850°C followed by subsequent decrease (drop). The vessel temperature does not exceed 600°C, its serviceability is retained.	$10^{-6} \div 10^{-8}$
8.	Loss of grid power supply and a failure of all reactivity control rods. (including shim rods and automatic control rods)		
8.1	Without additional safety rods, spontaneously coming into operation	Sodium boiling off, introduction of sodium void reactivity effect, super-prompt critical excursion, fuel melting down, molten fuel sodium interaction, possible vessel loss of tightness (depressurization) with a release of several m^3 of sodium. Radioactive releases within the requirements on NPP location.	10^{-8}
8.2	Taking into account additional safety rods, spontaneously coming into operation at a sodium flow rate decrease	Core temperatures remain within nominal values.	10^{-8}

3. Some Conclusion Notes

3.1 In the present work we have not touched upon the development of other reactors, in particular, the BN-1600. For the latter, the pool type of the primary circuit arrangement is under consideration as the main version; however, design studies of modular versions are also to be carried out and feasibility comparison is to be performed.

3.2 The total probabilities of severe accidents suggested in section 1 are meant for an appreciably larger (as compared to the present one) scale of nuclear power.

Probabilities of about 10^{-6}/(reactor year) appear to be more validated for the nearest ten years to come as it is considered, e.g., in INSAG-3.

3.3 In most published papers, as well as in the present one, the problems of increased safety of the reactor itself and of the reactor plant occupy the central place. There is no doubt that this is one of the most important problems in ensuring the nuclear power safety, but not the only one that should be borne in mind at comparing various reactor concepts (modular, poll type, the use of alternative coolants or original designs).

3.4 The safety of the sodium-cooled reactor itself, to our mind, does not practically depend on its being of a modular or pool type. In both cases advantages of alternative fuels can be used and inherent safety problems can be solved due to self control factors and passive safety systems (by various means for modular and pool-type reactors). A modular concept provides certain advantages from the viewpoint of higher-quality prefabrication of the vessel and a possibility of decay heat removal directly from its surface. In this case, however, other characteristics are deteriorated. The surface and the number of welds on modular-type reactor vessels are substantially increased in terms of the same capacity. The total risk of nuclear power depends on the number of power units; a decrease in unit capacity results in a corresponding increase of their number and, as a result, in, though out of proportion, an increase of the total probability of severe accidents. In other words, all other things being equal, for modular reactors a lower probability of severe accident realization per 1 power unit should be postulated.

We believe that when evaluating alternative design concepts or alternative coolant a search for advantages and their validation should be carried out not on the base of safety comparison but by comparing their economic characteristics; an equal level of safety will be achieved by different means and at various costs but they will form an integral part of general correlation between economic factors of equal-capacity NPPs.

SAFETY ASPECTS OF NEW HTGR DESIGNS IN THE FEDERAL REPUBLIC OF GERMANY

W. KRÖGER
Institut für nukleare Sicherheitsforschung,
Kernforschungsanlage Jülich GmbH,
Jülich, Federal Republic of Germany

Abstract

High-Temperature Gas-Cooled Reactors (HTGR) with pebble-bed core are under development in Germany, emphasizing inherent safety features to different extents. The small-sized (200 MWt) HTR-MODUL is designed in such a way that even events of extremely low frequency are not detrimental to public's health mainly because total loss of active decay heat removal does not induce a significant release of fission products.

Changes in safety philosophy aiming at improvement of worldwide public acceptance are proposed incorporating limitation of consequences and of maximum releases in case of hypothetical events for which a high potential for fulfillment has become evident for the HTR-MODUL. Nevertheless, the safety attainable with such a 'revolutionary design' may not be put rigorously on a level with absolute safety; specific limitations and aspects have to be faced.

---

1. INTRODUCTION

High-Temperature Gas-Cooled Reactors (HTGR) use helium as the coolant and graphite as the moderator and structural material. The fuel elements contain multiply coated particles embedded in a graphite matrix. In the German HTGR design, fuel spheres, each six centimetres in diameter, form a 'pebble bed', whereas prismatic blocks are favoured in the USA (see Table 1 for status of development /1/).

The experimental AVR-facility was operated successfully for more than 20 years. Before shutdown at the end of 1988, it was used for a comprehensive test programme including simulation of depressurization accidents and validation of nuclear and thermodynamic codes.

The THTR-300 prototype plant at Hamm was handed over to the utility in the middle of 1987, after intensive tests during the start-up phase. The operating experience to date has been reasonable for a prototype plant, although unplanned outages have been necessary for revision, maintenance, and repair. The plant has been out of operation since Oct. 88 after six hot gas ducts were examined and torn off heads of 33 central bolts and of two corner bolts were detected (a total of 2574 bolts of Incoloy 800 material are provided for the fixation of metallic insulation packages). This is not of safety relevance but it indicates severe technical and financial problem /2/; decommissioning of the plant has been proposed.

The follow-up HTGR concepts, developed by the industry, aim at electricity production with a single unit of medium size (HTR-500) or at combined heat and electricity production in a number of small-sized modules (HTR-MODUL).

Table 1: Characteristics of Gas-cooled Reactors (Oct. 1988)

	Magnox, AGR (CO_2 cooled)	HTR (He cooled)							
		test reactors			prototype reactors		current concepts		
country	GB and others	GB	USA	FRG	USA	FRG	FRG	FRG	USA
plant name (or number)	50 units	Dragon	Peach Bottom	AVR	FSV	THTR	HTR-500	HTR-Modul/ HTR-100	MHTGR
pressure vessel	steel, PCRV	steel			PCRV		PCRV	steel	
power (MW_{el})		20	115	46	840	750	1390	200/250	350
power density (MW_{th}/m^3)	≤ 2.7	14	8.3	2.6	6.3	6	6.6	3/4.2	5.9
enrichment (%)	≤ 3	93					8 – 10		20
Max. outlet temperature (°C)	≤ 675	750	730	950	840	750	725	700	690
operational	Magnox mid 1950s AGR mid 1970s	1968-75	1967-74	1967-88	1976-	1986-	–	–	–
total net power (TWh)*	1222	–	2.9		5.3	2.9	–	–	–
reactor-years*	1012	54					–	–	–

* for comparison LWR: 10764 TWh, 2495 reactor-years　　PCRV = Pretressed Concrete Reactor Vessel

All the HTGR concepts are designed or have to be designed to meet the well-known German licensing criteria. The concepts emphasize inherent safety features to different degrees: For the HTR-MODUL this is one of the driving principles of the design.

2. DESIGN GOALS AND SAFETY CONCEPT - THE INDUSTRIAL PROGRAMME

For the design of the HTR-MODUL safety has been established as primacy by SIEMENS/INTERATOM: Also in case of extremely low frequency events the environmental impact should be within the range of limits set by the Radiation Protection Ordinance for design basis accidents (StrlSchV § 28.3 - 5/15 rem whole body/thyroid), even if all mitigating measures would be omitted; evacuation of the public should not be regarded as necessary to avoid health effects.

To achieve this, the reactor was designed in such a way that maximum temperatures of fuel elements or coated particles, respectively, cannot significantly exceed 1600 °C even in case of failure of all active components/systems, provided for reactor shutdown and decay heat removal.

This goal has been derived from investigations into the behaviour of irradiated spherical fuel elements with TRISO-coated particles (Fig. 1). Ramp tests (50 °C/h) in the range of 1200 to 2500 °C and release tests with high precision at constant temperatures in the range of 1500 to 1800 °C indicate the following:

1) Taking Kr 85 as an indicator for particle defects, temperatures of about 1600 °C do not cause any damage, while for temperatures of ≥ 2100 °C a significant fraction of defective particles must be expected due to thermal decomposition of the SiC layer (Fig. 2).

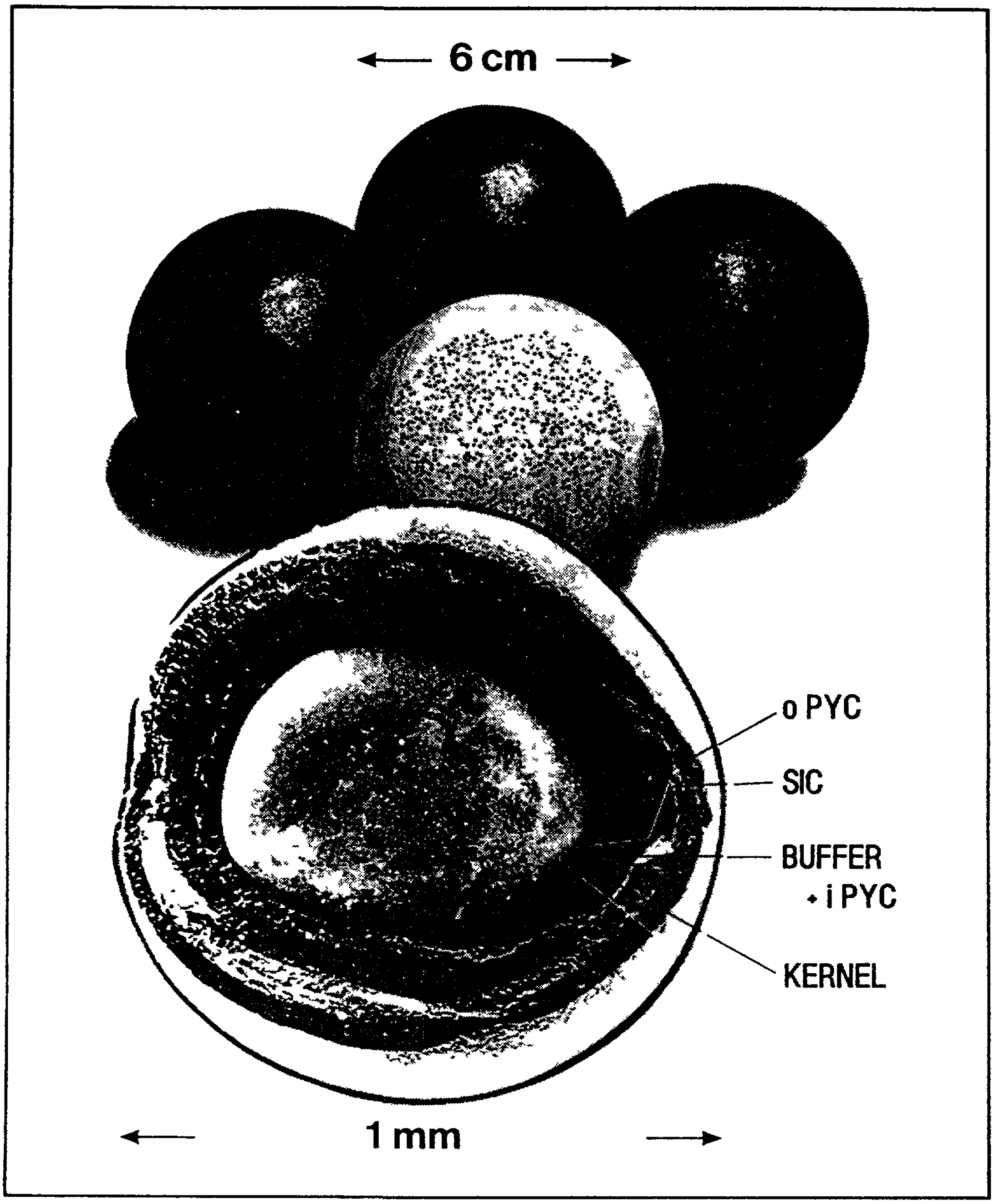


Fig. 1: HTGR Fuel Elements with Coated Particle

2) Metallic fission products, e.g. Cs and Sr, may diffuse through intact particles; this begins to become significant at long annealing times and temperatures above 1600 to 1700 °C (Fig. 3).

To ensure sufficient heat removal not by active but by passive means it is necessary to limit the power output and power density as well as the core diameter. It can be seen from Table 2 that the main design features of the HTR-MODUL resemble those of the AVR which is, therefore, suitable to demonstrate safety characteristics.

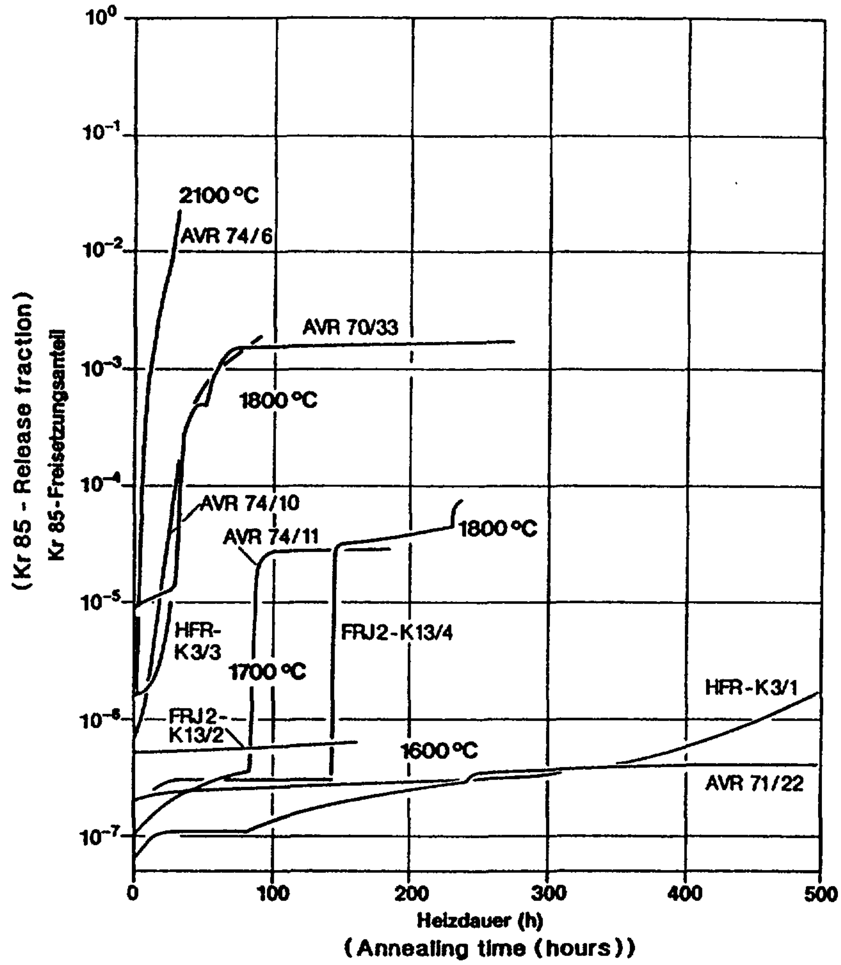


Fig. 2: Kr 85-Release from Irradiated Fuel Elements with UO_2-TRISO-Particles as Indicator for Particle Defects /3/

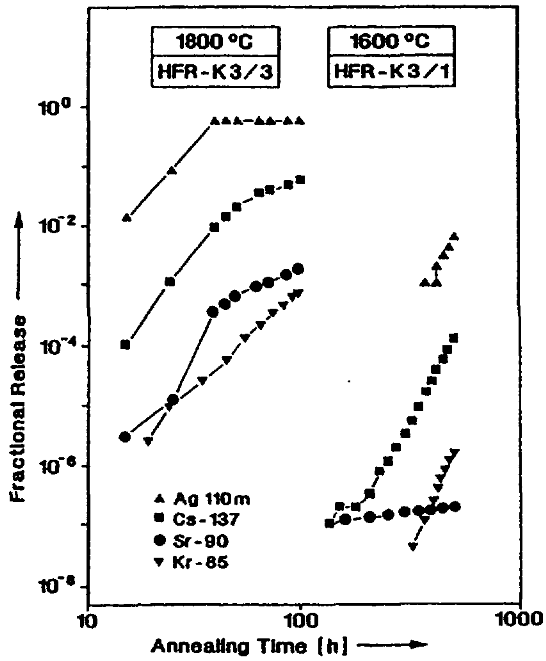


Fig. 3: Fractional Release versus Annealing Time for Irradiated TRISO Fuel Elements /3/

Table 2: Comparison of Main Design Features

Main Design Features	HTR-MODUL Conceptual Design	AVR Test Reactor
• power, power density	200 MWt, 3 MWt/m³	46 MWt, 2.6 MWt/m³
• pressure, temperature of He-coolant gas	60 bar, 250/700 °C	10.8 bar, 275/950 °C
• core radius, height	1.5/9.4 m	1.5/2.5 m
• heavy metal per fuel element	7 g	6 g

The schematic view (Fig. 4) and the outline of the safety concept (Table 3) emphasize that the intensive use of means of inherent or passive safety has been the guiding design principle for the HTR-MODUL, essentially:

- No active system is provided to remove decay heat from the (slim) core or to keep the maximum temperature of fuel elements below failure limits under all conceivable accident conditions, respectively.

- The concrete of the reactor cell is lined with a pumped surface cooling system designed to absorb heat losses during normal operation and decay heat transported from the inner core to the reflector and thereupon through the vessel. This system is not of relevance for safety.

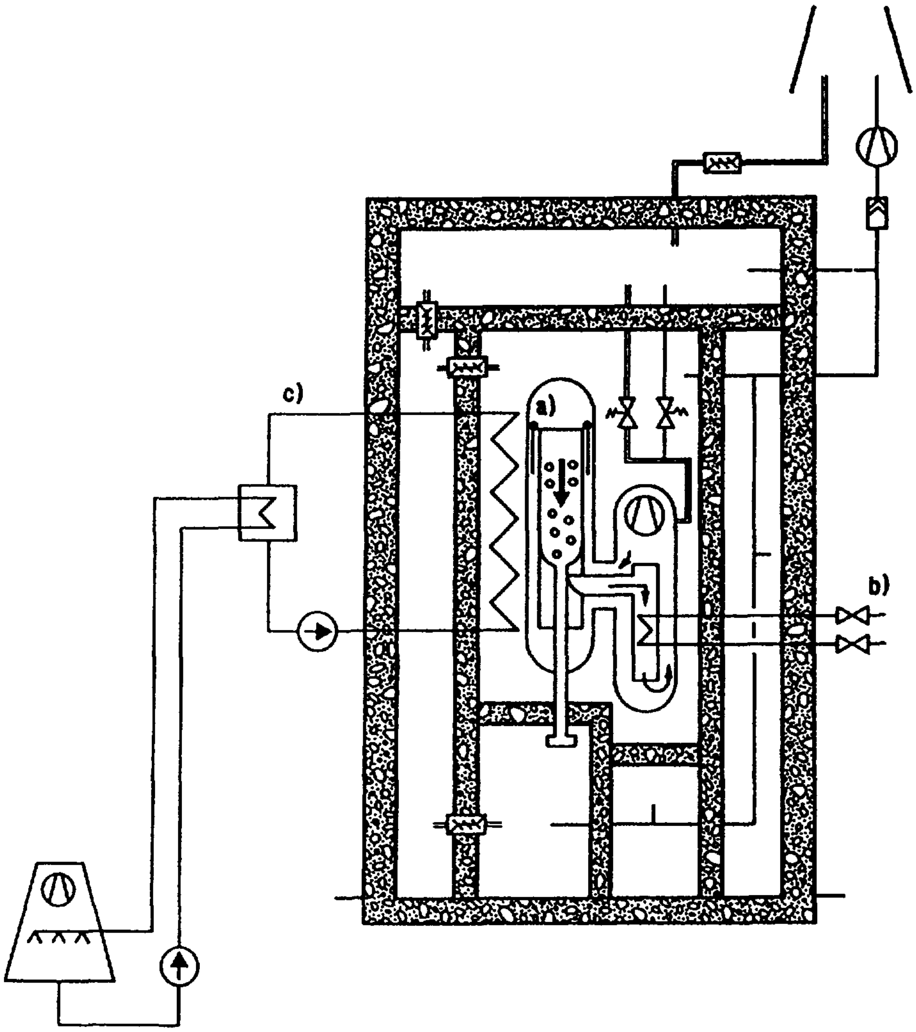
- Side-by-side arrangement of pressure units to suppress natural convection and to limit the amount of water potentially ingressing into the reactor. The steam-generator vessel is sized and located in such a way that even the total amount of feedwater entering the primary circuit could not result in the flooding of the core.

- The core is designed to reduce positive reactivity introduced by a withdrawal of absorber or water ingress.

- Two independent shutdown systems exclusively acting within the reflector region are provided to fulfill regulatory requirements.

In the hypothetical case of the failure of both shutdown systems the reactor would stabilize inherently due to its strong negative temperature coefficient and the thermal stability of the ceramic core. The difference between the operational and failure temperatures of the fuel elements, about 750 °C, can be used to ensure shutdown by inherent mechanisms /4/.

As mentioned before the surface cooling system is only of relevance for the protection of components, mainly to keep maximum temperatures of the pressure vessel and its bearings in the design range of about 400 °C in case of total loss of forced core cooling. Even if this system should fail, the core temperatures would not increase significantly. Although a loss of structural integrity, practically need not be expected, the primary circuit should be depressurized (if under pressure) after about 2 days as a precaution. The structural integrity of the concrete walls of the reactor cell is not endangered (see Fig. 5); the temperatures at the inner surface exceed 140 °C after about 15 hours and may reach up to 600 °C after about 10 days /5,6/.



reactor control and shutdown a)	afterheat removal		vessel (steel) protection		containment
	system b)	allowed time to fail	system c)	allowed time to fail	
absorber balls (cold) and rods (hot shutdown) system in side-reflector	operational, no auxiliary core cooling system	∞	3 x 100 % cavity cooling system	20 hours	vented confinement with filtered (small leaks) or unfiltered stack release

Fig. 4: Schematic Cross Section and Important Systems of HTR-MODUL

Table 3: Safety Concept of HTR-MODUL

Reactivity Control	**Inherent**
- temperature coefficient	- 0,5 % per 100 °C ($\Delta T \leq 750$ °C permissible for fuel element)
- excess reactivity	+ 1,2 % (100 - 50 - 100 % load range)
- reactivity effect of ingressing water	+ 0,05 % per 100 kg (slight undermoderation, 7 g HM per fuel element)
	active
- systems	6 reflector rods (hot) 18 reflector absorber-ball-systems (cold)
Decay Heat Removal	passive (no auxiliary system, surface cooler only for vessel protection)
Activity Retention	fuel elements ($T_{max} < 1600$ °C) pressure vessel units (burst proof) vented confinement with filters for small mass flow
Control of Water/Air Ingress Events	limition of amount by leak detection and isolation (active), side-by-side arrangement, suppression of natural convection/small, below reactor connecting pipes, exclusion of vessels' rupture
Plant Protection System	simple, fail-safe
- criteria	pressure, temperature, mass flow, flux, (moisture)
- actions	plant shutdown - hot standby, (SG relief)

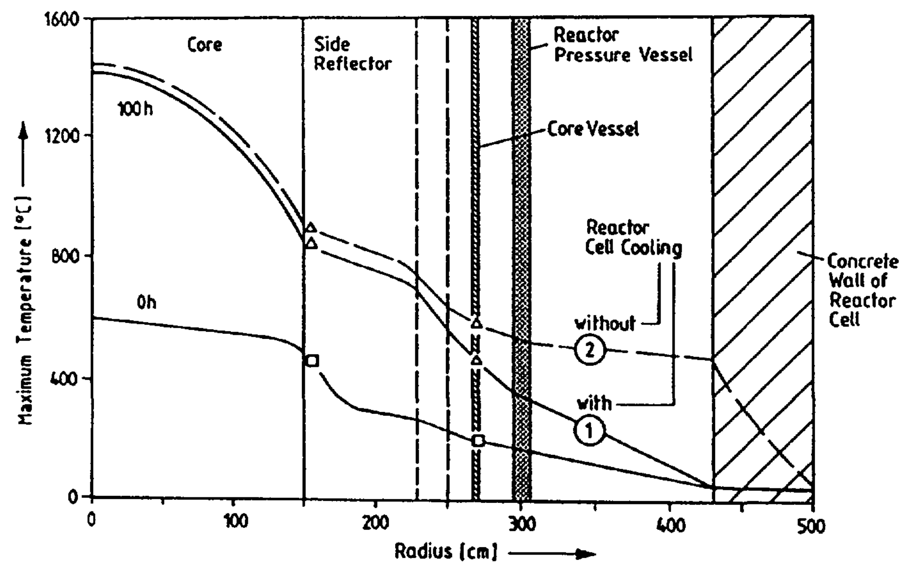


Fig. 5: Radial Temperature Distribution for HTR-MODUL (depressurized, no forced convection) /5/

In summary, the HTR-MODUL comprises safety features ensuring inherent reactivity control and protection against temperature-induced activity release. Nevertheless, the results depend on the assumption of stable geometric conditions, e.g. a sudden rupture of the pressure vessel units is ruled out by the designer, referring to the high standard of quality assurance provided according to principles of 'basic safety' developed for LWR and transferred to HTGR conditions.

The guiding principle for activity retention/containment is defense in depth but HTGR specific conditions have been taken into account:

- The fuel elements guarantee retention radioactive material at the "place of birth".

- The main objective of the pressure vessel units is to keep away corrosive media from the core and to prevent activity release induced by corrosion.

- The reactor building - a vented confinement instead of a gastight containment - is provided to minimize activity releases and in addition to protect the reactor against external impact.

Water and air ingress events are not only controlled by inherent means because the hot graphite is chemically not resistent. The guiding principle is to limit the amount of ingressing media by simple active systems, plant arrangement and again by exclusion of rupture of passive components.

The reactivity effects of ingressing water have been reduced by lowering the content of heavy metal from the usual 10 g to 7 g per fuel element. Even under worst-case conditions the maximum amount of water in the core is limited to 900 kg of saturated steam, resulting in an increase of reactivity of 3,2 % (Fig. 6). The physical effects are in the same range as in the case of the withdrawal of absorber rods: The expected values for short power peaks reach up to a factor of slightly above 2 and for maximum temperatures of the fuel elements (in combination with core heatup) up to 1540 °C.

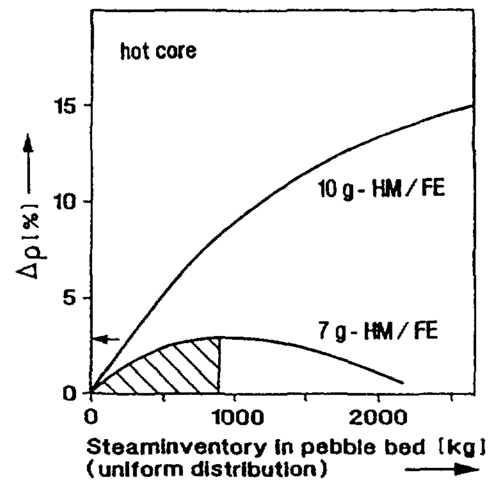


Fig. 6: Reactivity Increase versus Steam Inventory of Pebble-bed for Different Fuel-Element Heavy Metal Contents /4/

The HTR-MODUL is well documented in a safety report. It has been included in the licensing procedure in the Statė of Lower Saxony but the procedure was stopped due to legal (no selected site, no user's interest) and political reasons. Nevertheless, the safety evaluation work has been completed. The RSK will come up with results of its independent safety assessment and in the late summer of '89.

The safety evaluation and the initially intended approval of the plant concept have been based on current FRG licensing requirements. They are outlined schematically in Fig. 7 and do not claim to design the plant against low frequency events which are regarded to be excluded entirely. The excellent safety characteristics of the HTR-MODUL in this regime have only been credited for facilitation of decisions with regard to design basis accidents.

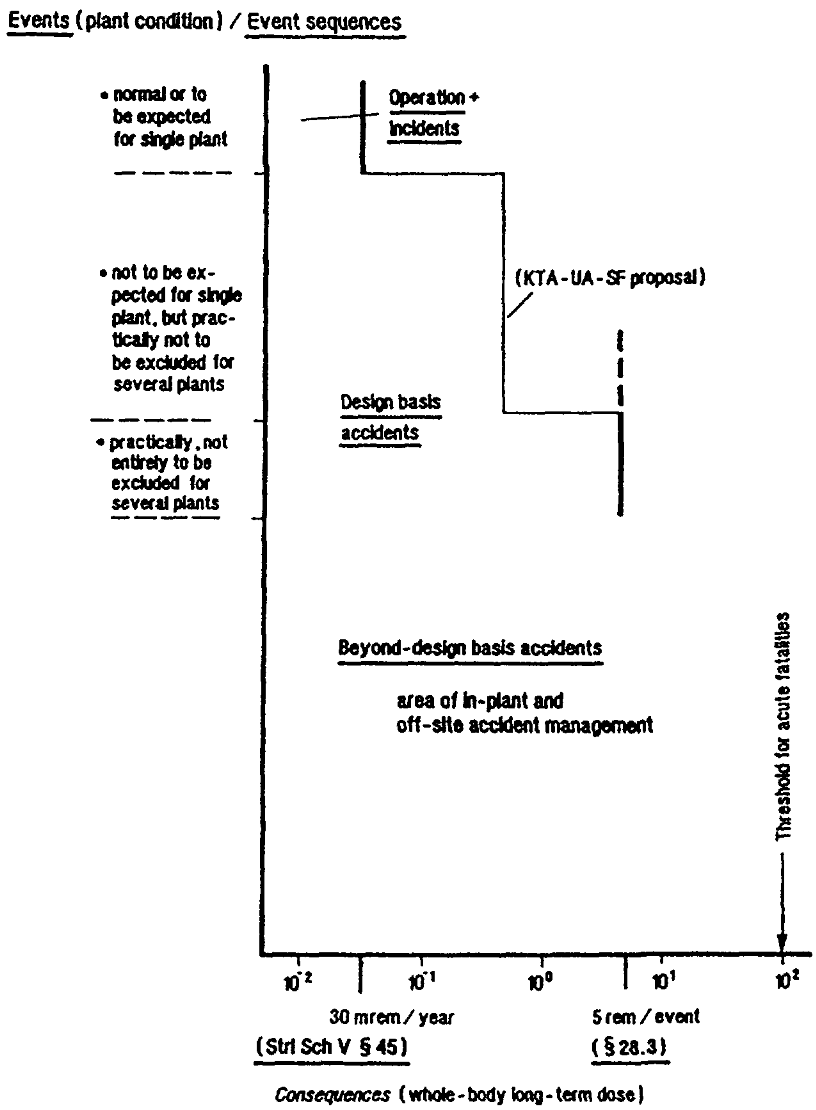


Fig. 7: Current Safety Requirement

3. ADVANCED SAFETY PHILOSOPHY, INDEPENDENT SAFETY ASSESSMENT - THE SCIENTIFIC PROGRAMME

Independent from the efforts of the industry the nuclear research centre at Jülich (KFA), at which the scientific work for German HTGR is concentrated, has tried to further develop the safety philosophy and to derive pertinent quantitative requirements as well as to assess the safety of HTGR concept by the application of PSA methodology.

The primary aim of changes in the safety philosophy is to improve the public acceptance and pre-conditions for a consensus among political parties; a 'revolutionary' approach is regarded as being most promising:

- Elimination of potential severe core damage and large releases by inherent properties.

- Robust design to drastically reduce vulnerabilities with regard to human and technical failures and to give ample time for corrective actions.

- Safety properties should be transparent and plausible for non-experts.

These qualitative aims have been transferred in factual terms and finally in more stringent quantitative requirements which are suitable for intra-technical discussion and to derive design criteria. This proposal which is not related to a specific reactor type can be outlined as follows:

. Separation of the term 'risk', e.g. late fatalities per year, into its elements allocating different importance to frequency (classification of events) and limitation of consequences (design criteria).

. Exclusion of acute and minimization of late health effects for the whole spectrum of events by technical means; short-term (sheltering, evacuation) as well as long-term emergency measures (relocation, decontamination) should no longer be considered necessary; daily activities of the public nearby should not be affected.

. Fixing of dose limits from which maximum allowable releases in case of hypothetical accidents can be calculated resulting in 'new' design features:

  1 (... 10) rem 7-days-whole body dose
  10 (...100) rem 30-years-whole body dose

  for event sequences analysed quantitatively up to a cut-off frequency.

  Qualitative proof of reduced vulnerability against extreme (deterministically) assumed loads including acts of sabotage.

This proposal can be presented in a frequency-consequence diagramm connected with the existing deterministic requirements which are interpreted probabilistically and retained for the region of normal operation and design basis accidents (Fig. 8).
The dose limits refer explicitly to individuals at worst location; sufficient protection of the public (collective dose) must be proven. The discussion of adequate values has not yet been completed.

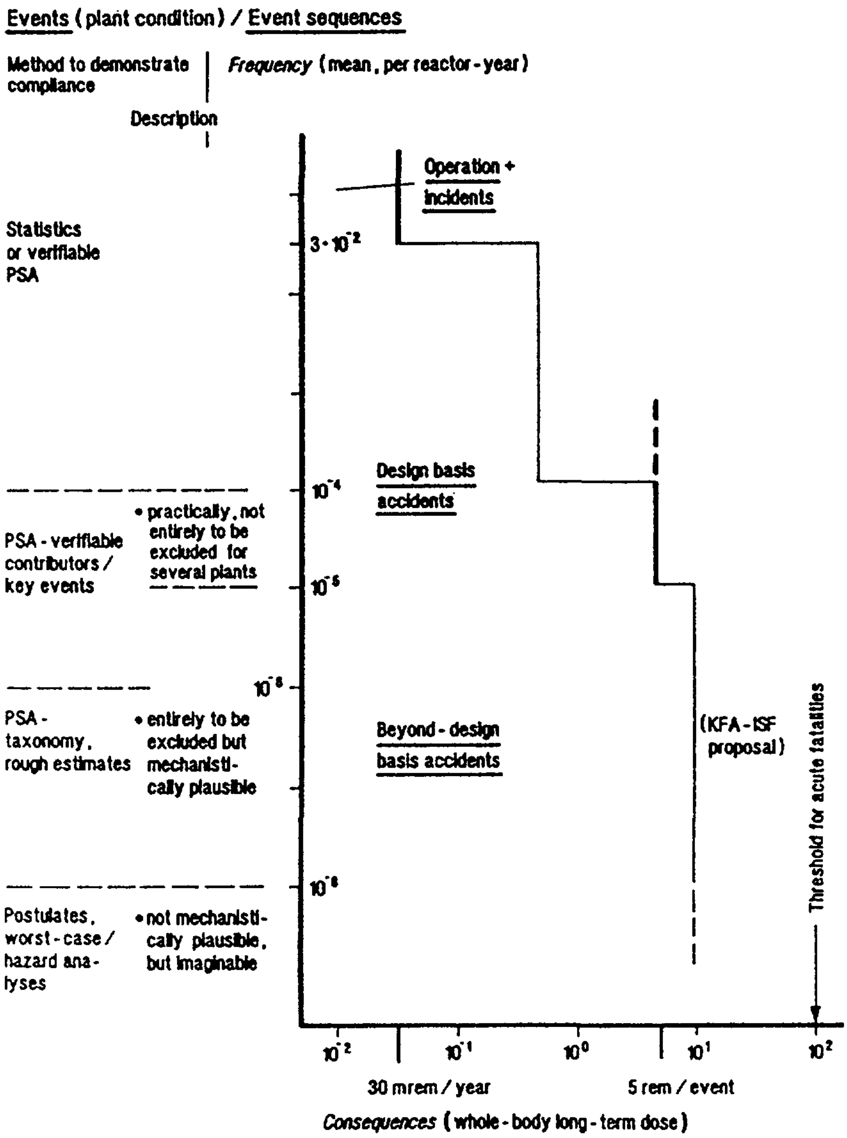


Fig. 8: Requirements for 'Extraordinary Safe' NPP of Next Generation

Attempts have been made to avoid a cut-off line but it turned out to be impossible from a rigorous technical point of view. Subsequently, the philosophical problem may arise that there is no radical change in principle but only a shift of current difficulties to a once again lowered frequency-level. This problem is narrowed down by the fact that the cut-off line can be determined in such a way that on one hand all mechanistically plausible event sequences can be identified and analysed with available tools and that on the other hand a change over from active engineered safeguards to inherent design characteristics will follow unavoidably.

PSA methodology is regarded as sufficiently developed for this screening and selecting purpose although uncertainties and proof of sufficient completeness increase with decreasing probabilities. Vulnerability against extreme loads, e.g. acts of sabotage or even war, rare natural events, can only be studied qualitatively.

The proposed approach and requirements have been compared with the 'Top Level Design Criteria' established in the USA within the MHTGR programme /7/. It turned out that the basic aims and principles do not differ significantly, but that the proposed dose limits and compliance procedures obviously deviate. These differences have been assessed in view of the maximum allowable release of radioactive material for design and beyond-design basis accident conditions (Table 4). The proposed West-German advanced safety requirements (ASR) cover a higher degree of hypotheticality; the releases of short-lived nuclides are guided by the short-term dose limits, whereas the long-lived nuclides (strontium, cesium) are limited by long-term doses. Focusing on official regulatory requirements (10 CFR 100, StrlSchV), currently applied within licensing procedures, tremendous differences become obvious. Even if the guidelines for protective actions (PAGs) are taken as limiting doses for the region of classical design basis accidents, the West-German regulatory requirements are more stringent.

Table 4: Summary of Single-nuclide Environmental Releases Meeting Criteria

Criteria	Region (mean frequencies per plant-year)	Release Height [m]	Maximum Release [Ci] [a]			
			Kr-88	Sr-90	I-131	Cs-137
U.S.A.						
10 CFR 100	$2.5 \cdot 10^{-2} \ldots 10^{-4}$	30	$2.7 \cdot 10^{5}$	$8.1 \cdot 10^{5}$	$3.1 \cdot 10^{3}$	$8.9 \cdot 10^{5}$
PAG	$2.5 \cdot 10^{-2} \ldots 5 \cdot 10^{-7}$	30	$8.9 \cdot 10^{4}$	$1.7 \cdot 10^{2}$	$4.7 \cdot 10^{2}$	$4.0 \cdot 10^{1}$
Germany, F.R.						
Strl Sch V § 28.3	10^{-6}	30	$38 \cdot 10^{4}$	$0.002 \cdot 10^{2}$	$0.03 \cdot 10^{2}$	$0.4 \cdot 10^{1}$
ASC - short term		30	$7.5 \cdot 10^{4}$	$3.8 \cdot 10^{2}$	$6.6 \cdot 10^{2}$	$130 \cdot 10^{1}$
- long term	$10^{-6} \ldots 10^{-8}$	30	$75 \cdot 10^{4}$	$19 \cdot 10^{2}$	$32 \cdot 10^{2}$	$2.7 \cdot 10^{1}$

[a] Based on dose calculations at an EAB of 425 m. Lower dose limits in USA PAG and proposed FRG ASC were utilized

The differences based on single nuclide calculations diminish in their overall significance if the real release characteristics of low-frequency HTGR accidents are taken into account, e.g. the different limit values for strontium (almost a factor of 100) are meaningless due to very small release figures, in principle.

As for other HTGR concepts a small-effort probabilistic safety analysis (Mini-PSA) has been carried out recently for the HTR-MODUL /8/ in order

. to find design-weaknesses and to check homogenity of the safety concept,

. to support the safety assessment by the RSK and

. to find out whether the proposed stringent safety requirements can be- or are already fulfilled.

The results confirm that due to the physical characteristics loss of forced convection (core heatup) accidents practically do not contribute to the risk. Even the most unfavourable temperatures are so low that no significant activity release from the core is induced. Furthermore, the nuclides of particular radiological relevance (Cs and Sr) would be partially redeposited on the 'cooler' graphite surfaces.

Water ingress accidents due to leaks in the steam generator proved to entail the largest source terms and to be the dominant risk contributors. In the worst case, after the additional failure of control measures, fractions of those fission products (Cs, Sr: 2.5 %, iodine: 100 %) which have been deposited on the metallic steam generator surfaces during normal operation may be detached and released into the environment via relief valves in the secondary circuit.
The frequencies of such accident sequences are in the range of $5 \cdot 10^{-7}$/a. The calculated release values are very small, e.g. about 210 GBq for I-131 and about 30 GBq for Cs 137.

Based on these analyses it is possible to derive a representative source term for the region of events of extreme low frequency (Table 5). Reflecting on releases, allowable according to the proposed requirements, a high potential of the HTR-MODUL to fulfil them becomes obvious. Furthermore, practically no lethal cancer cases and very small collective risk figures are computed for very low accidental dose estimates.

Table 5: Representative Source Term - Conservative Estimate

frequency	type of accident	activity release (in terms of fractions of core inventory)		
		Sr	Cs	I, Br
$<10^{-5} \ldots 10^{-8}$	water ingress (incl. core heatup)	$<10^{-6}$ %	$<10^{-3}$ %	$<10^{-4}$ %
		fraction of allowable releases according to proposed requirements		
		0.4 %	<15 %	<10 %
$<10^{-8}$		not significantly higher according to current state of knowledge		

For all recent HTGR concepts, massive corrosion effects on graphite in the case of an air ingress after depressurization of the primary circuit are not relevant to the risk; the necessary conditions for graphite burning, such as a very large leak or chimney draught, no restriction of oxygen quantity by the reactor building or other means, can be credibly ruled out /9/.
Parametric studies have been carried out and indicate that, in any case, hours would be available for simple limiting counter measures without restrictions before graphite corrosion can become a significant release mechanism. Moreover, the retention capability of corroded 'bare' coated particles is to be studied experimentally.

4. UNCERTAINTIES, DEMONSTRATION OF PHYSICAL PROPERTIES - A CONCLUDING OUTLOOK

As compared to present LWR the safety concept of modern HTGR, especially the HTR-MODUL, is mainly based on passive components and mechanisms and on inherent properties.

Although the plant and safety concept is not designed to the last detail the licenseability of the HTR-MODUL according to current regulatory requirements is beyond question, in principle, and a high potential to meet advanced more restrictive requirements to control with low-frequency events has become obvious. Nevertheless, the safety attainable with such a 'revolutionary' design may not be put on a level with absolute safety. Moreover, specific limitations and problems have to be faced:

1) Inherent safety features are not necessarily advantageous for all conditions, they are difficult to control and to 'switch-off', simple active systems are still necessary.

2) New characteristics may cause novel accident scenarios; loss of operating experience, expertise, and peer review must be coped with.

3) The dependence on structural (geometrical) integrity and postulates is on-going.

4) Proof and demonstration of the efficiency of physical properties are more difficult than of the proper functioning of active systems.

With regard to the demonstration of essential safety characteristics selective experiments at the AVR are of great importance and benefit for the HTR-MODUL. They comprise /10/:

- The negative feedback between a rise in core temperature and the reactivity of the reactor and the resultant inherent automatic nuclear shutdown via blower shut off and control via the blower speed ('stuck-rod experiments'). The negative feedback was also maintained for a reactor core with 50 % low-enriched uranium and resultant plutonium.

- Heat removal by means of simple principles such as heat conduction and radiation instead of sophisticated active emergency cooling systems.

- The retention of fission products by fuel elements and reactor graphite during normal operation (despite a subsequent temperature increase to 950 ^{o}C) and for plant conditions involving elevated temperatures.

The AVR furthermore provides the reservoir of real irradiated fuel elements for extensive heating experiments.
Simulation experiments will still be carried out with the AVR in 1989 serving to integrally determine the dust and activity discharge during depressurization.

The described design and safety features as well as specific uncertainties also mark out the key areas of safety research for HTGR-specific types of events. The basic understanding of phenomena and accident scenarios as well as the development of analytical tools (computer codes) and data base have been largely dealt with by investigations extending over several years in the past. Meanwhile, computer codes are available for the description of any important accident scenario. Priority is currently and in the future be given to tool validation and integral demonstration of safety features for which THTR and AVR operating experience and transient test results are used.

REFERENCES

/1/ KRÖGER, W., SCHULTEN, R.
Technology and Safety Aspects of German HTGR,(Proc. ANS Top. Meeting on Safety of Next Generation Nuclear Power Reactors, Seattle, 1988), pp. 662

/2/ KRÖGER, W., NICKEL, H.
Safety/Licensing Reviews in the FRG with Emphasis on THTR-300, scheduled for publication in Nuclear Safety, 4/1988

/3/ SCHENK, W., PITZER, D., NABIELEK, H.
Fission Product Release Profiles from Spherical HTR Fuel Elements at Accident Temperatures, Jül-2234 (1988)

/4/ LOHNERT, G.H., SCHERER, W.
Verhalten des HTR bei Reaktivitätsstörfällen, Jahrestagung Kerntechnik, Düsseldorf, 1988, Bericht Fachsitzung "Stand der HTR-Sicherheitsforschung"

/5/ REHM, W., JAHN, W., VERFONDERN, K.
Present Results and Further Developments on Safety Analysis of Small and Medium HTRs for Core Heatup Accidents, Nucl. Eng. and Design 109 (1988), pp. 281

/6/ ALTES, J., REHM, W., WEICHT, U.
Komponentenverhalten unter Temperatur- und Druckbelastung bei Kernaufheizunfällen, Jahrestagung Kerntechnik, Düsseldorf, 1988, Bericht Fachsitzung "Stand der HTR-Sicherheitsforschung"

/7/ KRÖGER, W.
Safety Criteria for Advanced HTGR Concepts, (Proc. of an IAEA TC Meeting on "Design Requirements, Operation and Maintenance for Gas-Cooled Reactors", San Diego, 1988), IWGGCR/19, pp. 143

/8/ KRÖGER, W., WOLTERS, J., MERTENS, J., MOORMANN, R., REHM, W.
Preliminary Results of an Updated Probabilistic Safety Analysis for the German HTR-MODUL, Post-SMiRT Seminar on Small and Medium-Sized Nuclear Reactors, San Diego, Aug. 1988

/9/ MOORMANN, R., KATSCHER, W.
Examination on Graphite 'Burning' in HTGR's, (Proc. 2nd Int. Symposium on Nuclear Reactor Severe Accident Chemistry, Toronto, 1988)

/10/ KIRCH, N., IVENS, G.
Ergebnisse der Versuche mit dem AVR, VDI-Berichte 729, "AVR - 20 Jahre Betrieb", (1989), pp. 87

SAFETY ASPECTS OF THE MODULAR HIGH-TEMPERATURE GAS-COOLED REACTOR (MHTGR)

F.A. SILADY
General Atomics,
San Diego, California

A.C. MILLUNZI
United States Department of Energy,
Washington, D.C.,

United States of America

Abstract

The Modular High-Temperature Gas-Cooled Reactor (MHTGR) is an advanced reactor concept under development through a cooperative program involving the U.S. Government, the nuclear industry and the utilities. Near-term development is focused on electricity generation and cogeneration uses such as water desalination. The design utilizes the basic high-temperature gas-cooled reactor (HTGR) features of ceramic fuel, helium coolant, and a graphite moderator. However, the specific size and configuration are selected to utilize the natural characteristics of these materials to develop a significantly higher margin of safety than current generation reactors. The qualitative top-level safety requirement is that the plant's operation not disturb the normal day-to-day activities of the public. Quantitatively this requires that the design meet the U.S. Environmental Protection Agency's Protective Action Guides at the site boundary hence precluding the need for sheltering or evacuation of the public.

The MHTGR safety response to events challenging the functions relied on to retain radionuclides within the coated fuel particles has been evaluated. A broad range of challenges to core heat removal have been examined which include a loss of helium pressure and a simultaneous loss of forced cooling of the core. The challenges to control of heat generation have considered not only the failure to insert the reactivity control systems, but the withdrawal of control rods. Finally, challenges to control chemical attack of the ceramic coated fuel have been considered, including catastrophic failure of the steam generator allowing water ingress or of the pressure vessels allowing air ingress. The plant's response to these extreme challenges is not dependent on operator action and the events considered encompass conceivable operator errors. In the same vein, reliance on radionuclide retention within the fuel particle and on passive features to perform a few key functions to maintain the fuel within acceptable conditions also reduces susceptibility to external events, site-specific events, and to acts of sabotage and terrorism.

INTRODUCTION AND DESIGN OVERVIEW

Under the sponsorship of the U.S. Department of Energy (DOE), four U.S. corporations, General Atomics; Combustion Engineering; Bechtel National; and Stone & Webster Engineering Corporation; along with Oak Ridge National Laboratory, and utility input through Gas Cooled Reactor Associates are developing a MHTGR that can provide safe, economic, and reliable power for the next generation of power plants.

The MHTGR design is based upon generic gas-cooled reactor experience, as well as specific HTGR programs and projects. These include the 52 carbon dioxide-cooled developed in the United Kingdom and the five helium cooled reactors built in Western Europe and the United States.

The MHTGR is being designed to meet the rigorous requirements established by the NRC and the electric utility/user industry for a second generation power source of the late 1990s. The plant is expected to be equally attractive for deployment and operation in the United States, other major industrialized nations, and the developing nations of the world.

The typical MHTGR plant includes an arrangement of four identical modular reactor units located in a single reactor building. The plant is divided into two major areas: a Nuclear Island (NI) containing the four reactor modules and an energy conversion area (ECA) containing two turbine generators. Each of the reactor modules produces a thermal output of 350 MW(t). The reactor modules are paired to feed the turbine generators to produce 538 MW(e) net of electric power. The steam conditions are similar to those of a modern fossil-fired plant.

Each reactor module is housed in adjacent, but separate, reinforced concrete structures located below grade and under a common roof structure. The below-grade location provides significant design benefits by reducing the seismic amplifications typical of above-grade structures.

The overall reactor configuration is shown in Fig. 1. The reactor components are contained within three steel vessels: a reactor vessel, a steam generator vessel, and a connecting cross duct vessel. The reactor vessel is approximately the same size as that of a large boiling water reactor and contains the core, reflector, and associated supports. Top mounted penetrations house the control rod drive mechanisms and the hoppers containing boron carbide pellets for reserve shutdown. The penetrations are also used as access for refueling and inspection.

The heat transfer during power operation or normal decay heat removal operation is accomplished by helium which is heated as it flows down through the core. It is collected in a plenum below the core and flows through a coaxial hot duct inside the cross vessel to a once-through helical bundle steam generator. After flowing downward over the steam generator tubes, the cool helium flows upward in an annulus between the steam generator vessel and a shroud leading to the main circulator inlet.

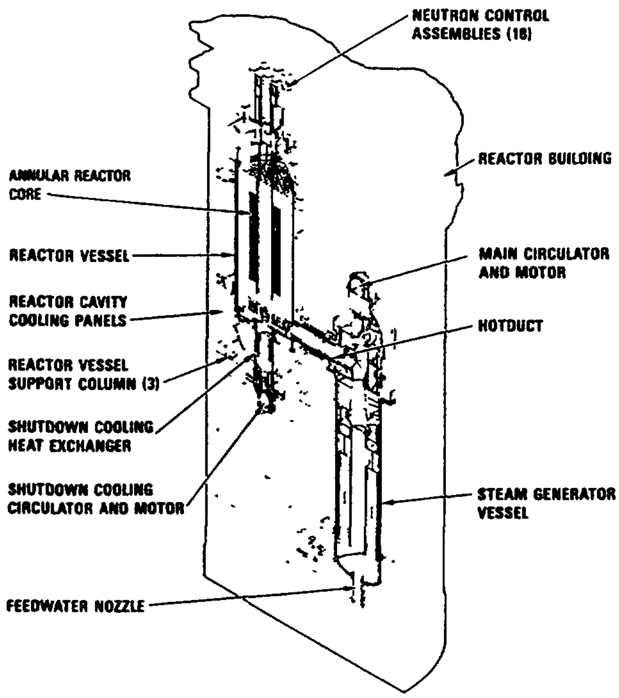


Fig. 1. 350 MW(t) MHTGR isometric

The main circulator is a submerged electric motor driven, two stage axial compressor with active magnetic bearings. The helium is discharged from the circulator and flows through the annulus of the cross vessel and hot duct and then upward to the top plenum over the core.

In order to meet availability and maintenance requirements, a separate shutdown cooling system (SCS) is provided as a backup to the primary heat transport system. A shutdown heat exchanger and a shutdown cooling circulator are mounted on the bottom of the reactor vessel. The heat removal systems allow hands-on plant maintenance to begin within 24 h after plant shutdown.

A reactor cavity cooling system (RCCS) is located in the concrete structure external to the reactor vessel to remove plant residual heat. This system is totally passive and provides a heat sink if the forced cooling systems are inoperative. The heat is transferred by means of conduction, convection, and radiation from the core to the RCCS This system has no controls, valves, circulating fans, or other active components.

The reactor core and the surrounding graphite neutron reflectors are supported on a steel core support plate at the lower end of the reactor vessel. A horizontal cross section of the reactor core and vessel internals is shown in Fig. 2. The reactor core contains graphite fuel blocks that are hexagonal in cross section. The fuel (Fig. 3) is in the form of coated particles of low enriched fissile uranium oxycarbide and fertile thorium oxide. The fuel particles are bonded together in fuel rods which are contained

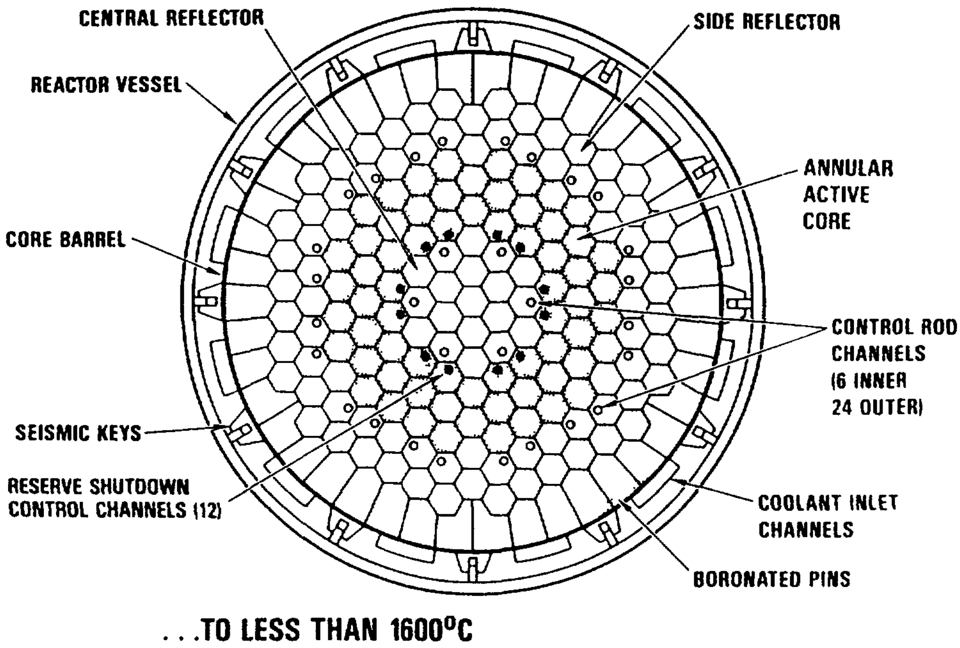


Fig. 2. 350 MW(t) modular reactor core cross section

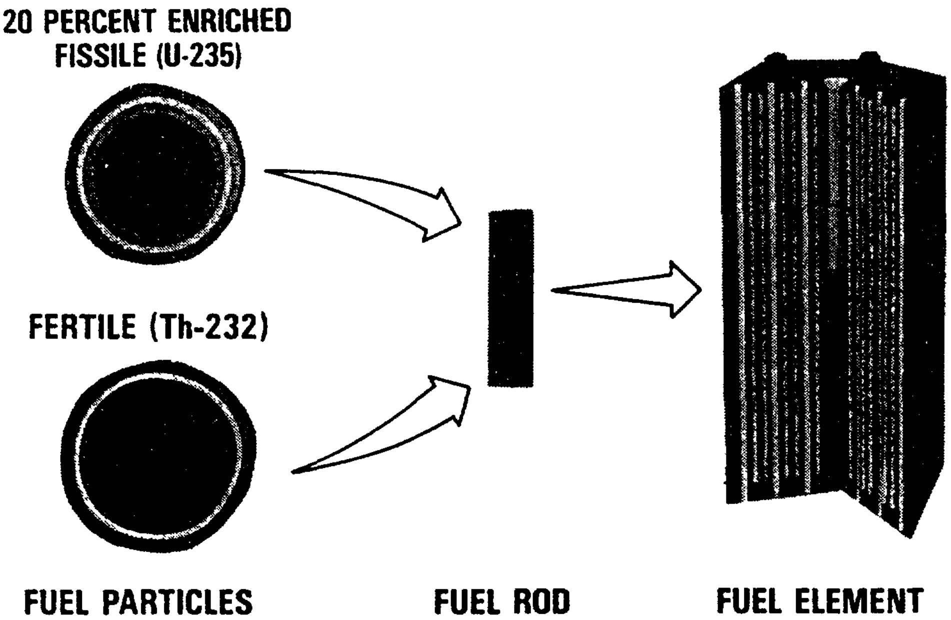


Fig. 3. MHTGR fuel components

in sealed vertical holes in the fuel blocks. These fuel blocks are stacked in columns to form an annular shaped core. Unfueled graphite blocks fill the center and surround the active core to form the reflector. Key reactor core design parameters are shown in Table 1

TABLE 1 PLANT AND CORE PARAMETERS	
Thermal power (4 modules)	1400 MW(t)
Electrical output	588 MW(e) gross; 538 MW(e) net
Net efficiency	38.4%
Steam conditions	538°C (1000°F)/16.6 MPa (2400 psig)
Core exit helium temperature	687°C (1268°F)
Cold helium temperature	259°C (498°F)
Core power density	5.9 W/cm^3
Annular core diameters Outer Inner	 3.5 m 1.6 m
Core height	7.9 m
Number of columns in active core	66
Number of fuel elements per column	10

SAFETY PHILOSOPHY

The overall safety philosophy guiding the design of the MHTGR is to produce a safe, economical plant design which meets NRC and user requirements by providing defense-in-depth through the pursuit of four goals: (1) maintain safe plant operation, (2) maintain plant protection, (3) maintain control of radionuclide release, and (4) maintain emergency preparedness.

With regard to the achievement of NRC criteria for the accomplishment of the first two goals, measures are taken in the design of the MHTGR to minimize defects in the fuel so that normal operational releases or any accidental releases of primary circuit activity are low and worker exposures are minimized.

The unique aspect of the MHTGR, however, is the approach which has been taken to achieve the third goal and thereby minimize the design requirements from the fourth goal. To accomplish this with high assurance, the design of the MHTGR has been guided by the additional philosophy that control of radionuclide releases be accomplished primarily by retention of radionuclides within the fuel particles with minimal reliance on active design features or operation actions. The overall intent is to provide a simple safety case that will provide high confidence that the safety criteria are met. This approach is consistent with the NRC's Policy on Advanced Reactors (Ref. 1). There are two key elements to this philosophy which have had a profound impact on the design of the MHTGR.

First, the philosophy requires that control of radionuclides be accomplished with minimal reliance on active systems or operation actions. By minimizing the need to rely on active systems or operator actions, the safety case centers on the behavior of the laws of physics and on the integrity of passive design features. Studies need not center on an assessment of the reliability of pumps, valves, and their associated services or on the probability of an operator taking various actions, given the associated uncertainties involved in such assessments.

Second, the philosophy requires control of releases primarily by the retention of radionuclides within the coated fuel particle and with decreasing reliance on secondary barriers (such as the primary coolant boundary or the reactor building). Proof of containment is dramatically simplified if evaluations center on issues associated with fuel particle coating integrity. This proof is further simplified if the evaluations are based on easily understood and modeled transient characteristics. Specifically, the MHTGR's single phase coolant and low power density, refractory, annular core preclude core melt, large internally generated energetics, geometric reconfigurations, and their associated phenomenological uncertainties.

TOP-LEVEL REGULATORY CRITERIA AND USER SAFETY REQUIREMENTS

Top-level criteria and requirements are defined from two sources: the regulator, whose concern is primarily public health and safety and the user, whose concern is all encompassing (e.g., safety, performance, availability, and economics). Each of the four goals has been quantified by a series of top-level criteria and requirements (Refs. 2 and 3). The top-level regulatory criteria are the basis for plant licensability.

The following bases were adopted for the selection of top-level regulatory criteria:

1. Top-level regulatory criteria should be a necessary and sufficient set of direct statements of acceptable health and safety consequences or risks to individuals or the public. This ensures that the criteria are fundamental to the protection of the public and the environment.

2. Top-level regulatory criteria should be independent of reactor type and site.

3. Top-level regulatory criteria should be quantifiable to ensure that compliance can be demonstrated through measurement or calculation.

The following regulatory sources have been found to contain numerically-expressed criteria or limits which appropriately form top-level regulatory criteria:

1. 51FR28044 – Policy Statement on Safety Goals for the Operation of Nuclear Power Plants.

2. 10CFR20 – Standards for Protection Against Radiation.

3. 10CFR50, Appendix I – Numerical Guides for Design Objectives ... to Meet the Criteria "As Low As Reasonably Achievable" for Radioactive Material ... in Effluents.

4. 40CFR190 – Environmental Radiation Protection Standards for Nuclear Power Operations.

5. 10CFR100 – Reactor Site Criteria.

6. EPA-520/1-75-001 – Manual of Protective Action Guides for Protective Actions for Nuclear Incidents.

The utility/user group has specified an additional safety requirement (Ref. 3) that is more restrictive in that item 6 above of the top-level regulatory criteria is to be satisfied at the plant boundary. In this way the emergency planning zone, which is generally 16,000 m (10 miles) for United States light-water reactors (LWRs), is reduced to the MHTGR's 425 m Exclusion Area Boundary (EAB). This allows the utility/user to limit emergency drills to the area and personnel within its control. The need for offsite sheltering and evacuation is obviated, and the public's normal day-to-day activities are not disturbed by the proximity of the MHTGR plant. The specific quantitative user requirements are the Environmental Protection Agency (EPA) Protective Action Guidelines (PAGs) of 5 rem thyroid and 1 rem whole body doses evaluated at the 425 m EAB.

LICENSING BASIS EVENTS

For the purpose of deriving the regulatory licensing bases for the design, the probabilistic bases for the design have been cast in a framework and format similar to that of traditional licensing approaches. Postulation of a set of bounding licensing basis events is one of the key elements in the traditional regulatory process. Licensing basis events (LBEs) are used to demonstrate compliance with dose criteria for a spectrum of off-normal events. The use of PRA for LBE selection provides a basis for judging, in a quantitative manner, the frequency of the entire event sequence and, therefore, the appropriate dose or risk criteria to be applied.

Figure 4 provides the frequency-consequence risk plot defining three regions bounded by three frequencies and by corresponding consequence limits related to 10CFR50 Appendix I, 10CFR100 or the PAGs. Depending upon their predicted frequency, selected events are assigned to one of the following three categories:

1. Anticipated Operational Occurrences (AOOs) – These are families of events expected to occur once or more in the plant lifetime. Their dose consequences are realistically analyzed in the SARs to demonstrate compliance with 10CFR50 Appendix I.

2. Design Basis Events (DBEs) – These are families of events lower in frequency than AOOs that are not expected to occur in the lifetime of one plant but which might occur in a large population of MHTGRs. The DBEs are evaluated conservatively in the SARs against the 10CFR100 dose criteria.

3. Emergency Planning Basis Events (EPBEs) – These are families of events lower in frequency than DBEs that are not expected to occur in the lifetime of

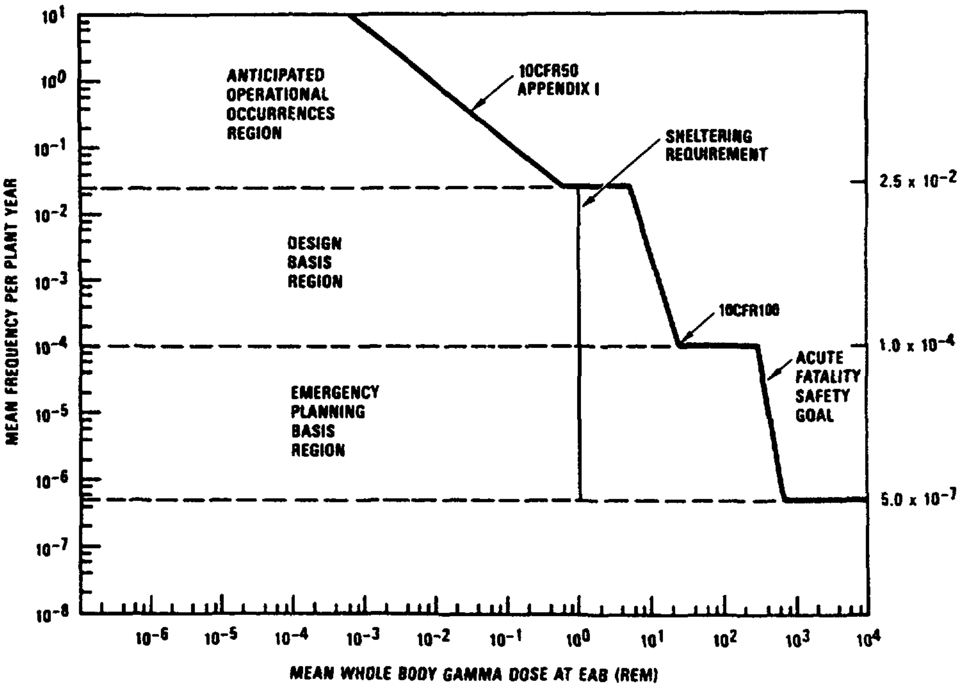


Fig. 4. Top-level regulatory criteria for mean frequency range/dose limits at site boundary

a large number of MHTGRs. The EPBE consequences are analyzed realistically in the PRA for emergency planning purposes and environmental protection assessments.

In addition to demonstrating compliance with the dose limits of the top-level regulatory criteria and the user safety requirements, the LBEs are considered collectively to show compliance with the NRC Policy Statement on Safety Goals (Ref. 4).

SAFETY DESIGN APPROACH AND RESULTS

The approach taken in the design of the MHTGR is to rely on the coated fuel particles for meeting the 10CFR100 doses and on other additional, largely passive retention barriers for meeting the more restrictive PAG doses. For example, even if all of the plateout and circulating activity is released, the total release is an order of magnitude lower than the 10CFR100 limits. Three functions have been identified which, when accomplished, assure that radionuclide retention within the fuel remains acceptable:

1. Remove core heat.

2. Control heat generation.

3. Control chemical attack.

There are many ways these functions can be accomplished, and the various LBEs utilize different design selections to perform the same function depending upon the accident scenario Generally, the less frequent LBEs rely more heavily on passive design features. For example, the MHTGR has three independent and diverse cooling systems, any of which can perform the function of removing core heat. However, while this multiplicity of systems contributes to increasing the margin of safety for the MHTGR and is considered in the LBE analyses, the MHTGR safety design approach emphasizes a minimum set of largely passive design features which, by themselves, are sufficient to accomplish these functions. How the MHTGR meets each of the three key safety functions is now briefly discussed by examining selected LBEs. Further, the ultimate capability of the MHTGR is demonstrated by examining events of still lower frequency that have been evaluated for the NRC to provide assurance that the plant's residual risk is negligible.

Remove Core Heat

The inherent features for heat removal include the intrinsic core dimensions and power densities of the reactor core, internals and vessel, and passive cooling pathway from the core to the environment as illustrated in Figs 5 and 6 Figure 7 presents the best estimate temperature transients for two LBEs, one with the primary system pressurized and one depressurized, in which the first two independent means of forced cooling are unavailable. Passive heat removal by conduction, radiation, and natural convection from the core through the vessel to the reactor cavity cooling system limit fuel temperatures to acceptable levels.

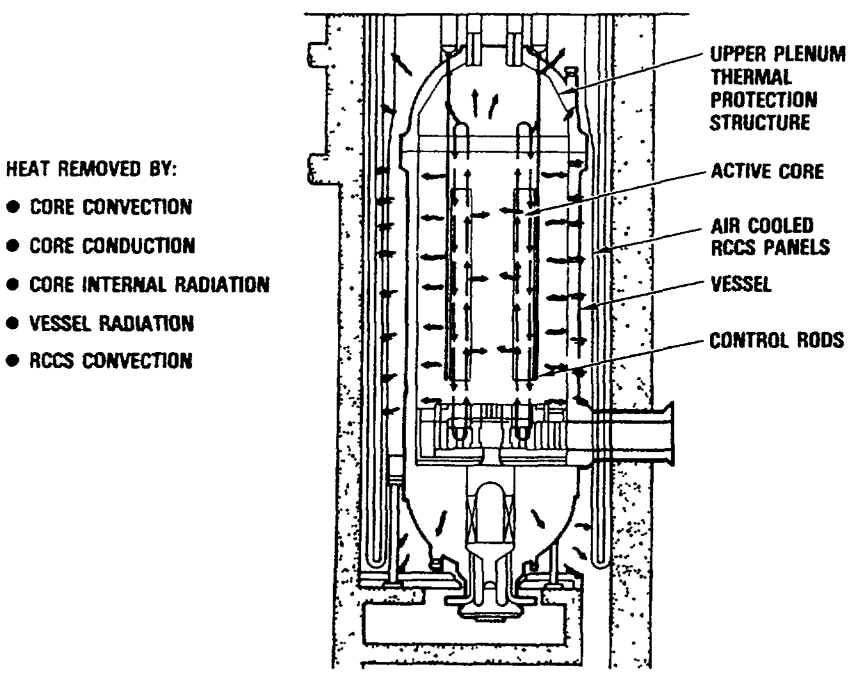


Fig. 5. MHTGR pressurized conduction cooldown heat flow paths

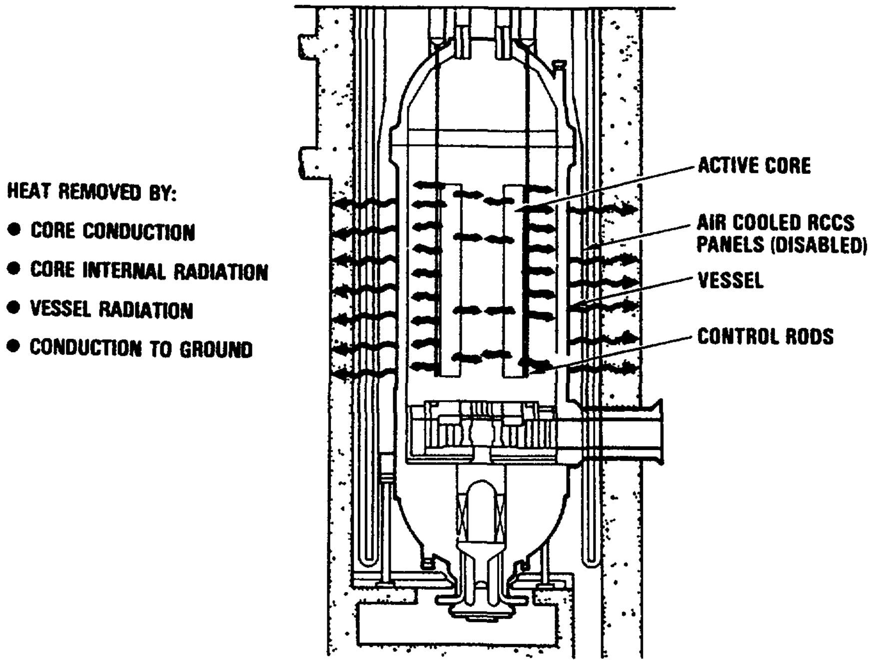


Fig. 6. Depressurized conduction cooldown heat flow paths

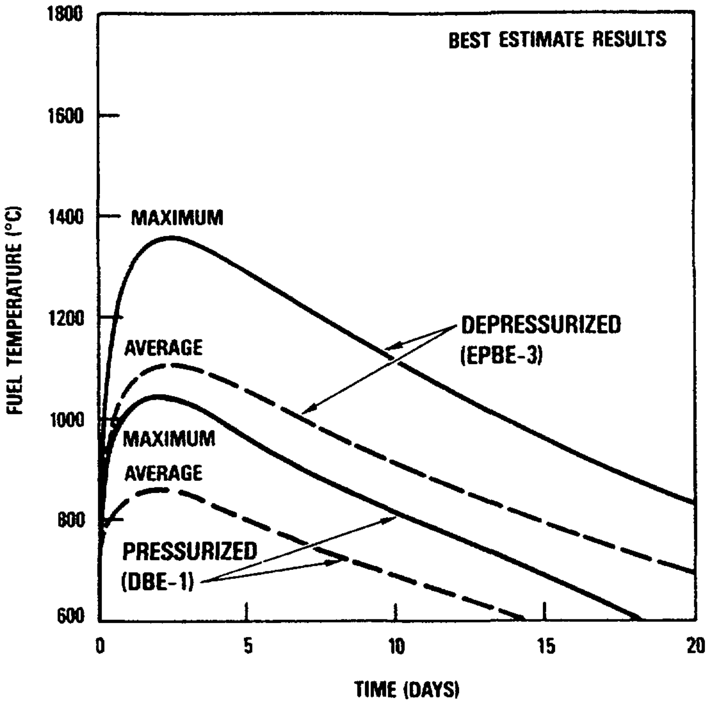


Fig 7 MHTGR fuel temperatures (best estimate) with passive heat removal during loss of forced cooling

Passive heat removal is possible due to the large thermal margins in the fuel. As shown in Fig. 8, the fuel must exceed approximately 2000°C before thermal decomposition for the silicon carbide coating results in significant failure. The normal peak fuel temperature is much lower at 1100°C.

Finally, the ultimate and unprecedented capability of the MHTGR to withstand challenges to heat removal is demonstrated in Fig. 9 where the passive air-cooled RCCS panels are assumed to be completely ineffective. As shown, the maximum core temperature are little effected and remain within acceptable levels as the heat is transferred into the building and ground. Note, also, that removal of core heat in the MHTGR is largely independent of maintaining any coolant flow path geometry.

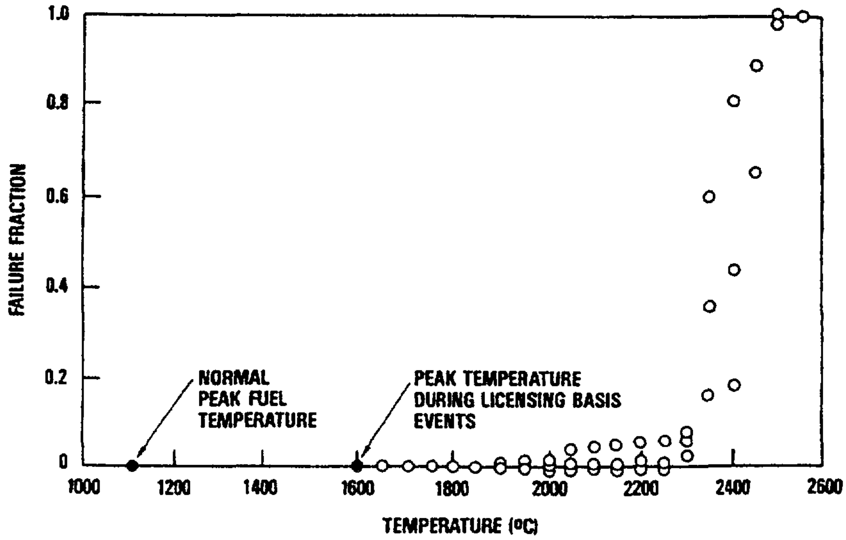


Fig. 8. Integrity of MHTGR coated fuel particles at high temperatures

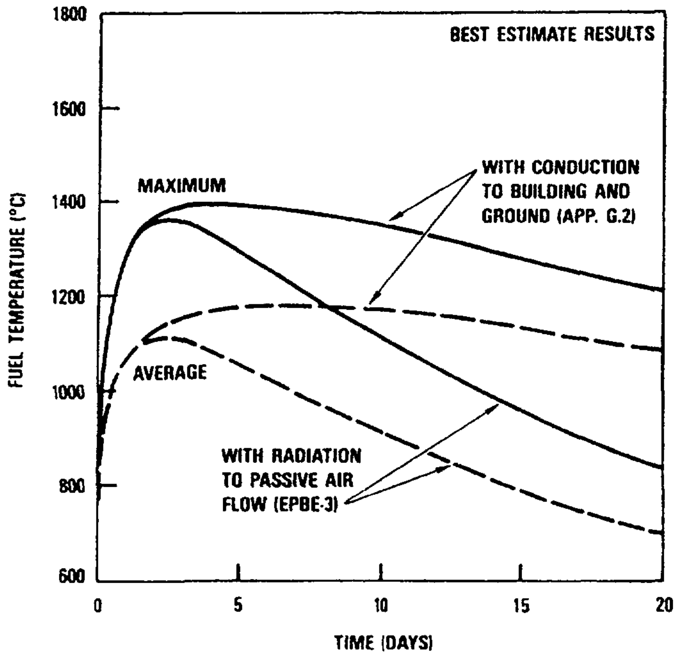


Fig. 9. MHTGR fuel temperatures (best estimate) during loss of forced cooling at depressurized conditions with and without the passive air cooling system

Control Heat Generation

The inherent features that control reactivity include a strong negative temperature coefficient, a single phase (no void coefficient) and neutronically inert coolant. These characteristics cause the reactor to inherently shutdown. As shown in Fig. 10 for a pressurized conduction cooldown, fuel temperatures remain low and within acceptable limits regardless of whether reactor trip occurs and even if all control rods are withdrawn (a reactivity addition of ~3%). Accidental ingress of water is limited by the amount of steam the core can physically hold (724 Kg pressurized and 63 Kg depressurized) and is, therefore, bounded by the above reactivity addition. Furthermore, the plant protection system, which is separate from the operational system, includes two diverse reactivity control systems that are gravity inserted and highly reliable to protect against even rarer events.

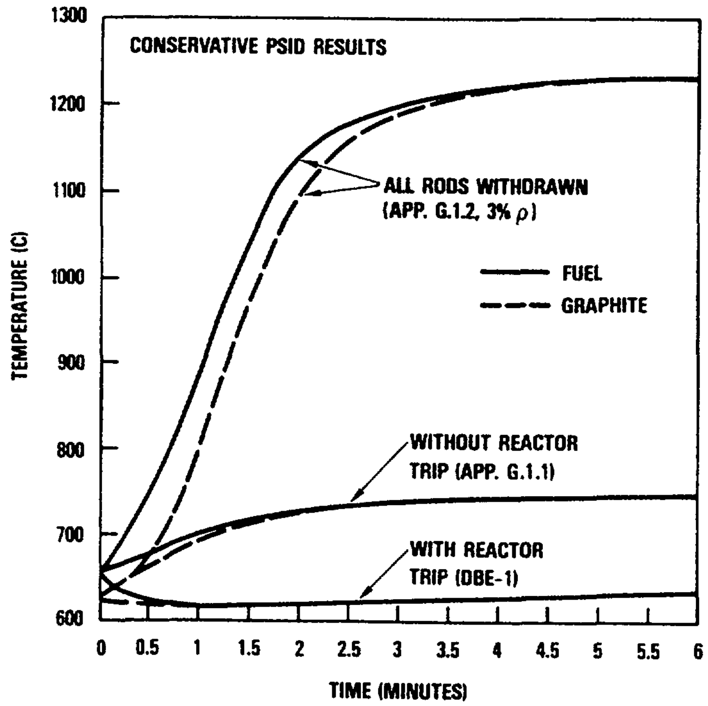


Fig. 10. Control of MHTGR fuel temperature by negative temperature coefficient during loss of forced cooling

Control Chemical Attack

The inherent features for controlling chemical attack of the fuel by water include the nonreacting coolant, a water-graphite reaction that is endothermic and requires temperatures above the average normal operating conditions and the silicon carbide coatings on the fuel itself. The MHTGR design features that limit water ingress and its consequences include the limited sources of water, reliable detection and isolation systems and two forced convection core cooling systems.

Figure 11 presents the time-dependent fraction of the core graphite oxidized for two LBEs and a very rare bounding event that challenge the control of chemical attack.

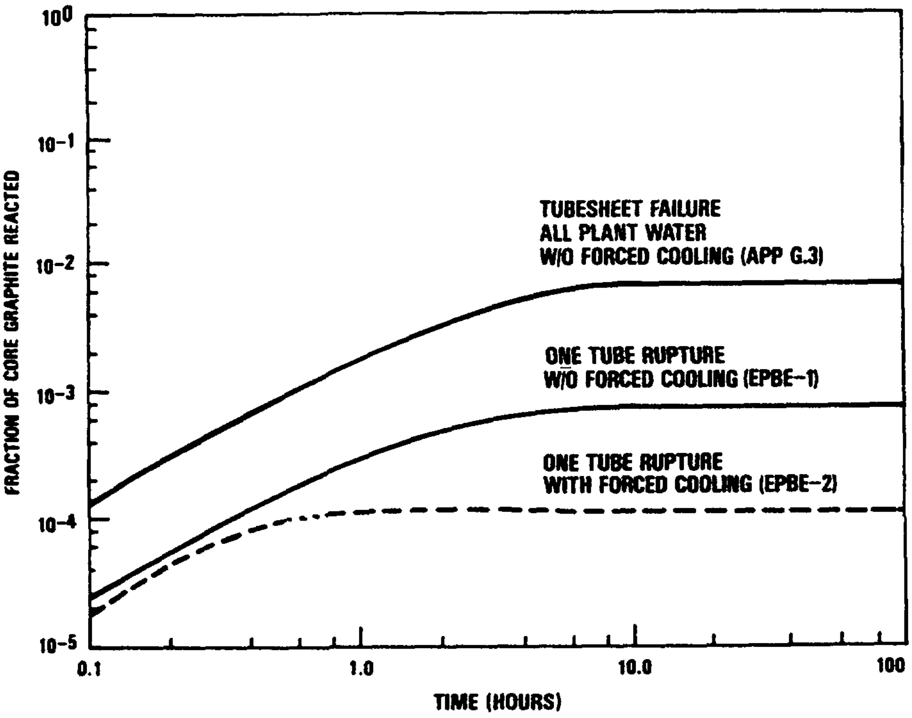


Fig. 11. Integrity assurance of MHTGR coated fuel particles during water ingress

In all cases, whether forced cooling is available or lost or whether one or more steam generator tubes fail, the impact on the core graphite is small even without successful moisture detection. Furthermore, and most importantly, the high quality of the fuel particle coatings limits the radionuclide inventory available for release due to water chemical attack to those particles with initially failed coatings (from either in-service failure or manufacturing defects).

The inherent features for controlling chemical attack of the fuel by air include the nonreacting coolant, the embedded ceramic fuel particles, the nuclear grade vessel and the below-grade reactor silo. Figure 12 presents the fraction of the core graphite reacted by air ingress following primary coolant leaks without forced core cooling (two LBEs and two extremely rare bounding events). As shown, the fraction reacted is very small in all cases. The primary reason for the small amount of oxidation is the large resistance to flow that the coolant holes provide (L/D > 700). Once again, the impact on the core graphite is small and the fuel remains intact.

SAFETY IMPORTANCE OF OPERATOR ACTIONS

By minimizing the need to rely on active systems or operation actions, the safety evaluations are more transparent and need only consider the integrity of and natural behavior of the passive reactor materials not on the reliability of pumps, valves, and their associated services nor on the probability of an operator taking correct actions. Furthermore, with emphasis on a passive safety design, the plant is insensitive to incorrect operator actions, thus largely removing the man-machine interface from the safety discussion.

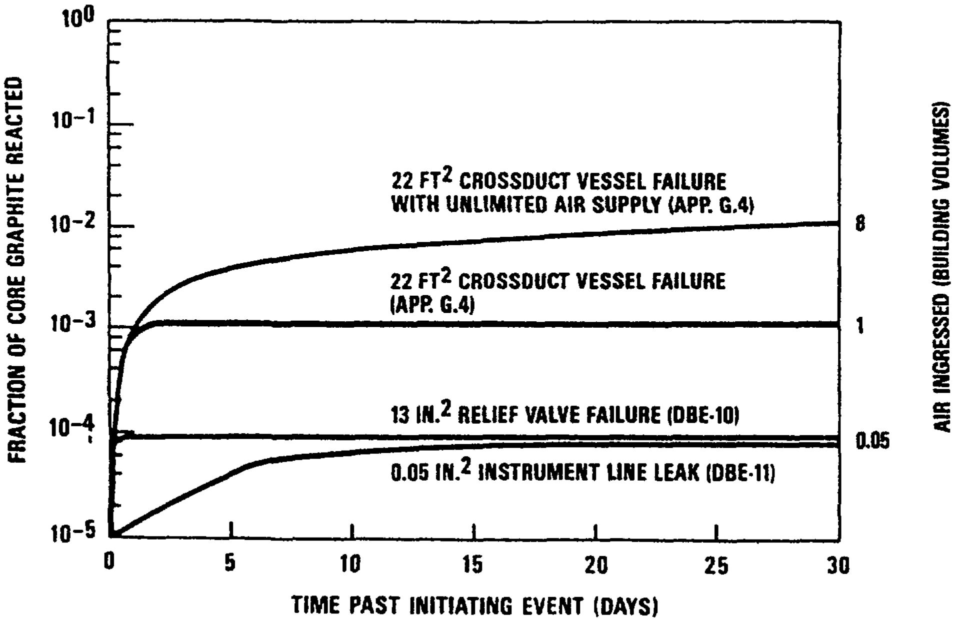


Fig. 12. Insignificant oxidation of MHTGR graphite limited by air mass transfer and core temperatures

The MHTGR safety approach of placing primary emphasis on retention of the radionuclides within the coated fuel particles narrows the assessment of incorrect operator errors to the same three key functions discussed above. As shown in Fig. 13, the broad spectrum of events considered bounds potential operator errors. No events have been identified in which an action by the operator can defeat the natural behavior of the passive feature. Similar conclusions can be drawn for intentional, malevolent acts of sabotage as extreme as the willful destruction of the reactor vessel in a catastrophic fashion

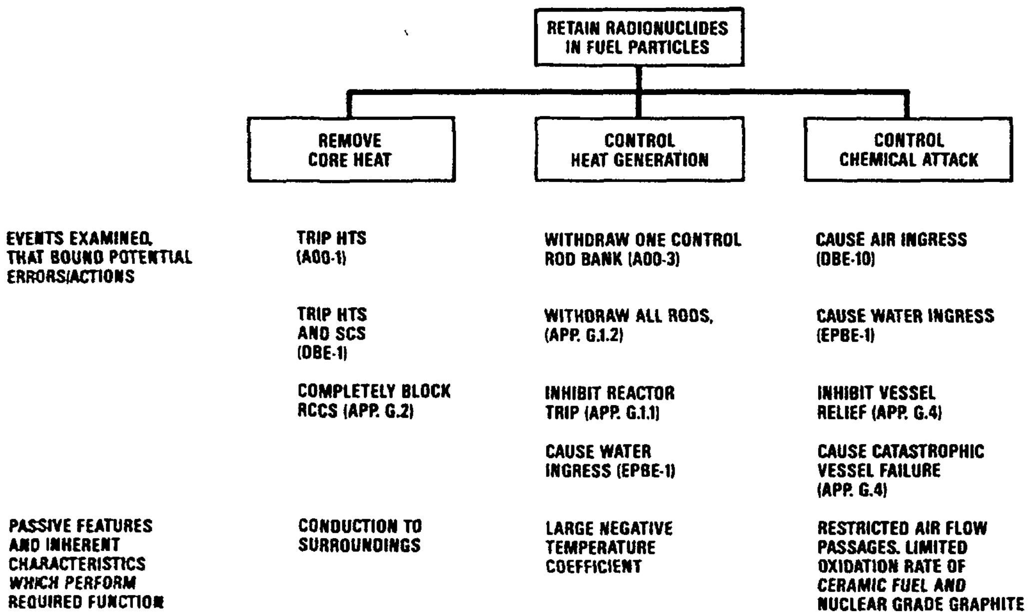


Fig. 13. Assessment of MHTGR sensitivity to operator errors and sabotage

The results of the PRA are depicted in Fig. 14 in comparison to the top safety criteria. As shown, the risk is below that received from commonly accepted activities even for very infrequent events. Essentially there is an intrinsic consequence cap that corresponds to the retention of the radionuclides within the fuel particles. Thus, the passive safety features of the design prevent and mitigate radionuclide release over a wide spectrum of off-normal events which include failure of active systems, operator errors of omission, and commission and acts of sabotage.

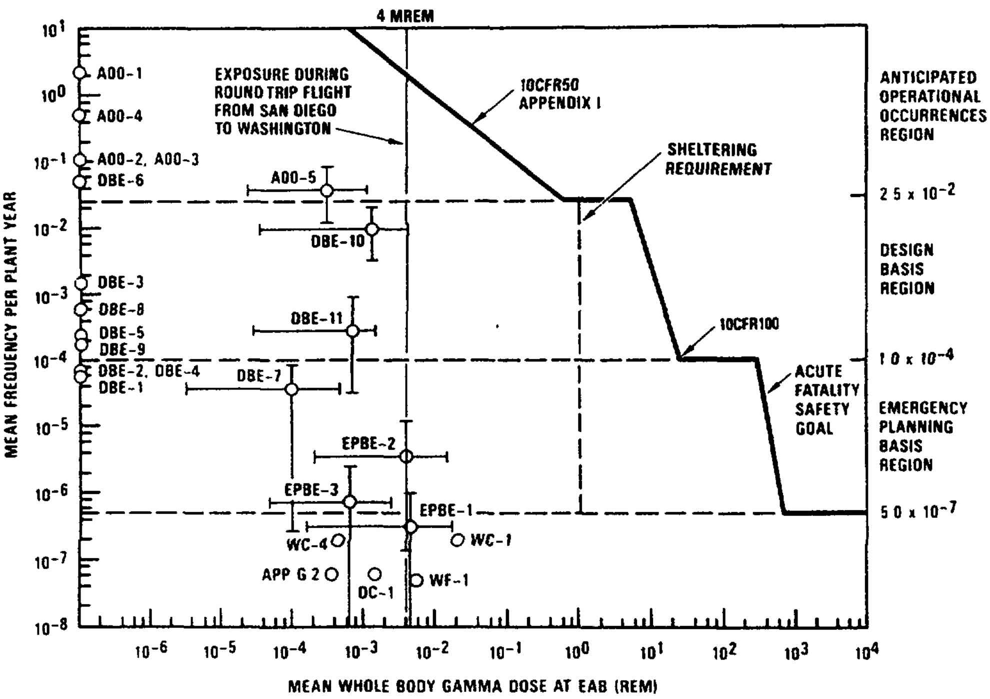


Fig. 14. Comparison of MHTGR risk to top-level safety requirements

ACKNOWLEDGEMENTS

The authors would like to thank U.S. Department of Energy for approval to publish this paper. Thanks are also expressed to the management of General Atomics for permission to write and present this work, which was supported by the Department of Energy, San Francisco Operations Office Contract DE-AC03-89SF17885.

REFERENCES

1. U.S. Nuclear Regulatory Commission, "Policy for the Regulation of Advanced Nuclear Power Plants," Federal Register, Vol. 51, p. 24643, July 8, 1986.

2. "Top-Level Regulatory Criteria for the Standard MHTGR," DOE Report DOE-HTGR-85002, Rev. 2, October 1986.

3. "Utility/User Requirements for the Modular High Temperature Gas-Cooled Reactor Plant," Gas-Cooled Reactor Associates Report GCRA 86-002, Rev. 3, June 1987.

4. U.S. Nuclear Regulatory Commission, "Safety Goals for the Operation of Nuclear Power Plants, Policy Statement," Federal Register, Vol. 51, No. 149, pp. 28044-28049, August 4, 1986.

SPECIAL INVITED PRESENTATION

PUBLIC ACCEPTANCE OF NUCLEAR POWER

C. Starr

Electric Power Research Institute
Palo Alto, California
United States of America

I would like to take this luncheon opportunity to explore the general question of what actions the technical community might take to keep nuclear power alive and growing. I assume that objective is our common goal.

This meeting is focused on the need for nuclear power, its safety objectives and criteria, and its engineered and inherent safety characteristics. These are obviously important issues for an audience of nuclear engineers, the electricity industry, and government planners and regulators. As a technologist, I do not question the long-term importance of our technical developments. However, I believe that such matters are of minor significance to the public, and will have only secondary influence on public acceptance of nuclear power. For the future of nuclear power in a democratic world, I believe public attitude is more significant than advanced technology. With the pervasive public fear of radiation, the issue becomes protection of the public from radiation exposure.

Public attitude is (in my opinion) intuitively determined by the public's perception of the quality of the risk management for prevention and emergency preparedness. While the public does pay attention to the opinions of expert professionals, it is generally skeptical of the "trust me" attitude of technologists, especially when there is professional controversy. Most of the public does not believe that "accidents can't happen," and thus interprets real performance accordingly.

Each reported accident is a signal to the public that something is wrong with either the engineering design or the management of operations. The post-accident consequences reveal the state of emergency preparedness, the scope of the public exposure, the long-term effects, and the ease of recovery. The public reacts intuitively to this body of information, and develops its own perception of the magnitude of the risks to them. The public does not have an intuitive confidence in professional risk assessments or probability estimates.

Our classic example is the TMI-2 accident. If this had been a pre-planned demonstration of the containment efficacy of a severe accident, and had been technically and publicly organized for this purpose, it would have been declared a great success. As an unplanned accident, it revealed engineering errors, lack of institutional preparedness, and official hysteria and incompetence. The public's strong intuitive interpretation of these signals was a major blow to our national nuclear power program. To the public, the demonstration of containment was secondary, whereas the demonstration of incompetence was primary.

In a lecture I presented five years ago to the Society of Risk Analysis on the importance of public confidence in risk management, I described the following illustrative scenario.

Almost every big city has a zoo, and in any popular zoo there is usually a tiger. It would be intriguing to make a public risk assessment of the consequences of a tiger escaping from the zoo. We might crudely estimate from historical reports that there is a probability of 1 in 1,000 per day worldwide (or once in three years) of a tiger escaping, followed by a 1 in 10 chance of killing a nearby resident, resulting in a 1 in 10,000 chance of death per day worldwide (or about once in 30 years) for populations near zoos.

What are the options to protect the public? There are basically three--political, technical, and managerial. A political solution is to eliminate all tigers from zoos. A technical solution is to declaw and defang the tiger. A managerial solution is to cage the tiger securely and provide alert zoo keepers to keep the access gates closed. How has the public chosen among these three?

The public acceptability of zoos is obviously not influenced by risk assessments. Even though we know that wild animals do occasionally escape from zoos, the public certainly considers them safe and acceptable enough to visit frequently with their children. What is obviously acceptable to the public is the assurance by the zoo keeper that the tiger is securely caged. The point I wish to make is that it is not the risk assessment of the hazard from escaping tigers which is key to societal acceptance of zoos, but rather confidence that the management approach to coping with the risk is reasonably reliable.

My point is very simple. Public acceptance of any risk is more dependent on public confidence in risk management than on the quantitative estimates of risk consequences, probabilities, and magnitudes. This, of course, shifts the important assessment from a frequency/consequence analysis to a determination of what is meant by "reasonably reliable" risk management. I am suggesting that the practical public answer to the question, "How safe is safe enough?", depends more heavily on the operations established for the management of risk than it does on the quantitative description derived from risk assessments. If this is indeed so, then we should recognize this in our public discussions of the societal acceptability of nuclear power.

It is clear that the public wants credible assurance of no harm to any individual involuntarily exposed to the consequences of an accident. This is the criterion of the maximally exposed individual, as contrasted with group risk taking. When a new alternative is proposed as a supplement rather than as a replacement for an existing system to which it has adjusted, the public perceives an added risk to an existing accepted level. Nuclear power faces this issue, and we, the technical community, should focus our attention on those areas of risk management that involve public exposures. We also face the issue of establishing public confidence in our risk management competence.

We know what these are, but they have not had the level of technical and institutional attention they need for public confidence. For example, the technical community should seek improved systems for handling, transporting, storing, and disposing of both high- and low-level wastes. Technology may also be applicable to improved early warning systems, source term reduction, emergency preparedness equipment and organization, radioactivity surveillance for both ground and air, medical support, and all the other features of a fully adequate emergency capability. The demonstration of this capability may also be required to establish its credibility. This is a complex public relations issue. Our past industry reluctance to accept the burden of complex emergency response preparedness has created a negative image of the industry's concern for public safety.

We should also be professionally concerned with the criteria for initiating remedial steps, both pre- and post-accidents. We need international and interagency common standards for the de minimis physiologic levels which guide the several action steps involved in regional emergency responses. These are based on a mix of tradeoffs among societal objectives, comparative risk assessments, and regional cultures. They are too important to be left solely to the regulatory agencies.

I believe that the technical community can develop a fully credible risk management system that has the capability to protect every member of the public from significant involuntary exposure. The unpredictable difference between system capability and actual future performance is commonly accepted by the public as characteristic of rare event preparedness, and is presumably minimized by assiduous training (as with firefighting departments). Public confidence in nuclear system capability should be our target. We should make this goal a top priority.

SPECIAL SAFETY ISSUES:
SAFETY ASPECTS OF NEW DESIGNS AND CONCEPTS FOR NUCLEAR POWER PLANTS
(continued)

(Session VII)

Chairmen

J. BERANEK
Czechoslovakia

K.B. STADIE
Nuclear Energy Agency of the OECD

EXTERNAL EVENTS: EARTHQUAKES, FIRES AND FLOODS

D. OKRENT
Mechanical, Aerospace and Nuclear
Engineering Department,
University of California,
Los Angeles, California,
United States of America

Abstract

A subjective perspective will be given of the current state of affairs in the U.S.A. with regard to the treatment of risks to nuclear power plants arising from earthquakes, fires and floods, with relatively brief mention of high winds/tornadoes and transportation accidents. The emphasis will be on existing light-water reactors (LWRs).

1. INTRODUCTION

The principal references for this paper are the 1987 report by Kimura and Budnitz [1], the 1988 supplement by Prassinos [2[, the May, 1989 report by Budnitz and Lambert [3], and NUREG 1150: Second Draft for Peer Review [4]. Budnitz is attending a competing workshop in Idaho this week on a similar subject, or he could be here in person. Let me begin by quoting from Budnitz and Lambert, as follows:

"Unfortunately, the limitations that continue to exist in the external-initiator methodologies have convinced many safety decision-makers that the insights available are not reliable and therefore not useful. Often, these decision-makers decide to give little or no weight to the results obtained, even though externally-initiated accident sequences typically account for 10% to 30% of the total core - damage frequency in most recent full-scope PRAs. A few recent items attest to this strong negative attitude:

"At a recent (August, 1987) NRC-sponsored symposium in Annapolis on the subject of external initiators, the IDCOR representative stated that external-initiators analysis of existing plants, in the context of the IPE, was not necessary, or at least sufficiently low priority to justify being left out of the IPEs all together (Ref.LLNL/Annapolis, 1987). This opinion is apparently shared by many in the industry, although a gradual shift is underway.

"The recent NRC IPE (Individual Plant Evaluations) generic letter (Ref/ NRC/IPE GL, 1988) requires examining only internal initiators, and states that external-initiator IPE evaluations will be required only sometime later.

"The number of papers on external initiators at the recent PSA'89 international conference in Pittsburgh (Ref. PSA'89/Pittsburgh, 1989) was only about 4% of the total, all in one session.

"In the key opening session of PSA'87 in Zurich (Ref. PSA'87/-Zurich, 1987), in which top regulators from all of the principal countries spoke, there was no mention of external initiators. In the question-and-answer period, in response to a direct question from Dr. Budnitz, one top regulator stated that in his opinion the concern for external-initiator accident was overstated, and the other top regulators on the panel seemed to agree fully."

This paper appears to be the only invited paper on external events at this workshop, which, if correct, seems to continue the pattern observed by Budnitz and Lambert [3]. They do note that the NRC Staff has recently increased its attention to the overall issue of how external initiators should be regulated, but go on to state that the underlying problem remains, namely that too many utility, regulatory and other decision makers still don't understand that these initiators can be very important.

Kimura and Budnitz [1] identify two figures-of merit from the NRC Policy Statement on Safety Goals [5], namely that the mean core damage frequency should be in the range of 1 E-5 per reactor year or less and that the overall mean frequency of a large release of radioactivity to the environment (which they associate with early containment failure) should be equal to or less than 1 E-6 per reactor year. They examine internal fires, high winds/tornadoes, external floods, and transportation accidents in terms of these evaluation criteria, keeping in mind that there is a distribution about the mean. They conclude that all the aforementioned external events must initially be considered, based on a comparison of available information with the core damage figure-of-merit, that the potential importance of internal fires is generic to all plants, but that it may be possible to screen out winds/tornadoes, external floods, and transportation accidents based on site or plant characteristics, or frequency considerations. The five PRA's they examined did not reveal any fire-initiated sequences leading to large releases with frequencies above about 1 E-9. However, they stated that whether this finding was generally applicable could not be determined. NUREG-1150, Draft 2 [4], appears to provide contradictory evidence. Peach Bottom and possibly Surry, the two plants evaluated for external events, yield early containment failure frequencies due to fire which are comparable to or larger than the 1 E-6 figure-of-merit.

In a supplement to Reference 1 that deals with seismic hazards, Prassinos concludes that the seismic external hazard is important with respect to both figures-of-merit [2]. NUREG-1150, Draft 2 corroborates the finding by Prassinos.

2. INTERNAL FIRES

Kimura and Budnitz present the core damage frequencies from seven different internal fire PRAs reported during the period 1982-84 [1]. Table 1 reproduces the fire PRA results presented in Reference [1].

Budnitz and Lambert [3] present an evaluation of the reliability and usefulness of external initiator PRA methodologies. They conclude that the methodology can be competently used for screening potential fire locations; that the data base provides a good starting point for the determination of fire-initiation frequencies; and that although the COMPBURN III code [6] has limitations and that several technical issues are not well analyzed, the code can provide reasonable quantitative results on the time for fire growth, spread, and damage, albeit with large uncertainties. Barrier adequacy (ie, will a nominal 3 hour barrier really meet its rating?) is one issue of potential significance [7].

TABLE I. Core Damage Frequencies from Internal Fire PRAs.

Station	Mean, Core Damage Frequency/Rx-yr for Fires	for All Initiators	Fraction
Zion 1-2	1.8 E-6	5.7 E-5	3%
Indian Point 2	1.4 E-4	4.7 E-4	30%
Indian Point 3	9.6 E-5	2.3 E-4	40%
Big Rock Point	2.3 E-4*	9.8 E-4	23%
Limerick	2.3 E-5	4.4 E-5	55%
Seabrook	2.5 E-5	2.3 E-4	12%
Oconee 3	1.0 E-5	2.5 E-4	4%
Millstone	4.8 E-6	7.0 E-5	7%

*The Big Rock Point analysis Produced a "point estimate", not a mean value.

Budnitz and Lambert conclude that the time duration for detection and suppression is subject to considerable uncertainty, and that there are several weaknesses and omissions in current fire PRA practice, including the following:

- the fire fragility of cabling warrants more detailed treatment
- indirect and secondary effects such as the effects of smoke, low-level thermal exposures, and interactions among smoke, corrosive gases, water and steam are not well understood
- seismic-initiated fires and accidents arising from spurious or inadvertent actuation of fire suppression equipment have not been studied [7].

Overall, Reference [3] concludes that uncertainties in the bottom-line results can be plus-or-minus an order of magnitude or more, but that fire analysis PRA should be done, and it has many significant side benefits.

The NUREG-1150, Draft 2 results for core damage frequency are summarized in Tables 2 and 3 for Surry and Peach Bottom. The NUREG-1150 conditional probability distributions for early containment failure at Surry and at Peach Bottom are given in Figures 1 and 2.

Table II. Summary of Core Damage Frequency Results: Surry.

	5%	Median	Mean	95%
Internal Events	6.8 E-6	2.3 E-5	4.1 E-5	1.3 E-4
Station Blackout				
Short Term	1.1 E-7	1.7 E-6	5.4 E-6	2.3 E-5
Long Term	3.2 E-8	4.2 E-7	1.6 E-6	5.9 E-6
ATWS	3.2 E-8	4.2 E-7	1.6 E-6	5.9 E-6
Transient	7.2 E-8	6.9 E-8	2.1 E-6	6.0 E-6
LOCA	1.2 E-6	3.8 E-6	6.0 E-6	1.6 E-5
Interfacing LOCA	3.8 E-11	4.9 E-8	1.6 E-6	5.3 E-6
SGTR	1.2 E-7	7.4 E-7	1.8 E-6	6.0 E-6
External Events				
Seismic (LLNL)	3.9 E-7	1.5 E-5	1.2 E-4	4.4 E-4
Seismic (EPRI)	3.0 E-7	6.1 E-6	2.5 E-5	1.0 E-4
Fire	2.2 E-6	8.3 E-6	1.1 E-5	3.1 E-5

Table III. Summary of Core Damage Frequency Results: Peach Bottom.

	5%	Median	Mean	95%
Internal Events	3.5 E-7	1.9 E-6	4.5 E-6	1.3 E-5
Station Blackout	8.3 E-8	6.2 E-7	2.2 E-6	6.0 E-6
ATWS	3.1 E-8	4.4 E-7	1.9 E-6	6.6 E-6
LOCA	2.5 E-9	4.4 e-8	2.6 E-7	7.8 E-7
Transient	6.1 E-10	1.9 E-8	1.4 E-7	4.7 E-7
External Events				
Seismic (LLNL)	5.3 E-8	4.4 E-6	7.7 E-5q	2.7 E-4
Seismic (EPRI)	2.3 E-8	7.1 E-7	3.1 E-6	1.3 E-5
Fire	1.1 E-6	1.2 E-5	2.0 E-5	6.4 E-5

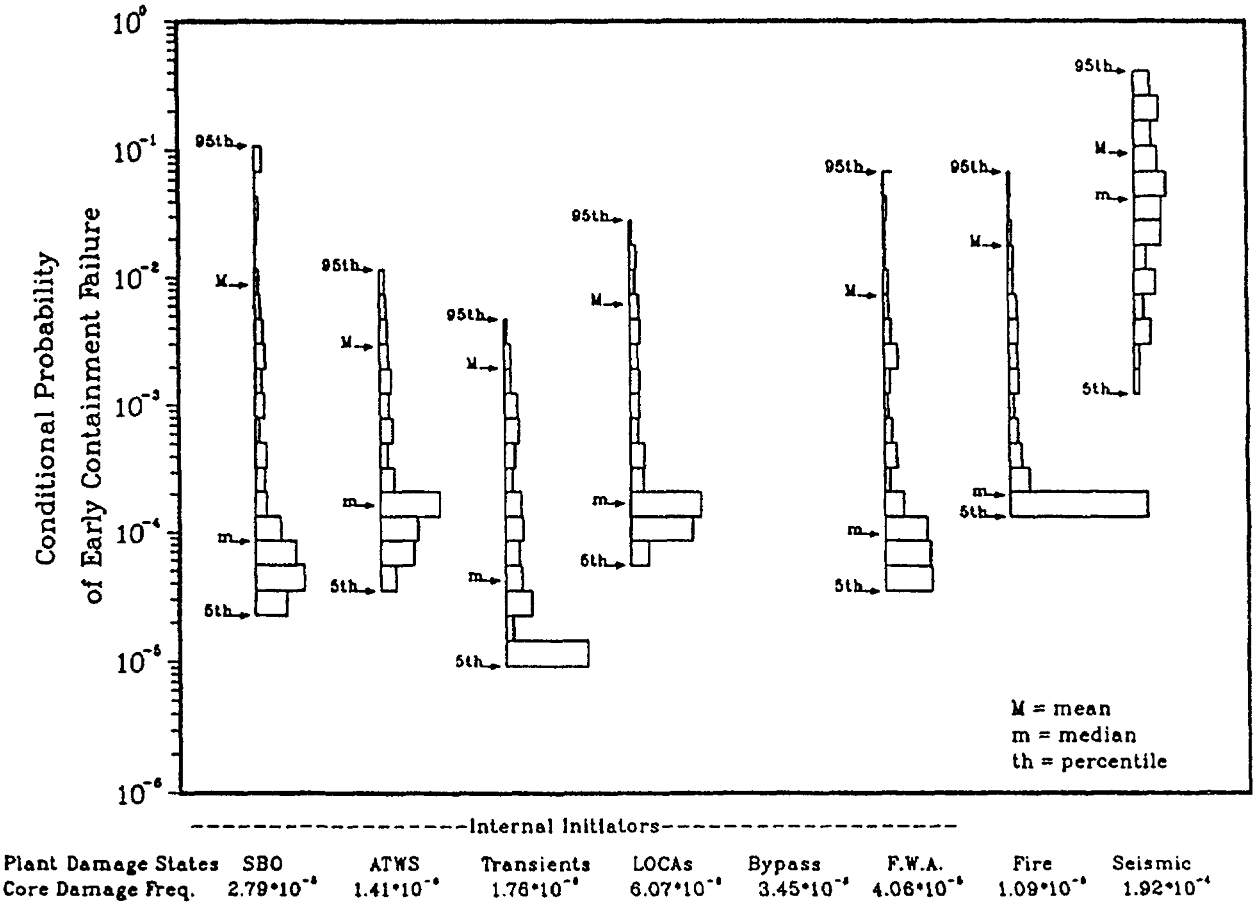


Figure 1: Conditional Probability Distributions for Early Containment Failure at Surry.

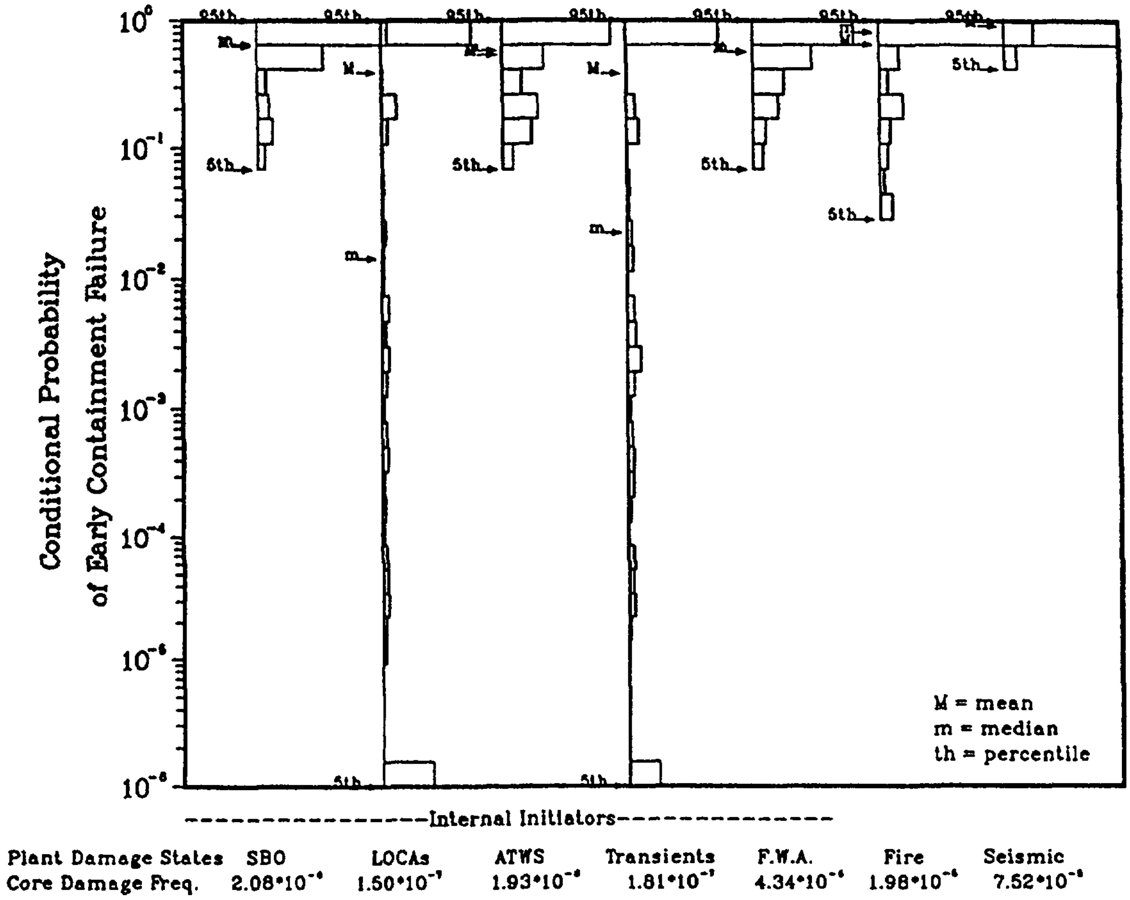


Figure 2: Conditional Probability Distributions for Early Containment Failure at Peach Bottom.

With regard to the results presented for Surry and Peach Bottom, one needs to keep in mind that these plants have each been subject to a few PRAs over the years, and the risk evaluations in NUREG-1150 reflect a fixed-up plant, albeit an older plant. By no means is it the plant as it was when it first went into operation.

3. HIGH WINDS/TORNADOES

Kimura and Budnitz [1] examined the PRA predictions of core damage frequency for seven plants and the results of abbreviated PRAs performed under the auspices of the NRC's program on generic issue A-45, Decay Heat Removal, for five relatively older plants. Of the twelve plants reviewed, several yielded mean or point core damage frequency estimates significantly larger than 1 E-6 or 1 E-5. In each such case, one or more structures were assessed as vulnerable to high winds and/or tornado winds. Some relatively newer plants, such as Seabrook or Millstone 3, were evaluated as having a negligible contribution to risk from this initiator.

Budnitz and Lambert [3] conclude that, although site-specific wind hazard curves used in PRAs have significant numerical uncertainties, the methodology is mature and reasonably reliable., and that for most plants the analysis can be abbreviated or consist of a screening effort which demonstrates that the plant layout and design are very well protected against extreme winds.

4. EXTERNAL FLOODS

The different types of flooding events are generally classified in terms of the type of site, as follows: [1]

1. All sites: flooding due to severe local precipitation and runoff effects;
2. River sites: flooding due to too much water in the river (from precipitation runoff, ice jams, etc.);
3. River sites: flooding due to an upstream dam failure;
4. Ocean, estuarine sites: flooding due to combinations of wave effects, high wind-driven water levels, surges, seiches, etc.;
5. Ocean sites: flooding due to a tsunami;
6. Lake sites: flooding due to a combination of high lake water level, wave effects, high wind-driven water levels, surges, seiches, ice jams, etc.;
7. All sites: flooding due to earthquake -induced effects, such as landslides, dam failures, etc.

1. Kimura and Budnitz [1] conclude that there seems to be no generally accepted methodology for developing peak flood levels for severe local precipitation events having a frequency of 1 E-3, and the situation deteriorates for less frequent events. During the Systematic Review Program of ten of the oldest U.S. nuclear power plants, one plant (Ginna) did have to backfit this event, but the level of risk reduction was not quantified [8]. Like many of the external flooding events, comparative evaluation against the core damage or the large release figure-of-merit is very difficult, and for plants vulnerable to such flooding, assessing the risk contribution is very uncertain.

2. Kimura and Budnitz [1] again conclude that for flooding of river sites extrapolations beyond the historical record are difficult except in those few (site-specific) situations where good regional data and a good local site model allow defensible analyses. In any event, extrapolations beyond about 1 E-3 per year are highly uncertain [1,3]. In support of this pessimism, they refer to a 1986 report by an Interagency Advisory Committee which questions extrapolations to 1 E-3 [9]. They also refer to an 1988 study performed under the auspices of a Committee of the National Academy of Sciences, which was somewhat more optimistic, believing that methods do exist for making estimates down to the range of 1 E-3 per year, or even lower, if appropriate watershed data can be obtained [10].

   Although the frequency of exceeding design basis flood levels does not automatically translate into core damage frequency, estimates of the risk contribution from this source remain highly uncertain , if the plant is vulnerable.

3,7. Kimura and Budnitz state that realistic calculations of dam failure probability as a function of extreme conditions are difficult to find in the literature. The Oconee PRA [11] estimates 1 E-6 per year or lower for modern, well-engineered dams. On the other hand, some dam failures could be in the range 1 E-3 or 1 E-4 per year, [11].

   A recent probabilistic flood hazard assessment for the N Reactor at Hanford found that the extreme floods occur as a result of dam failure, in this case the Grand Coulee Dam or the Mica Dam in Canada upstream of the Grand Coulee Dam. The N Reactor pumphouse has a floor elevation of 421 feet mean sea level (msl), while other safety related structures are located at approximately an elevation of 450 feet msl.

The results of the probabilistic analysis by McCann and Boissonnade [12] indicate the mean frequency of exceeding the elevation of the pumohouse floor, 421 feet msl, is 7 E-4 per year, while the mean frequency of floods exceeding plant grade is 7.5 E-5 per year. One other similar benchpoint arises from the Systematic Evaluation Program in which Connecticut Yankee was vulnerable to an upstream dam failure at roughly the same frequency [8]. The Oconee PRA [11] found a mean value of 2.3 E-5 for core damage frequency from flooding, due to the possible failure of Jocassee Dam from non-seismic causes.

4,5,6. In connection with other modes of flooding, it is noted that a study of Turkey Point performed as part of the A-45 project estimated a core-damage frequency of 2 E-4 with no offsite power recovery due to hurricane-induced/storm-surge flooding. With offsite power recovery, this number dropped to 1 E-5 per year.

In summary, without consideration of any potentially adverse impacts from the Greenhouse effect in future years, predictions of external flooding-caused core damage from the various flood scenarios are subject to great uncertainties at vulnerable sites, when one considers frequencies less than 1 E-3 per year.

5. TRANSPORTATION ACCIDENTS

Kimura and Budnitz conclude that transportation accidents may need to be considered among the external hazards to U.S. nuclear power plants. They state that this is primarily due to the lack of probabilistic analysis of the plant's response to a nearby transportation accident [1].

They divide transportation accidents into five categories, namely, aviation, marine (ship/barge), pipeline, railroad, and truck. Empirical data is thought to provide a reasonable basis for estimating the accident frequency for railroads, general aviation, and commercial aviation [3]. For pipeline operations, military aviation, and ship/barge traffic, current reliable date were not found, nor does up-to-date frequency information exist for truck accidents [3]. For some plants, like San Onofre for truck accidents, and the Waterford plant for railroad and marine accidents, the accident frequency is sufficiently large that an analysis of the impacts is needed [1].

Another issue which arises is that of a change in accident conditions over the life of the plant. For example, according to the Three Mile Island 2 Safety Evaluation Report, the risk from commercial plane crashes was judged acceptably low for Units 1 and 2, provided that less than 2400 operations per year occurred at Harrisburg Airport by aircraft whose weight exceeded 200,000 pounds. Since the time of that safety evaluation, air traffic has grown to about 6000 departures per year, about half of which are planes exceeding 200,000 pounds. Kimura and Budnitz estimate this leads to an accident frequency within 2.5 miles of the Three Mile Island site of 1 E-4 per year for the heavier aircraft [1]. A probabilistic evaluation of the effects of such crashes is not available.

6. SEISMIC

Prassinos [2] reviewed a large body of seismic-safety related information, including seismic PRAs performed by industry, and the seismic analyses performed as part of the work on TAP A-45, Decay Heat Removal Requirements.

The summary of industry PRA results is reproduced from Reference [2] as Table 4. The summary of A-45 seismic PRA results is reproduced as Table 5.

Table IV. Seismic Core Damage and Release Frequencies from Published Probabilistic Risk Assessments.

Plant	Type	SSE (g)	Seismic Core Damage Frequency (mean) Per Year	Seismic Release Frequency (mean) Per Year	% of Total Core Damage	Rank of Release Sequence	Dominant Earthquake Level (g)
Zion 1 & 2	PWR	0.17	5.6 E-6	-------	3	1	>0.35
Indian Point 2	PWR	0.15	1.4 E-4 (rev. 4.8 E-5)	1.4 E-4	30	1	>0.30
Indian Point 3	PWR	0.15	3.1 E-6 (rev. 2.5 E-5)	2.4 E-6	1	8	>0.30
Limerick	BWR	0.15	4.0 E-6	2.0 E-7	--	1	>0.35
Millstone 3	PWR	0.17	9.4 E-5	-------	68	3	>0.30
Seabrook	PWR	0.25	2.9 E-5	-------	13	30	>0.30
Oconee 3	PWR	0.15	6.3 E-5	6.0 E-5	25	1	>0.15

Table V. Seismic Core Damage and Release Frequencies from the Decay Heat Removal Requirements Tap A-45 Plants

Plant	Type	SSE (g)	Seismic Core Damage Frequency (point estimate) Per Year	Seismic Release Frequency (point estimate) Per Year	Dominant Earthquake Range (g)	Seismic as Percent of Total Core Damage Frequency
Point Beach 1&2	PWR	0.12	6.0 E-5	2.5 E-5	0.12-0.24 0.24-0.36	49% 38%
St. Lucie 1	PWR	0.10	1.3 E-5	5.8 E-6	0.20-0.30 0.30-0.40	52% 39%
Quad Cities	PWR	0.24	8.3 E-5	-------	0.24-0.48 0.48-0.27	62% 23%
Arkansas Nuclear One 1	PWR PWR	0.20	7.3 E-5	3.7 E-5	0.20-0.40 0.40-0.60	55% 25%
Turkey	PWR	0.15	1.0 E-5	4.6 E-6	0.15-0.30 0.30-0.45	44% 39%

Prassinos found that four out of seven industry PRAs have a core damage frequency comparable to the core damage figure-of-merit of 1 E-5 per year, while three out of four PRAs yielded a seismic release frequency comparable to the 1 E-6 large release figure-of-merit. When accounting for the large uncertainty ranges, Prassinos found that these ranges bracketed the core damage and large release figures-of-merit for most plants examined in the industry studies.

Prassinos also found that the point estimate values obtained in the A-45 seismic studies are consistent with the core damage and large release figures-of-merit.

Prassinos concluded that the seismic (external) hazard has been found to be important with respect to both figures-of-merit, and that the seismic hazard should be included in the Severe Accident Policy implementation.

Budnitz and Lambert [3] determine that almost every full scope PRA that has examined earthquake-initiated events has found this category represents one of the important initiator groups, and that occasionally an earthquake initiated sequence is among the few largest contributors to core damage frequency and/or to offsite risk. Usually the sequences identified are very plant-specific in character.

The NUREG-1150 core damage frequency results for the seismic initiator for Surry and Peach Bottom are to be found in Tables 2 and 3 respectively. The conditional probability of early containment failure for seismic events is to be found in Figures 1 and 2. The NUREG-1150 results corroborate the findings of Prassinos [2] and of Budnitz and Lambert [3]. The seismic initiator is an important, if not dominant, contributor to core damage and to large releases for both Surry and Peach Bottom.

7. SOME PERSONAL COMMENTS

1. I agree with the conclusions and findings of References [1-3] with regard to the need to include external initiators in any risk estimate for a nuclear power reactor. This has been clear for a decade. What is unclear is the reason for the slow pace of the NRC Staff to accept this, and the uneven pace in industry to seek out and fix on their own initiative the more obvious, the more significant deficiencies present in specific plants.

2. Considerable attention has been given to trying to understand the differences between the estimations of seismic hazard for ten Eastern sites by the experts and methods employed by the Lawrence Livermore National Laboratory (LLNL) and the expert groups and methodology that comprised the program for the Electric Power Research Institute [13]. In view of the still large gaps in our growing knowledge of earthquakes and their causes, large uncertainties and large differences among different experts and expert groups should be expected. NUREG-1150, Second Draft, acted reasonably in displaying two sets of seismic.hazard curves and seismic risks.

3. Most current estimates of the recurrence interval for safe-shutdown earthquakes (SSEs) at reactor sites in the Eastern U.S. lie in the range 1 E-3 and 1 E-4 years. Our nuclear history is relatively brief in geological terms. We have had, say, a few thousand reactor-years of operation. We have had a substantial seismic event at the Humboldt Bay reactor. However, for such rare events three thousand reactor years is

insufficient to provide confirmation or its inverse. One should note that a single very severe earthquake in the Eastern U.S. might catch several reactors.

4. NUREG-1150, Second Draft, carries the seismic risk analysis through Level 2 but does not undertake a risk calculation for this part of the overall risk. Changed evacuation conditions due to off-site earthquake damage certainly may significantly affect the risk reduction measures usually assumed in Level 3 analysis. Also, as NUREG-1150 suggests, the NRC may wish to reevaluate how to apply its safety goal policy for an accident initiator which also carries with it large, off-site, non-nuclear casualties and costs. Of course, a similar, albeit not identical, consideration could apply for certain other external events, e.g., a sudden, catastrophic dam failure.

5. My personal intuition about the state of seismic PRA is that it has reached the position internal events had in the early 1980's. In other words, it has passed through its initial formulation and application, been subject to considerable review and been applied to many reactors. However, much was learned in the internal event arena during the past decade, both from analysis and from a range of empirical experience. I believe seismic PRA still has such a learning period to go through. Design and construction errors, aging, seismic-induced fires, sensor failure, bolt-degradation, operator confusion, these are some of the matters that come to mind when the question of completeness is raised for seismic PRA. The very large host of components, sensors, joints, tubing, etc., all of which it is impossible to treat specifically in estimating fragilities for a seismic PRA, lead one to anticipate substantial modification in current day predictions.

6. Particularly in view of the small numbers frequently being estimated for core damage frequency due to internal events, and the relatively small conditional likelihood of early containment failure, given a core melt, that is estimated for some large dry PWRs, it seems all the more relevant to examine in reasonable detail the impact that large earthquakes may have on the potential for early containment failure.

7. One possible lesson we may draw from LWR experience is that advanced LWRs and proposed new power reactors of other design would do well to incorporate evaluation of risk from external events into their design as an ongoing process from the beginning. This seems not to have been fully the case for the small liquid metal reactor (LMR), the small high-temperature gas-cooled, graphite reactor (HTGR), or for the PIUS reactor. At least my information is that seismic PRA has lagged. Thus, this leads to a degree of skepticism on my part where very small overall core damage frequencies are being predicted.

REFERENCES

1. C.Y. Kimura and R.J. Budnitz, "Evaluation of External Hazards to Nuclear Power Plants in the United States", NUREG/CR-5042, UCID-21223, December 1987.

2. P.G. Prassinos, "Evaluation of External Hazards to Nuclear Power Plants in the United States: Seismic Hazard", NUREG/CR-5042, UCID-21223, Supplement 1, April, 1988.

3. R.J. Budnitz and H.E. Lambert, "An Evaluation of the Reliability and Usefulness of External-Initiator Methodologies", Future Resources Associates, May 1989.

4. U.S.N.R.C., "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants", NUREG-1150, Second Draft for Peer Review, June 1989.

5. U.S.N.R.C., "Policy Statement on Safety Goals", *Federal Register*, Vol 51, pg. 30028. August 21, 1986.

6. V. Ho, N. Siu and G. Apostolakis, "COMPBRN III - A Fire Hazard Model for Risk Analysis", *Fire Safety Journal*, 13, 137, 1988.

7. J.A. Lambright, S.P. Nowlen, V.F. Nicolette, and M.P. Bohn, "Fire Scoping Study: Investigation of Nuclear Power Plant Fire Risk, Including Previously Unaddressed Issues", NUREG/CR-5088, 1988.

8. U.S.N.R.C., "Integrated Plant Safety Assessment, Systematic Evaluation Program, Nuclear Power Plant," NUREG-0821, 1982. See also USNRC, "Integrated Plant Safety Assessment, Systematic Evaluation Program, Haddam Neck Plant," NUREG-0826, 1983.

9. Interagency Committee, 1986. Work Group on Probable Maximum Flood Risk Assessment, under the direction of the Hydrology Subcommittee of the Interagency Advisory Committee on Water Data, "Feasibility of Assigning a Probability to the Probable Maximum Flood", 1986.

10. National Academy of Sciences, Committee on Techniques for Estimating Probabilities of Extreme Floods, Water Science and Technology Board, "Estimating Probabilities of Extreme Floods, Methods and Recommended Research", 1988.

11. Oconee PRA, Electric Power Research Institute/Nuclear Safety Analysis Center and Duke Power Company, Report NSAC-60. "Oconee PRA, A Probabilistic Risk Assessment", 1984.

12. M.W. McCann and A.C. Boissonnade, "Probabilistic Flood Hazard Assessment for the N Reactor, Hanford, Washington, Report UCRL-21069, 1988.

13. D.L. Bernreuter, J.B. Savy, and R.W. Mensing, "Seismic Hazard Characterization of the Eastern United States: Comparative Evaluation of the LLNL and EPRI Studies, NUREG/CR-4885, UCID-20696, May 1987.

IMPROVED CONTAINMENT CONCEPT FOR FUTURE PWRs

H.H. HENNIES, G. KESSLER
Kernforschungszentrum Karlsruhe GmbH

J. EIBL
Universität Karlsruhe

Karlsruhe, Federal Republic of Germany

Abstract

Improvements to PWR containment design are discussed which, at a moderate cost increase over present-day containments, would permit the deterministic exclusion of the catastrophic consequences of the most severe accidents such as core melt through, steam explosion or hydrogen detonation.

---

1. INTRODUCTION

So called "inherently safe" and small reactors have been proposed and been discussed during recent years as a "future generation" of nuclear reactors [1,2]. Their promotors claim that the risk of a core melt down can essentially be made zero for these small reactors, by applying simple inherently acting physics principles. However, neither licensing nor operational experience is available on a broad basis for such small reactors. In parallel presently existing LWR technology was also reviewed during recent years with the aim of improving and extending the already existing safety features [3,7]. Probabilistic risk studies were performed for typical LWR designs, e.g. in the US [4] and in the FRG [5]. These studies pointed to areas where the overall safety concept could be further improved. Safety R&D programs performed in the US, Europe, and Japan, during the past years resulted not only in a deeper understanding of the physics phenomena determining the accident sequences [6] but also allow to define - as will be shown in this paper - design principles having the potential not only to reduce the consequences, but to cut deterministically the further propagation of the most severe accident sequences.

In this paper we try to define extended design measures on the outer containment level for, e.g. a future PWR plant of e.g. 1300 MWe power. Our approach shall allow to exclude in a deterministic way, i.e. beyond any reasonable doubt, the catastrophic consequences of containment destructive events discussed in context with severe core accidents, e.g. core melt through, steam explosion, H_2-detonation etc. Concerning the overall safety concept, this shall provide an ultimate barrier which envelops in a protective sense the spectrum of preventive and mitigative accident management measures [3,7].

Our ultimate aim can be defined as follows:

In the very unprobable case of a core melt (failure of safety systems and failure of accident management measures) the radioactivity should remain within the reactor containment. Any release of radioactivity to the environment should be almost zero or at least be extremely small. The outer containment shall retain its integrity and tightness.

Probabilistic risk studies [4,5] confirm that the most severe accident consequences are always initiated by failure of core cooling and subsequent core melt down. We therefore discuss mainly the problem areas of:

- failure of the reactor pressure vessel at high pressure
- steam explosions within the reactor pressure vessel
- H_2 detonations following core melt down
- basemate erosion by molten core concrete interaction.

Possible leak paths through the outer containment via pipes or ventilation valves, e.g. the leak path into the compartments containing the emergency cooling systems of German PWR's or internal flooding, as analyzed in [5] are not especially discussed here, because these problems can be resolved by appropriate design.

2. FAILURE OF THE REACTOR PRESSURE VESSEL

Core melt down is assessed in the German risk study [5] with a total probability of occurence of $3\cdot 10^{-5}/a$. If additional accident management procedures are applied this probability of occurence can be lowered to $4.5\cdot 10^{-6}/a$. Failure of the reactor pressure vessel could occur:

- under low pressure, e.g. <2 MPa after depressurization of the primary system following large leaks and failure of all emergency core cooling systems (including accident management measures),
- under high pressure (16 MPa) following a failure of heat removal via the steam generators and a subsequent failure of depressurization of the primary system (including accident management measures).

2.1 Melt through of the pressure vessel under low pressure

After melt through of the pressure vessel the core melt will interact with and penetrate into the concrete of the containment basemate. The possible consequences of such a melt through and the technical design features to avoid the melt through will be discussed in section 5. H_2 generated during core melt down and during core melt/concrete interaction will be released into the containment. The problem of H_2 burning, H_2 deflagration and detonations is discussed in section 3.

If the core melt gets into contact with, e.g. the sump water, steam will be produced and the pressure will rise within the containment. However, only within about 4 days the pressure can rise up to about 0.6 MPa [5] (Fig. 1). German PWR's have existing exventing lines through which the pressure will then be decreased in order to avoid a further pressure increase and thereby not endanger the integrity of the containment. The containment atmosphere can be released through this exventing pipe and will be filtered by exventing filters [12].

2.2 Melt through of the pressure vessel under high system pressure

In the very unprobable case of a failure of heat removal via the steam generators and subsequent failure of depressurization of the primary system (including accident management)

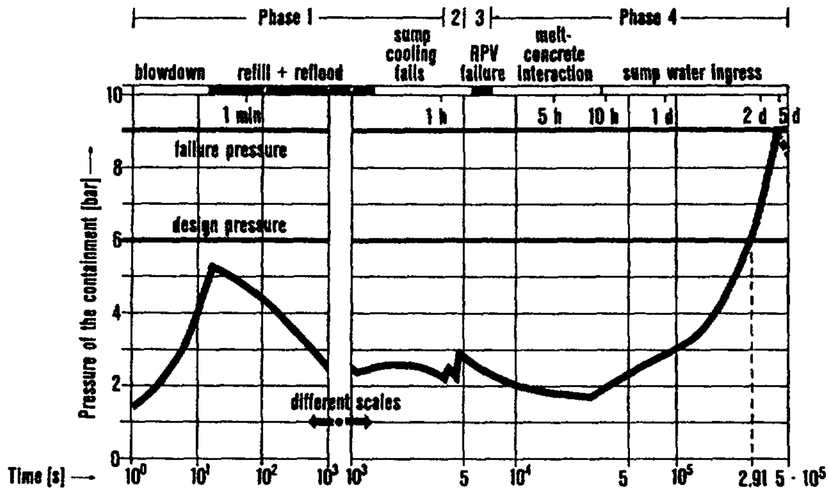


FIG. 1. Containment pressurization during core melt accident (low-pressure path).

the core melt would heat the bottom of the reactor pressure vessel which would fail then [4,5]. The probability of occurence for this accident sequence was assessed to be $5\cdot10^{-7}$/a [5, 9].

An assessment of stress and strains in the vessel support structure (of the BIBLIS-B reactor) shows that [5]

- melt through and flashing from vessel internal pressures of 2-3 MPa will not endanger the vessel support structure
- melt through and flashing from vessel internal pressures of 3-8 MPa will destroy the vessel support structure and the primary coolant piping system. The pressure vessel and support structures will move upwards, but will not endanger the outer containment's integrity or tightness.
- for internal vessel pressures between 8-16 MPa before failure and flashing the pressure vessel will move upwards and destroy the steel structures of the outer containment.

The forces acting on the reactor pressure vessel for the time span of flashing or depressurization are on the order of 60 MN.

In order to avoid an upward movement of the pressure vessel the vessel support structures must be reinforced or additional concrete structure above the reactor vessel must be provided such that the reactor pressure vessel cannot move upwards such that it would endanger the integrity of the outer containment. Our assessment shows that there appears to be no reason why this should not be technically feasible for the internal pressure range up to 16 MPa. Such a design proposal will be discussed in Section 6.

3. THE PROBLEM OF H_2-DETONATION IN THE REACTOR CONTAINMENT

Core melting and penetration of the melt downwards into the concrete of the containment basemate results in a total of 1350 kg H_2 generated mainly by chemical reaction of steam with Zircaloy. This quantity of H_2 is released into the outer containment if not parts of it burn already during melt through of the pressure vessel [5]. A detailed analysis shows that despite of the presence of steam and reaction gases (e.g. CO,

CO_2) from the melt/concrete interaction, the limits for the detonability of mixtures of H_2 with air, steam and reaction gases can be reached or even be exceeded in certain compartments of the PWR-containment, located close to the pressure vessel. But it also shows that local H_2-detonations in these lower compartments cannot destroy their heavy concrete structures or endanger the overall integrity of the outer containment [5].

There remains then the question: can large scale H_2 detonations which could endanger the tightness and integrity of the outer containment be excluded from risk and consequence analysis? The answer is not an absolute no. The reasons are that the generation of steam after contact of the core melt with sumpwater is not certain in all possible cases and H_2-air mixtures with H_2 volume fractions exceeding the detonability limits could develop after steam condensation. In such cases the occurence of deflagration to detonation transition (DDT) phenomena cannot be excluded [5,10,14].

One can resolve this remaining problem in two different ways:

a) by installing H_2-igniters (spark igniters, catalytic igniters) or catalytically acting foils to burn the H_2 already close to its generation. Both devices were developed during recent years and are ready for installation in German PWR's [11]. The installation of such ignitors or catalitically acting foils will drastically reduce the probability of occurence of large scale H_2 detonations, or even bring it to zero.

b) One can try to design a PWR containment which keeps its integrity even after a large scale H_2 detonation. This must be seen in relation to the following experimental and theoretical results for H_2-detonations:
   - Overpressure spikes measured during H_2-detonations can reach maximum pressures which are by a factor of 10-38 higher than the initial pressure. The highest overpressures ratios up to 38 were measured during tests in the FLAME facility (a large scale test facility of 1,8x2,4 m crosssection and 30 m length at SANDIA), when obstacles were positioned into the test space [10,14]
   - velocities of the detonation front up to 2 km/s were measured [10, 14].
   - The half width of these detonation overpressure spikes during the propagation of H_2-detonations is in the range of about 5 ms [10,14].
   - The initial pressure within the containment can be in the range of 0.1 to at most 0.6 MPa. At the upper boundary of this pressure range (0.6 MPa) containment venting would be initiated [11].

   Pressures in the containment of 0.2-0.6 MPa can only be attained if steam is generated which at the same time prevents the H_2-Air-steam mixture from reaching detonability limits [5].

   From the above mentioned experimental facts it can be concluded that the maximum H_2 detonation overpressure could be - as a conservative upper boundary - in the range of 0.6 MPa (initial pressure) x 38 (max. overpressure ratio) = 23 MPa with a half width of this overpressure spike of about 5 ms.

This means that a containment which can sustain a pressure pulse load of 0.12-0.2 MPa·s cannot be endangered any more by a large scale H_2-detonation. In other words: For such containments the probability of failure due to detonation is essentially zero.

A containment design which will sustain such shock pressures will be discussed in section 6.

4. STEAM EXPLOSION

Core melt down at low system pressure following large leaks in the primary system can lead to contact between large masses of the molten core with water in the lower part of the pressure vessel (below the grid plate). In this case a steam explosion could develop [4,5]. A careful assessment of experimental and theoretical investigations was made in the German Risk Study, Phase B. This leads to the conclusion that a steam explosion with a mechanical energy release beyond 1.5 GJ and a pressure peak of more than 75 MPa has a very low probability. A detailed stress analysis of the reactor pressure vessel under such shock loading shows that the pressure vessel will remain intact if a steam explosion doesn't exceed the above cited values [5]. As a consequence the outer containment is not endangered by such a steam explosion. We emphasize that we fully agree with these results.

However, discussion in the scientific literature [4,15,16,17,18] does not yet present an unanimous opinion. It seems therefore interesting to ask the question under which loads the pressure vessel would fail and what would the design measures be to prevent failure of integrity of the outer containment at all.

As an example, twice the explosion energy considered in the German Risk Study, Phase B, i.e. 3 GJ could be taken as an extremely conservative upper bound [23]. Such a release of mechanical energy would probably lead to a failure of the spherical bottom of the reactor pressure vessel. Following the assessment by Theofanous et al. [16] 3 GJ of explosion energy would then lead to the formation of a vessel internal missile that consists of parts of the (previously molten) core, the upper internal structures, and the upper support plate. These masses impact on the vessel head with an energy of about 220 MJ. Following a realistic but still conservative estimate [19] this impact would turn the whole pressure vessel and internals into a missile with about 40 MJ energy. With this energy, however, the pressure vessel could rise only less than 10 m so that a failure of the outer containment can be excluded. Only if additional unrealistically conservative assumptions are made, a smaller missile (vessel head and associated masses) with an energy of 150 MJ would result. Such a missile would endanger the integrity and tightness of the outer containment of the present PWR.

However, a design proposal is given in section 6 that could cope with even higher energies, e.g. 220 MJ and more. It should be emphasized that in the presence of such additional safety design features the steam explosion problem would become an accomodated event sequence in risk analysis.

5. BASEMATE EROSION BY MOLTEN CORE MATERIAL

After melt through of the bottom of the reactor pressure vessel, the molten core material would erode the concrete basemate of the containment. Experimental and theoretical studies on molten core concrete interaction in recent years mainly in US [20] and FRG [21] have quantified the process of basemate erosion.

The mass of core material of a 1300 MW-el PWR possibly in contact with the basemate would be some 200 t of oxide and metal, with a decay heat of 20 MW at start of the interaction and typically 10 MW after about 10 days. This considerable amount of heat plus additional chemical energy from the oxidation of the zircaloy cladding leads to substantial erosion of the basemate. As early coolability of the ex-vessel core materials cannot be generally anticipated for the presently existing plants, melt-through of the basemate must be expected to occur within a week. The consequences to be considered in case of ground water contact after melt-through are the leaching of fission products from the encrusted melt and the transport and retention of activity in the soil, generally dominated by the Sr-90 nuclide [22]. A new containment concept must resolve these issues by avoiding basemate penetration.

5.1 Control of the ex-vessel coremelt

In an accident sequence with melt-through of the reactor pressure vessel, the core material shall be controlled by a core retention device (core catcher) located in the lower part of the containment. The aim of this retention device is the safe confinement and heat removal of the core material, the prevention of structural erosion and retention of the fission products in the core debris. Therefore, it is neccessary to cool the core materials to low temperatures, so that they are solidified after a relatively short period of time.

The conceptual design (Fig. 2) relies on the principles of spreading the melt over a large area and subsequent fragmentation and cooling by direct water contact. Consequently, the decay heat is transferable to steam, which condenses at the upper steel shell of the containment and drains back to the core retention device at the lowest part in the containment. The decay heat is finally removed via the steel shell to e.g. convective air flow or to a water coolant system in the annulus. In this situation, the containment internal pressure is far from the design limits and venting is dispensable.

The core catcher (Fig. 2) has the following design principles:

- A flat perforated steel plate, which forms the final catcher shell, is connected with the basemat by a massive support structure. In case of an accident, the interfacial gap is filled by water from the primary circuit and the accumulators, while the catcher remains dry due to the drain-pipeline.
- The catcher is covered by a sacrificial layer of concrete to protect the steel from the early high temperature melt and to promote lateral spreading of the melt.
- After ablation of the concrete layer, cooling from the lower side starts by the evaporating water with the steam and possibly some water streaming through the perforated plate and leading to some melt fragmentation.

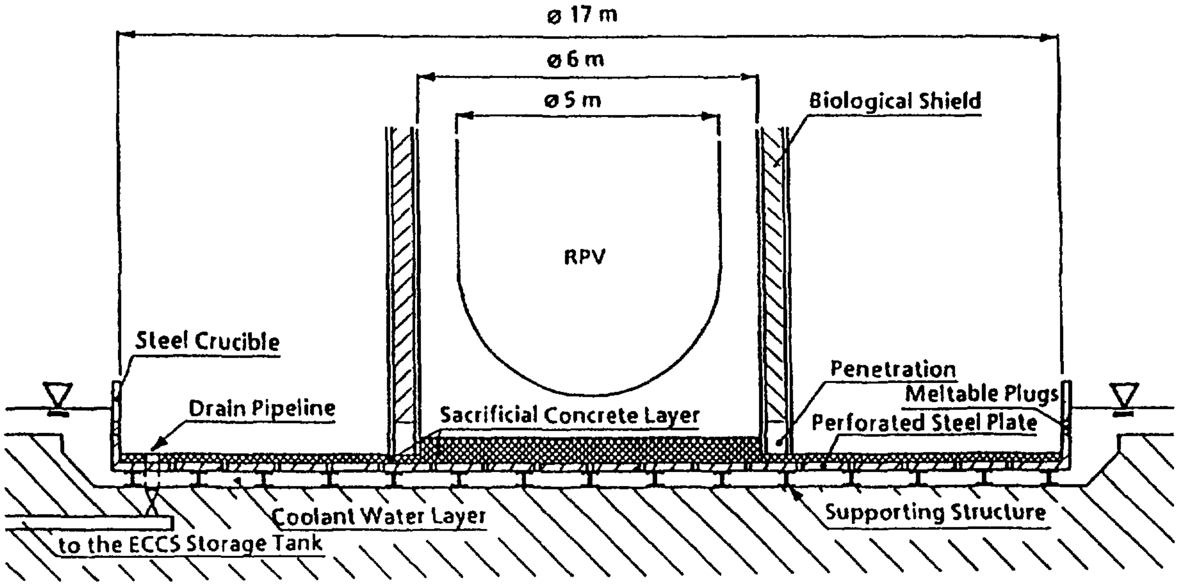


FIG. 2. Core debris cooling system.

- Later on, the upper side of the melt is flooded by water when the meltable plugs in the sidewalls of the catcher open. This leads to the final long-term stable configuration.

The diameter of the device is some 17 m, if no fragmentation of the core material is anticipated. If substantial fragmentation of the melt layer can be demonstrated in future investigations, a higher layer thickness and consequently a smaller catcher diameter can be obtained. Due to its simple design, the core catcher can be integrated into the containment without modification of present design criteria.

6. NEW OUTER CONTAINMENT DESIGN

Design principles are shown by Fig. 3 for a new outer containment by which the most severe accidents, e.g. large scale H_2-detonation, steam explosion, pressure vessel failure at high steam pressure and core melt through can be contained [24]. This containment consists of an inner steel liner (about 40 mm thick) which - when under high internal pressure - can lean against a 2 m thick prestressed outer concrete containment. This concrete containment has a staggered structure at its inner surface such that chimney type channels become available through which air can flow under natural convection to cool the outer surface of the steel liner. Water cooling at the outer surface of the steel liner is also possible. Radioactivity leaking through the steel liner could be filtered at the top of the containment before the air is released. This type of containment can withstand an inner static pressure of about 3 MPa and inner pressure pulses of more than 23 MPa peak value and 5 ms half width of the pressure spike, as it could originate from a large scale H_2-detonation (Section 3). Penetrations through the containment must be designed such that they withstand the same pressure loads.

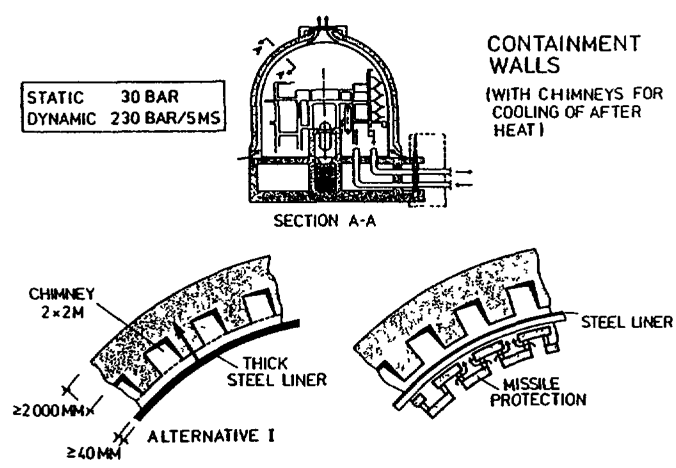


FIG. 3. Design principles of new outer containment design.

Prefabricated concrete structures could be attached to the inner surface of the steel liner serving as a shield against internal missiles. The outer containment protects the plant against air plane crash, explosive gas clouds and other possible external events.

The inner concrete structures surrounding the reactor pressure vessel are equipped with long unbonded prestressed steel cables of 15-20 m length and a total cross section of 0.5 m^2 (Fig. 4), anchored within the lower concrete building structure. They hold down a thick prestressed concrete cover consisting of a number of segments.

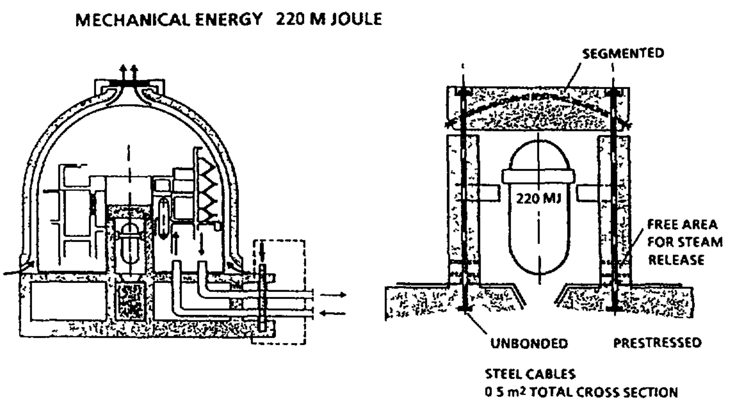


FIG 4. Design principles for concrete structures surrounding the pressure vessel.

In case of pressure vessel failure after core melt under high pressure (16 MPa) (Section 2) or in case of a steam explosion (Section 4) the upward moving pressure vessel or vessel cover (missile) will be hold down by the concrete cover structure. The energy of the upward moving missile will be transformed into strain of the long steel cables. More than 220 MJ, given as an example in Fig. 4, can be taken by the elongation of the steel cables for this up to 300 MJ acting upwards on the pressure vessel head could be accomodated [24]. Steam released from the pressure vessel can stream through openings in the concrete structure thereby avoiding static pressure build-up in the pit around the reactor pressure vessel. Design provisions to avoid the direct containment heating problem [4] must be analysed and if necessary appropriate design measures must be realised. For refueling of the reactor core the concrete cover can be lifted in different segments.

Fig. 5 shows another alternative proposal for a core melt retention device. The core melt can flow into a core catcher which is filled with a sacrificial material. Its walls are clad with ceramics to cope with high temperatures. The walls are cooled by water either in natural or forced convection.

All electrical cables and coolant pipes going out from the containment should be arranged in a few special vaults equipped with the capability to interrupt the gas or coolant flow out of the containment in case of a severe core melt accident.

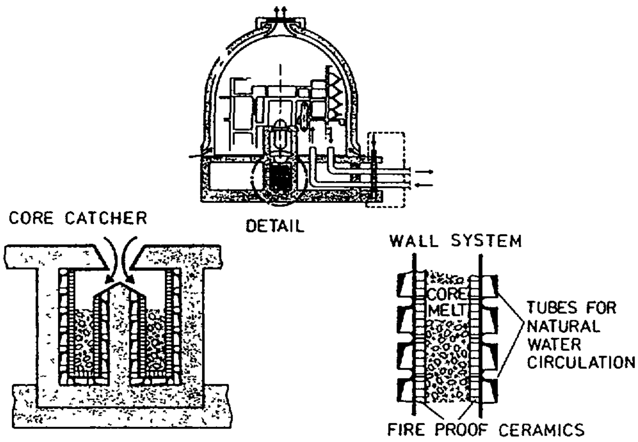


FIG. 5. Alternative core melt retention and cooling device.

7. CONCLUSIONS

Results from R&D programmes of the last few years allow now to study the question whether the consequences of the most severe accidents initiated by core melt down can be restricted to the containment of a PWR. A design proposal for a new containment concept was presented which can cope with the consequences of

- core melt through the pressure vessel bottom under low and high system pressure (including steam explosions)
- large scale H_2-detonation within the containment
- core melt through the basemate of the containment.

The main goal of the present proposal is to protect the population and the environment in the neighbourhood of the reactor plant. Consequences of the most severe accidents will be restricted to the containment itself.

The probability of a core melt accident for existing plants is extremely small and actions have been decided to minimize the consequences by corresponding accident management measures.

But for future plants it could be simpler and more efficient to install the proposed containment system. In such a case more detailed design work is needed.

The authors want to thank H. Jacobs, H. Alsmeyer, W. Tromm, B. Kuczera, R. Krieg, F.H. Schlüter for their scientific contributions and helpful discussions to this paper.

REFERENCES

[1] Hannerz, K., Towards intrinsically safe Light Water Reactors. ORNL: Institute for Energy Analysis, ORAU-IEA-83-2(M), 1983.

[2] Weinberg, A.l., et al., The second nuclear era, Praeger, New York, 1985.

[3] Mayinger, F., Birkhofer, A., Neuere Entwicklungen in der Sicherheitsforschung und Sicherheitstechnik. Atomwirtschaft, August/September 1988, p. 426.

[4] NUREG 1150, Reaktor Risk Reference Document (1987).

[5] Deutsche Risikostudie Phase B, GRS, June 1989.

[6] Hennies, H.H., Consequences of core melt down accidents in large LWR's. Int. Scientific Forum on Fueling the 21 Century. Moscow, December 1987.

[7] Mayinger, F., New developments in nuclear reactor safety philosophy and the role of large scale facilities. NURETH-4, Karlsruhe, October 1989.

[8] Ehrhardt, J., et al., Example applications of the program system UFOMOD in decision making. KfK report (to be published).

[9] Heuser, F.W., Basic aspects and results of the German Risk Study Phase B. Int. Top. Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, USA, April 1989.

[10] Marshall, B.W., Hydrogen-Air-Steam Flammability limits and combustion characteristics in the FTS. NUREG/CR-3468, SAND 84-0383, December 1986.

[11] Tiltmann, M., Rhode, J., Fabian, H., Nachrüstmaßnahmen an Sicherheitsbehältern von DWR und SWR. Reaktortagung Düsseldorf, 1989

[12] Kuczera, B., Wilhelm, J., Druckentlastungseinrichtungen für LWR-Sicherheitsbehälter, Atomwirtschaft, March 1989, p. 129-133.

[13] HCTR Analysis of the NEVADA Test Site (NTS) premixed combustion experiments. NUREG/ CR-4916, SAND87-0956 (November 1988).

[14] Sherman, M.P., et al., FLAME facility. The effects of obstacles and transverse venting on flame acceleration and transition to detonation for Hydrogen-Air mixtures at large scale. NUREG/CR-5275, SAND85-1264 (April 1989).

[15] Chu, C.C., Corradini, M.L., One-dimensional transient fluid model for fuel/coolant interaction analysis. Nucl. Science and Engineering, Vol. 101, 1989, 48-71.

[16] Theofanous, T.G., et al., An assessment of steam-explosion induced containment failure, Part I-III. Nucl. Science and Engineering, Vol. 97, 1987, 316.

[17] Berman, M., A critique of three methodologies for estimating the probability of containment failure due to steam explosion. Nucl. Science and Engineering, Vol. 96 (1987), p. 173-191

[18] Berman, H., Marschall, R.W., Corradini, M.L., Letters to the Editor, Nucl. Science and Eng., Vol. 100, 1988, p. 149

[19] Jacobs,H., Krieg, R., Discussion of steam explosion structural consequences in German Pressurized Water Reactors, Third Int. Seminar on Containment of Nuclear Reactors, Los Angeles, USA, August 10-11, 1989.

[20] Power, D.A., "Interactions of Core Debris with Concrete", Sympos. on Severe Accidents in Nuclear Power Plants, Sorrento, 21-25 March 1988, Vol. 2, 215-233

[21] Alsmeyer, H., "Melt-Concrete Interaction during Severe Light Water Reactor Accidents", Kerntechnik 53 (1988) No. 1, 30-36

[22] Bayer, A., Tromm, W., "Abschätzung der Radionuklid-verteilung und der Strahlenexposition bei Auslaugung einer erstarrten Kernmaterial-Beton-Schmelze durch Grundwasser", KfK 4512 (1989)

[23] Jacobs,H.: "Steam Explosions during LWR Melt Down Accidents", Third Int. Seminar on Containment of Nuclear Reactors, Los Angeles, USA, August 10-11, 1989.

[24] Eibl, J.: "A New Containment Design for PWR", Third Int. Seminar on Containment of Nuclear Reactors, Los Angeles, USA, August 10-11, 1989.

SAFETY ASPECTS OF THE CANDU MAN-MACHINE INTERFACE

R.A. OLMSTEAD
CANDU Operations,
Atomic Energy of Canada Limited,
Mississauga, Ontario,
Canada

Abstract

There have been significant improvements in the man/machine interface in CANDU stations over the past three decades. The continuing rapid technological developments in computers and electronics, coupled with an increasing understanding and application of human factors principles is leading to further enhancements. This paper outlines progress to date and trends for future stations.

INTRODUCTION

The man/machine interface represents an exceptional opportunity for industrial plant designers to realise significant gains through cost avoidance, operational reliability and safety. This opportunity exists because of rapid technological development in computers and electronics, coupled with significant progress in the behaviourial sciences that greatly increases our knowledge of the cognitive strengths and weaknesses of human beings. That there is progress in these fields is common knowledge in industrialized countries, consequently the improvements are likely to be recognized and appreciated by the general public, regulators, industries and politicians.

Significant event data from operating nuclear plants in many countries consistently indicates that the root cause of events leading to equipment or safety barrier impairment results from operator/maintenance human error in 40-60% of the cases. The contribution of human error to the accidents at Three Mile Island and Chernobyl further underscores the need for design features that accommodate human cognitive strengths and weaknesses.

This paper emphasizes the safety improvements achieved in the CANDU man/machine interface design. The same design features, however, provide significant <u>cost avoidance</u> in equipment, construction time and operation. The significant events attributed to human errors represents a large cost iceberg in operating power stations.

In CANDU stations, as in most complex industrial plants, the man/machine interface design has progressed through three generations.

- <u>First Generation</u> control rooms consisted entirely of fixed, discrete components (handswitches, indicator lights, strip chart, recorder, annunciator windows, etc. Human factors input was based on intuitive common sense factors which varied considerably from one designer to another.

- Second Generation control rooms incorporated video display units and keyboards in the control panels. Computer information processing and display are utilized. There is systematic application of human factors through ergonomic and anthropometric standards and cookbooks. The human factors are applied mainly to the physical layout of the control panels and the physical manipulation performed by the operators.

- Third Generation control rooms exploit the dramatic performance/cost improvements in computer, electronic display and communication technologies of the 1980s. Further applications of human factors address the cognitive aspects of operator performance.

At AECL, second generation control rooms were installed on CANDU stations designed in the mid 70s and early 80s. Third generation features will be incorporated in the CANDU 3 station design and future CANDU stations.

A. SECOND GENERATION MAN/MACHINE INTERFACES

The control centre in the four operating CANDU 6, single unit stations represent a typical second generation man/machine interface (See Figure 1). Some of the features are described below:

The Dark Panel Concept

Human factors research and experience in the aircraft industry has made this concept standard practice in the cockpit. In the CANDU 6 control room, a light always signals a situation that requires operator action- an annunciator, handswitch discrepancy, a computer program that has failed, etc.

The Fifteen Minute Rule

There is sufficient automation to ensure that no operator action is required in the first fifteen minutes of the worst case dual event, analyzed as part of the safety system analysis for the plant. Consequently, CANDU operators have, as a minimum, fifteen minutes to perform diagnostics and planning before taking direct action but for single event cases at least 10 hours is available.

Automation

The use of computers in process and safety systems has, in many cases, freed the operator from tedious, distracting, stressful tasks to allow him to concentrate on more strategic matters. For example, the boiler feedwater transient after a reactor trip requires no operator attention. Automatic warm-up and cool down of the primary and secondary process systems is another example.

Human Engineered Testing

In the later second generation units, some periodic testing has been automated to reduce human errors that are often associated with tedious, boring, repetitive tasks. When manual tests are required, the design ensures that the tests are "non-intrusive". This ensures that maintenance staff do not modify or contact the internals of the plant equipment to carry out the tests.

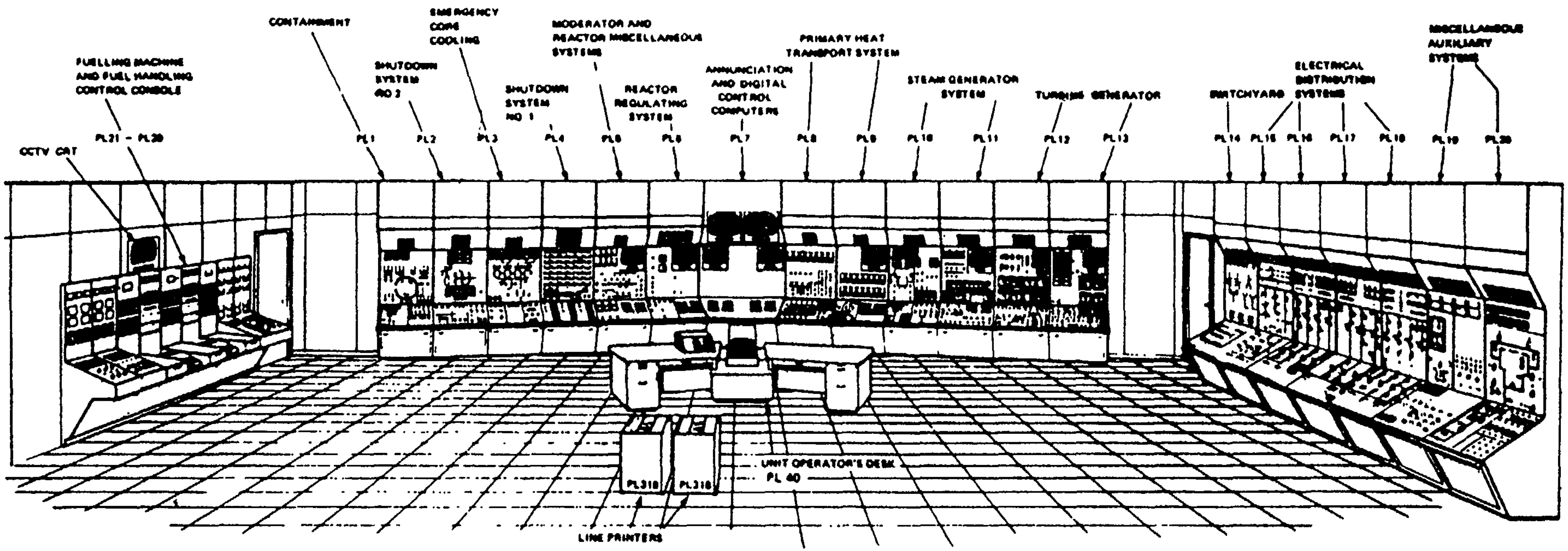


FIG. 1. CANDU 6 control centre.

Reduced Panel Congestion

This was accomplished in three ways:

1. Reducing the number of annunciator windows by limiting their use to major alarms and group alarms.

2. Use of CRTs to present displays that integrate information from different systems and equipment.

3. Automation of tasks previously accomplished by operator manipulation of control panel devices.

Good Anthropometrics

Making reference to the appropriate design "cook books", the size, shape, slope, illumination level, and many other parameters of the physical interface were optimized to accommodate the physical characteristics of the operator.

Good Control Panel Layout

The design incorporates logical grouping and clear delineation of panel switches and indicators. Panel mimics are utilized with hand switches located to represent the location and status of the controlled device as it relates to the mimic. The design incorporates standard shapes, position codes, colour codes, and a systemic and consistently applied method for labelling panel components. The alarm annunciation system classifies, sorts and allows conditional suppression of unnecessary alarm messages is incorporated.

B. THIRD GENERATION MAN/MACHINE INTERFACES

Future CANDU stations will include a third generation man/machine interface. The principles underlying many of the design requirements are based on theories established by the discipline of Cognitive Science that seeks to integrate engineering and psychology to describe the behaviour of humans as components in an information processing system. In particular, the work of Rasmussen(1), Weiner(2) and Woods(3) has had a significant impact.

The superordinate goals for the design of CANDU third generation controls rooms are the following:

1. Cost Reduction

   Reduce cost, avoid schedule risk and increase plant capacity factor.

2. Operational Design Objectives

   Change the design process so that high level operational objectives drive the detailed design of the cognitive and physical man/machine interface.

3. Elevate the Role of the Operator

   Apply additional automation selectively in order to remove tedious, distracting activities and provide the operator with tools to function on the level of a situation manager who plans, organizes activities and solves problems.

4. Context Sensitive Information

   Package and present information, to suit the context of a particular situation, so that the operator can quickly absorb the relevant data.

5. Keep the Operator in Touch with the Plant

   Provide information and activity that will keep the operator alert and in touch with the plant.

6. Flexible Control Room

   Provide the operating utility with a control room that uses a minimum number of standardized components in a flexible interface that can be tailored to suit a different operating philosophies and methodologies.

The Nature of Man

For the third generation man/machine interface, the designer must be aware of certain unique characteristics of men that set them apart from machines. Figures 2 and 3, for example, list some intuitively derived strengths and weaknesses of men and machines in performing plant control functions.

MAN

\+ CREATIVE

\+ USE OF JUDGEMENT, EXPERIENCE, HEURISTICS

\+ MAKES DECISIONS OUT OF INCOMPLETE DATA

\+ CAN SYNTHESIZE SUPERORDINATE OBJECTIVES

\- FORGETS

\- GETS OVERLOADED

\- TUNNEL VISION

\- SUBJECT TO FATIGUE AND EMOTIONAL INTERFERENCE

\- LOGIC AND REASONING FAULTS OCCUR

FIG. 2. Strengths and weaknesses of men in performing plant control functions.

MACHINE

+ REPEATABLE RESULTS
+ PREDICTABLE CAPACITY
+ NOT SUBJECT TO FATIGUE OR EMOTION
+ CAN SIMULATE LEARNING AND JUDGEMENT
+ CAN PERFORM COMPLEX COMPUTATION AND LOGIC

- NEEDS COMPLETE SET OF INPUTS TO FUNCTION
- LIMITED ABILITY TO LEARN
- SUBJECT TO DESIGN ERROR
- REQUIRES MAINTENANCE
- SOMETIMES FAILS CATASTROPHICALLY

FIG. 3. Strengths and weaknesses of machines in performing plant control functions.

Exploiting Human Creativity

Some of the features of the third generation control room are designed to facilitate man's unique ability to synthesize volumes of information and make good decisions, even when the data is incomplete or inconsistent. This is the key to ensuring an adequate response to the unanticipated or obscure cause events that are a fact of life in complex industrial facilities.

A Fresh Perspective

Regardless of the quality of the man/machine interface design, the public perceives human variability to be such that any task given to man has a relatively high probability of being performed in error. This perception tends to suggest that there are higher probability failure modes than those identified in the random equipment failures covered in the probabilistic safety analyses.

The familiar concepts of redundancy and diversity will be applied so that a second human is available to confirm the safety critical actions of the operator. The most difficult requirement is to ensure that the redundant human is also sufficiently "diverse". This means his knowledge, training and recent activities should be sufficiently different to ensure that he does not make the same cognitive error as the first man and become part of a common mode human error. In CANDU stations, separation of perspective is achieved through the roles and activities assigned to the shift supervisor and the first operator respectively.

Rationalizing Conflicting Objectives

The Chernobyl and the Three Mile Island incidents were partly the result of conflicting operational objectives. Procedures in these plants did not adequately resolve the potential for inappropriate action. For example, at Three Mile Island, the objective to cool the fuel conflicted with the objective to maintain two phases in the pressurizer. For the third generation MMI, man/machine interface detailed procedures and the detailed interface design will be systematically derived from a complete set of high level operational objectives. If implicit objectives are present, they must be made procedurally explicit.

The Information Interface

Figure 4 illustrates the concept that the plant operator performs both procedural and strategic/judgemental functions. Note that the "human" interfaces with the plant mainly through information while the direct manipulative interface, by comparison, is trivial. The interface is not man to machine but to information about a machine. (See Reference 6)

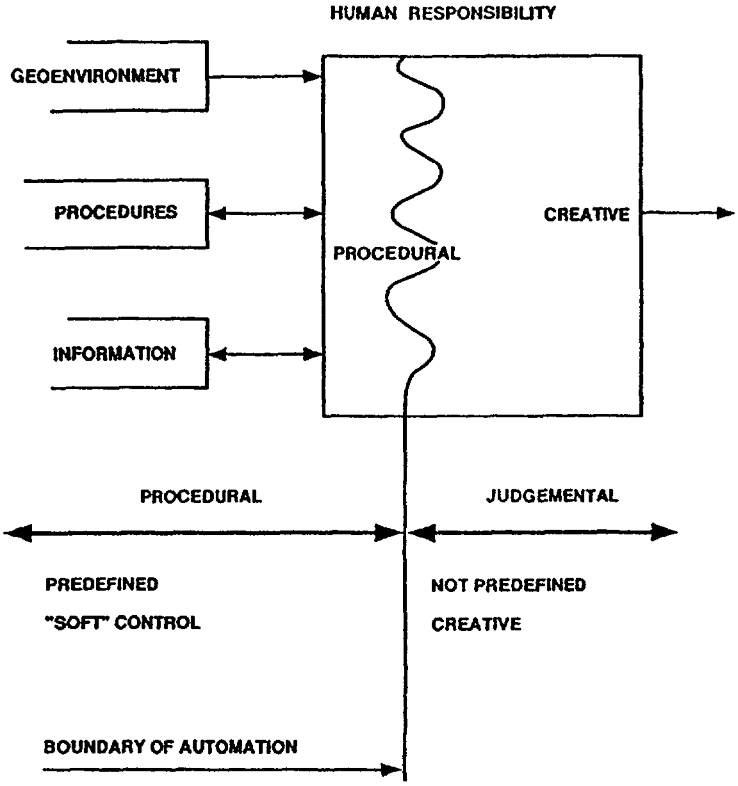


FIG. 4. The automation boundary is in the human.

Information will be available to the operator in the context of his specific objectives in a particular situation. This means that, instead of organizing information in association with systems, areas of the plant or equipment, the operator will have access to information and control facilities focussed on functions such as maintenance of fluid or energy balance, achievement of poison override or execution of an emergency operating procedures.

Automation

For third generation control rooms, automation will seek to transfer the low level, distracting and stressful procedural tasks from the man to the machine. Both manipulative and cognitive tasks of this type will be automated. For example, the normal equipment sequencing required to valve in the shutdown cooling system will be performed by the machine. This will allow the man more freedom to perform at the level of a planner or situation manager. When complex manual sequences are automated, a few manual operations will be retained in order to keep the operator aware of and involved with the process.

Flexibility

In the past, the control room design left the operating station staff with insufficient scope to apply their experience to determine the form of information presentation or to define operating methodologies. Third generation control rooms will utilize standard keyboard/CRT based operating consoles for interaction and banks of CRTs for information displays. The utility will have more capability to influence operational procedures and make changes over the life of the plant.

Changing the Design Process

For the advanced CANDU control room, the design process is a significant departure from previous practice. The traditional approach was to break the information interface down by plant system or equipment. Each system designer then specified the alarms, displays and control interactions they believed were adequate in that narrow context. The station technical unit was then given the job of creating operating and emergency procedures based on the design as given. In the new approach, after the basic plant operational requirements are established, draft procedures will be produced. Then, a mixed team of designers and operating staff will define an information/interface system design that will be based on the real objectives, tasks and activities of the operators.

Context Sensitive Information

The traditional large area of panels containing complex configurations of handswitches, recorders, meters and indicator lights will be eliminated. The control room will be a compact module containing a few sit-down computer consoles that will provide information to the operator that has been processed to reflect the context of his specific objectives and tasks in each particular situation. Figure 5 illustrates these features. The detailed operating procedures are written at the beginning of the design and form the basis for the information system design.

"Blackboard Displays"

The control room environment will be dominated by several large dynamic colour graphic mural mimics. One will depict the major equipment and system status of the entire plant. Another will provide an easily interpretable picture of critical plant parameters and how they are changing or interacting. These displays are the "blackboards" upon which information is presented to everyone in the control centre without censoring because of limitations in the size of regular CRTs. Current plant status at the most detailed level will be available on both the "blackboards" and console CRTs. Traditional annunciation windows will be replaced by indications on the blackboards and pattern displays on the CRTs. Figure 5 illustrates these features.

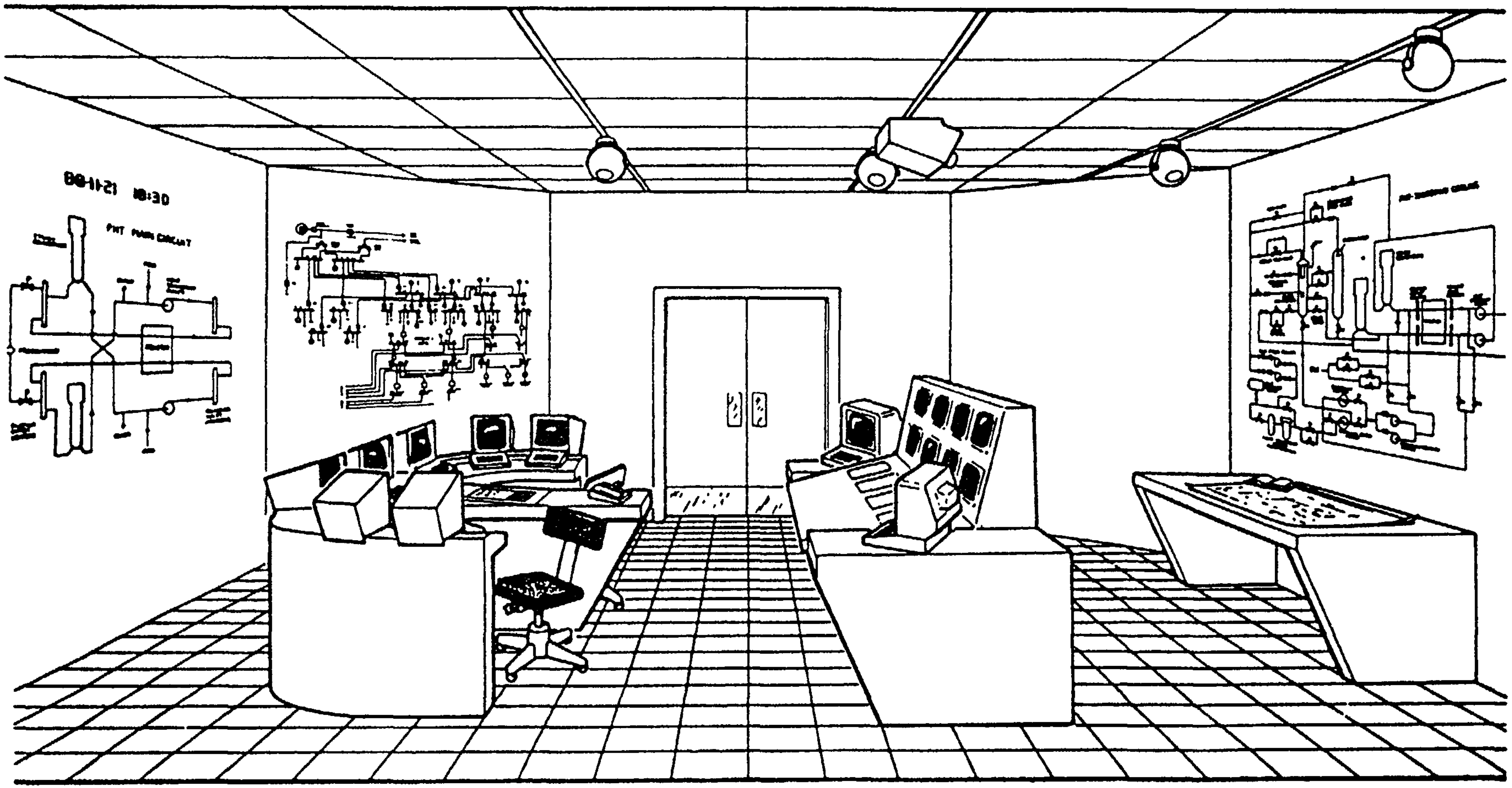


FIG. 5. Advanced control centre.

Computer Assisted Procedures

Computer assisted procedures will minimize the need for paper procedure books. The operators will use CRT screens that present integrated text, graphics and check lists, possibly supported by a computer synthesized voice. The displays will guide them in a systematic and rapid execution of the procedure. A particularly valuable aspect of the procedure presentation is an Event Confirmation Field which, at each stage of an event specific procedure, indicates to the operator if plant conditions are confirming the correct event diagnosis. Some of the procedures will be "context sensitive" in that the computer will edit and simplify them based on its knowledge of the actual state of the plant (e.g. it will not display an instruction to turn on a pump that is already on).

Decision Support Facility

In advanced, third generation control rooms a knowledge based decision support system utilizing several online expert systems will provide the operator with information and, when appropriate, a "what if" query facility to help him anticipate and plan for future action. Associated with this facility are knowledge based event diagnostics that will help locate root cause events. The output is in the form of recommendations with the rationale for each recommendation provided on request.

Already available is a system to inform the operator which channel to fuel next and another to indicate the exact channel containing a defective fuel bundle.

Pattern Recognition

Cognitive science recognized that humans are particularly effective in learning to associate significant meaning from shapes and patterns. Control room displays will seek to exploit this factor by presenting alarm configurations and plan parameter deviations in the form of interpretable patterns.

Critical Safety Parameters

Critical safety parameters, a short list of "vital signs" relating to the public safety defence barriers, will be prominently displayed in graphical pattern form permanently on a dedicated CRT screen or blackboard displays.

Voice Annunciation

Voice annunciation will be utilized in a few selected situations where redirecting the operators' attention is imperative. For example, voice will be used to announce that the entry conditions for an Emergency Operating Procedure have been realized.

Equipment Configuration and Status Display

Plant Equipment Status Schematics on the control room CRT will be operated directly from the plant Computer Aided Design and Drafting data base. The state of devices such as locally operated valves will be semi-automatically updated on the CRT displays from bar code readers connected into the data highways by the plant operating personnel.

Operation Information System

The basis for an Operation Information System will be provided. This capability will electronically integrate and automate many of the tedious, labour intensive activities associated with operating a nuclear station. For example, maintenance records, work control, man-rem statistics, equipment status, event logging and reporting and work scheduling. The result will be a significant reduction in operating costs and operator stress levels and perhaps operations staff. This facility will be developed by the operating utility associated with the plant.

Computer Annunciation Alarm Overload

With approximately 6000 measured and calculated variables for a single nuclear unit, there are operational circumstances when so many alarms can arrive that an overload situation develops. Such alarm overloads can impose severe demands upon the operator and have significant implications in terms of training, the structure of procedures and safety.

To some extent, the problem is a consequence of the availability of better instruments and tools to handle direct and derived data. Computerized techniques have contributed to the problem; they will also be part of the solutions. It is easy to present a very large volume of alarm data spanning many different fault scenarios with various degrees of importance and credibility. The challenge is to package the messages that are relevant in a particular situation and time and to articulate the alarm information in such a way that it directs the operator's attention to the remedial task at hand. Notice that we are not proposing to suppress information but rather to package and prioritize it in ways that make sense in a particular situation.

Recognition of the above problems has stimulated development of solutions. These include the following:

- The use of a high level, easy to use, programming language so that the station staff will be able to introduce the results of real operating experience.

- Improved alarm categorization strategies, including:

  (a) Plant state (e.g. reactor shutdown or at power, heat transport system pressurized hot or pressurized cold, class IV power available or not).

  (b) Action Time (e.g. Operator action within one hour, maintenance action within 8 hours, longer term maintenance action.

  (c) Response Category (i.e. plant diagnostic message, equipment status message, maintenance message, software and hardware error messages).

- Increased use of interpretable shapes and patterns for presentation of alarms and deviation displays.

- Nuisance alarm suppression.

- Selected voice annunciation.

Standardization

Although there may be several design and architect engineers performing the detailed design, the layout, architecture, ergonomics and control philosophies of the entire control room will be universally consistent.

Access to Control Room Data

Because all plant data is available on high speed data highway; simple interfacing will provide controlled access to all control room information for use in the plant management computer system or on terminals on or off the site.

Cost

The elimination of fixed panels, utilization of standard operator consoles, the application of computers to operational configuration control and the reduction in trunk cabling will yield significant cost benefits.

CONCLUSION

Third generation CANDU control room brings together the principles of cognitive science, new technology and lessons learned by CANDU operators. In this control room, the operator will work with tools that were crafted to serve his objectives and work on his tasks. Most important, he will function on a level that exploits his unique ability to innovate and form strategies to deal with unanticipated obscure cause events.

This design approach should result in improved operator reliability while, at the same time, reducing costs.

REFERENCES

1. RASMUSSEN, J. "Information Processing and Human-machine Interaction- An Approach to Cognitive Engineering". Elsivier Science Publishers, New York, 1986.

2. WIENER, E., "Fallible Humans and Vulnerable Systems : Lessons Learned from Aviation" NATO ASI Series, Vol. F322.

3. ROTH, E.M., WOODS,D.D., "Aiding Human Performance. I: Cognitive Analysis". Le Travail humain, tone 51 No. 1/1988.

4. HURST, R & L (Editors). " Pilot Error - the Human Factors". Jason Aronson, New York, 1982.

5. WAGNER, E.L., NAGEL, D.C. (Editors) "Human Factors in Aviation". Academic Press Incorporated, 1988.

6. LIPSETT, J.J., OLMSTEAD, R.A., STEVENS, J.E.S. "Balancing the Roles of Humans and Machines in Power Plant Control". AECL-9959, Atomic Energy of Canada Limited, Chalk River, Ontario, 1989.

7. SWATON, E., NEBOYAN, V., LEDERMAN, L., Human Factors in the Operations of Nuclear Power Plants by Nuclear Power and Safety. Date Unknown.

8. SHERIDAN, T.B., VAMOS, T. AIDA, S. "Adapting Automation to Man, Culture and Society", Automacia, Vol. 19, #6, pp 605- 612, 1983.

9. ADAMS, J.A. Issues in Human Reliability. Human Factors, 1982, 24(1), 1-10.

10. DUNN, J.T., FINLAY, R.B., OLMSTEAD, R.A., Advanced CANDU Reactors, AECL-9817, Atomic Energy of Canada Limited, Chalk River, Ontario, December 1988.

11. OLMSTEAD, R.A., FENTON , E.F., "The Advanced CANDU Single Unit Control Room", Atomic Energy of Canada Limited and E.F. Fenton, Ontario Hydro. Presented at the Conference on Advances in Nuclear Technology, Madrid, Spain, April 1989.

12. WOODS, D.D., ROTH, E.M., Aiding Human Performance II: From Cognitive Analysis to Support Systems, Le Travail humain, tone 51, #2/1988

13. WIENER, E., "Cockpit Automation: In Need of a Philosophy" Presented at the Aerospace Technology Conference & Exposition, Long Beach, Calif. October 14-17, 1985.

ENHANCED SAFETY DISTRICT HEATING REACTOR UNIT

F.M. MITENKOV, O.B. SAMOILOV
Experimental Machine Building Design Bureau,
Gorki, Union of Soviet Socialist Republics

Abstract

The main physical and technical features of the reactor units for nuclear district heating plants (NDHP) (space heating and hot water supply) are described.

To ensure the NDHP safety, engineering decisions based on the inherent properties of the reactor self-protection and passive safety systems were required. It is shown that AST reactors for the plants under construction in the USSR meet the demands of enhanced safety concept. Radiological consequences of severe accidents near residential area (5 km, min. away from plant) are limited by the known fluctuation range of radioactivity background on the Earth (less than 10 mSv per accident).

Introduction

Use of nuclear energy for heat supply is one of the most effective means of saving of oil and gas with simultaneous improvement of ecological conditions due to absence of combustion products' release into the environment.

Cost effective heat supply requires the low-potential heat generating plants to be located nearby the city boundaries. Thus, more stringent safety requirements are imposed on NDHPs.

Therefore, prior to the plant design the additional safety requirements for nuclear power sources of such type were developed as supplement to the main national safety Code . The radionuclides' release during the most severe accident should not exceed 1000 Ci for I-131 and 100 Ci for Cs-137.

AST reactors were developed with account of location peculiarities and necessity for assuring qualitatively higher safety level compared with NPPs. Priority was given to engineering decisions assuring reactor plant inherent safety by natural processes and use of passive safety systems. Such approach enabled the development of a plant of enhanced safety. Core damage probability in severe accidents with coincidents of a large number of failures and errors does not exceed 10^{-7} I/reactor year.

Nuclear-Engineering Peculiarities Assuring Reactor Plant Safety

For AST-500 reactor plant is accepted a pressurized water reactor (PWR) of vessel-type with inherent positive properties the main of which being power self-regulation due to negative temperature, power and steam coefficients of reactivity.

Unlike NPPs an essential advantage of AST is considerably lower thermal power of reactor unit (up to 500 MW), lack of fast transients associated with consumer's demands.

The principle feature of AST-500 reactor plant is the use of coolant natural circulation in all regimes what ensures the independence of circulation circuit, absence of coolant flow stimulators and enables to eliminate complicated fast transients typical for reactors with coolant forced circulation.

A feature of coolant natural circulation is the coolant flow increase in the reactor with power that is of paramount inportance in emergencies. This also refers to the possibility to withstand due to flow self-profiling considerable local power increases in fuel assemblies.

In the AST-500 reactor plant in contrast to existing power reactors integral arrangement of primary circuit equipment is used where core, HXs, and pressurizer are closely located in a common reactor vessel what enabled to realize a simple circulation circuit scheme and eliminate large diameter pipings which are potentially dangerous from viewpoint of their rupture. Low power density, pressure and temperatures required for a reactor producing heat for residential areas, allows more time to remain without cooling compared with other reactors.

Height of water layer above the core ensures more than 12 hrs before fuel assemblies become uncovered.

A considerable water inventory in the reactor (per unit power) ensures at integral layout the possibility of large accumulation of heat and determines great inertia of accidental processes associated with RHR loss.

Due to heat accumulation in primary and secondary circuits the time for attaining limiting pressure amounts to 2 hrs. Such margin of time in the AST-500 reactor plant gives practically the possibility to dispense with any automatic actions for actuation of heat removal systems.

A principally new solution for the AST-500 reactor plant is the use of guard vessel around the reactor. The main function of the guard vessel is toeliminate core fuel elements' uncovering at reactor vessel depressurization. At the same time the guard vessel comprises a system confining the radioactive fission products in a small volume on the immediate vicinity of the reactor.

System of emergency heat removal from the reactor to the ultimate heat sink (atmosphere) functions owing to coolant natural circulation in all the circuits without use of external power sources and water evaporation from special tanks during several days, one channel out of three being sufficient for lowering pressure in the reactor.

Safety Concept

From the onset designing of the AST reactor has been directed towards provision of enhanced safety by way of step-by-step introduction of the inherent self-protection features and passive systems, since the very features provide reactor stability against the personnel errors and equipment failures.

Reactor self-shutdown takes place at a power rise. Therefore, rapid power rise in reactors of the AST type is eliminated. What is more, there is not any physical ground for the explosion type processes. The power is under self-control, power self-limitation and self-regulation are effected as well.

Contrary to all current power reactors, the AST reactor does not have circulation pumps, and the coolant circulates through the core due to natural convection. Water heated in the core ascends to the upper reactor section, where it enters the primary/secondary circuits heat exchanger (HX) and after cooling it descends to the core inlet. Continuous and independent of any external power sources natural coolant circulation provides reliable heat removal from the core and its cooling down under accident conditions.

For the PWR reactor, the accident with loss of integrity of the primary circuit is considered to be the most severe which can result in core uncovering, fuel elements' overheating and radioactivity release. In the AST such accident is eliminated.

Reactor vessel (RV) arrangement inside the guard vessel (GV) is a unique feature of this reactor, so that even in case of the RV loss of integrity the core remains under water, that completely excluding its meltdown.

Thus, the most severe accident, i.e. reactor vessel loss of integrity, is presented by the aid of the inherent features of the selected reactor arrangement that is one pressure vessel inside the other. This solution is unique in the LWR technology.

Residual heat removal (RHR) from the shutdown reactor under accident conditions, e.g. during station blackout, is an important objective of safety provision.

RHR from the reactor is effected through natural processes without energy consumption. Thus, the principle of inherent self-protection is adopted with respect to the reactor RHR.

The integral layout of equipment, low power density and parameters provide reactor inherent self-protection feature that is self-cooling of the core.

The principle concept of self-protection is an effective means of protection against personnel errors.

Power self-regulation and self-limitation, coolant self-circulation and self-cooling - all these features are easily verifiable and allow the reactor to come out of the difficult situation all by itself. Reactor without any consequences can remain without heat removal for several hours and for tens of hours without power supply. Low power density, heat accumulating capacity, coolant natural circulation provide reactor inertia - "sluggishness". Emergency transients' duration takes tens of minutes and hours, but not seconds as in the case of LWR. This additional safety feature provides ample time to take remedial actions.

Thus, it can be stated, that at the AST enhanced safety PWR is adopted, in which through the new design solutions positive features of the inherent self-protection has been developed against all types of accidents (reactivity, loss of heat removal loss of coolant accidents). On the one hand, this reactor is a direct successor of PWRs used at nuclear power stations the number of which is predominant and the world operating experience of which, as of the end of 1988, amounts to 4000 reactor-year, on the other hand - it is a unique integral reactor with the coolant natural circulation and robust secondary vessel.

Safety Analysis

As shown, reactor safety is achieved through the design quality, high quality equipment, assembly and construction, qualified operation, inspection and diagnostics. This level of safety provides prevention of accidents.

But the second safety level plays still greater role. Here, despite the most rigid quality requirements it is assumed, that "everything is possible".

A wide range of accident scenarios has been taken into consideration involving loss of heat removal , reactivity variation processes, loss of integrity of the primary circuit systems (Figs 1-6).

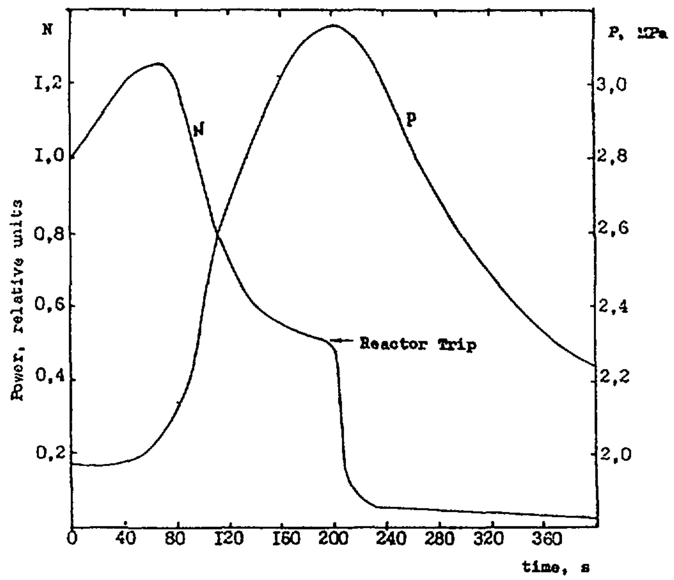


FIG. 1. 6 CPS CMs' removal at nominal power operation and 3 minutes trip delay.

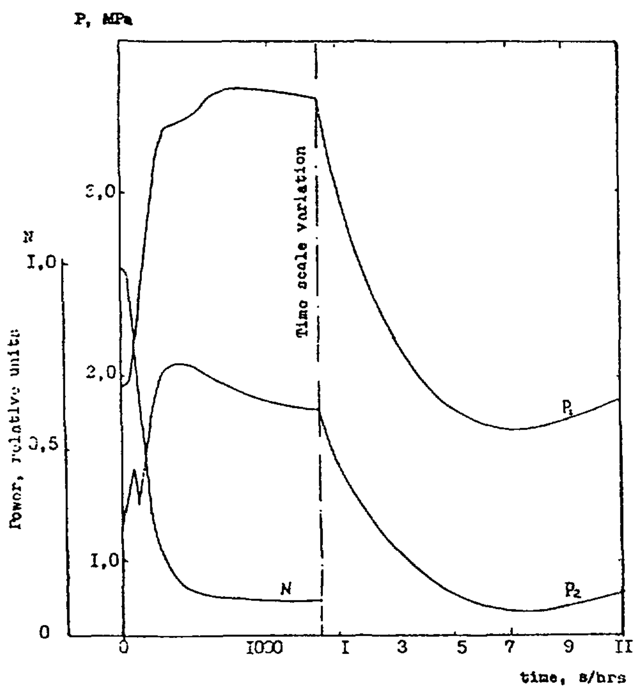


FIG. 2. 'Stop grid' accident without scram.

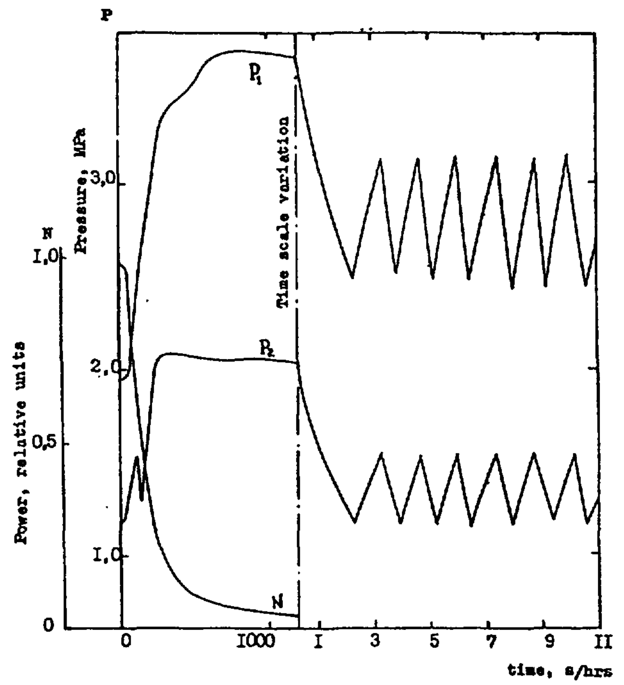


FIG. 3. 'Stop grid' accident without scram and ERHRS non-actuation. Heat removal through PORD actuated by direct action of pressure in secondary circuit.

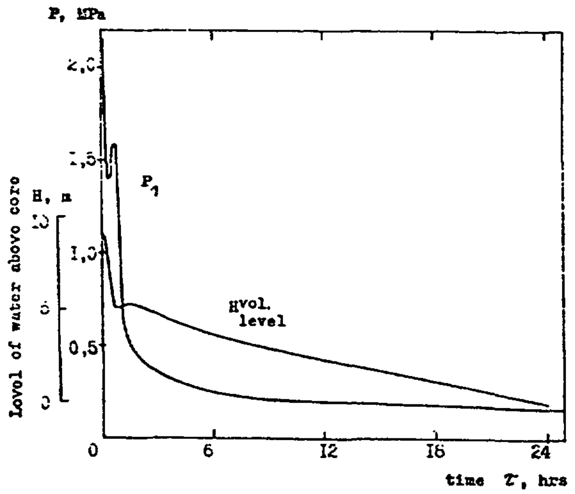


FIG. 4. Cleanup system pipeline rupture beyond guard vessel boundary with complete failure of isolation valves and of two ERHRS channels.

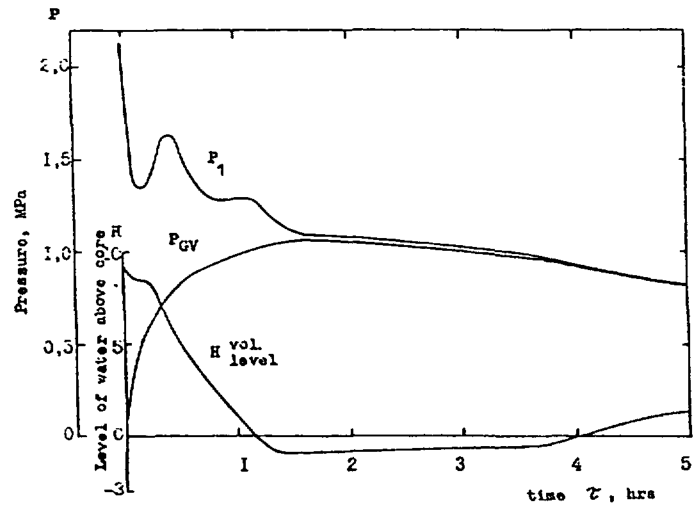


FIG. 5. Loss-of-integrity (ND 45) of reactor vessel in its lower part with two ERHRS channels failure.

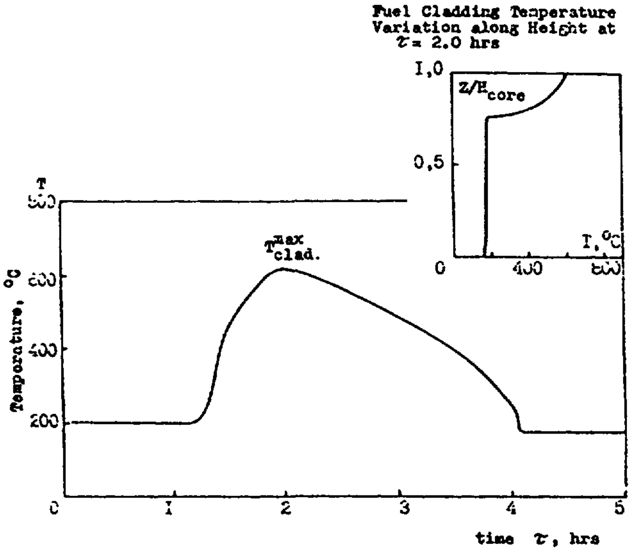


FIG. 6. Loss-of-integrity of reactor vessel in its lower part (ND 45) with two ERHRS channels failure.

The design accidents have been analysed using the principle of single failure (initial event plus a single failure in safety systems). Radiological consequences of all design accidents' combination do not exceed 0,01 mSv.

A second type of accidents has been pointed out, that is beyond design basis accidents involving superposition of several failures (initial event plus 2-3 failures in safety systems or errors). The worst consequences of beyond design basis accidents are estimated by radiation impact of 0,02 mSv that is considerably less than radioactivity background value.

Taking "protection in depth" principle as a guide the most severe hypothetic accidents with safety systems' failure were investigated. The measures against dangerous accidents' development and necessary actions for accidents' consequences localization were considered. As a result of hypothetic accidents' run investigations and measures for their control including safety--protection systems, ample time reserve for operators intervention, possibility for personnel to visit the local posts, etc. was shown that radiological consequences of severe accidents with superposition of many unlikely failures of elements or safety systems' failures and errors are limited in the NDHP by radiation bachground range, i.e. do not exceed 10 mSv at the city boundary.

Quantitative Estimation of DHP Safety Level

According to the concept of admissible risk formed in nuclear energy the total probability of core damage accident and radioactivity release beyond the reactor unit should account for 10^{-6} - 10^{-7} per reactor-year.

The estimation of safety assessments probability were made for AST-500. Probability accident analysis is done using the methodology presented in the well-known report WASH-1400. Safety systems' reliability was determined, wide spectrum of accidents and their scenarios ("event trees") was considered. The independent failures, common-cause failures and personnel errors were taken into account.

The accidents with inadvertent insertion of positive reactivity, loss of heat removal from the reactor and primary circuit loss of integrity were considered.

The total probability of accident with severe consequences (core damage) does not exceed 10^{-7} per reactor-year.

It is evident, that radioactivity release probability above admissible level and corresponding risk value will be considerably lower than the given value.

Conclusion

Safety concept adopted for AST reactor including such engineering decisions as primary coolant natural circulation, emergency heat removal systems based on passive principle, use of guard vessel, integral PWR, lowering parameters and power density of the core determine core inherent safety and self-protectiveness at the reactor relating it to the category of improved safety systems.

The analysis of numerous beyond design and hypothetical accidents with postulating of highly reliable safety systems' failures enabled to ascertain that with account of plant physical and engineering features, time sufficient for remote doubling of automatic actions for putting the safety systems into operation, using protection systems, fuel melting is not realized technically and radiological consequences of the most severe accident with fuel element damage are limited and does not exceed 10 mSv per accident.

According to AST-500 principles and with account of first AST construction experience one can develop a power set of safe and reliable reactor plants for application in different district heating systems.

APPENDIX

PRINCIPLES IMPORTANT FOR SAFETY PROVISIONS IMPLEMENTED IN THE AST REACTOR PLANT

1. Gravity laws, convection, evaporation, condensation
   a) for chain reaction interruption (scram system operation by gravity);
   b) for emergency heat removal (coolant natural circulation in all the circuits up to the ultimate heat sink).
2. Low power density - slow emergency transients' development, ample time for remedial actions and errors' correction.
3. Heat accumulation - circuits' water heating up without pressure excess allows not to take any urgent measures for RHR during more than 2 or 3 hours.
4. Reactor Vessel radiation embrittlement id excluded.
5. Primary circuit simplicity - confidence in process understanding and validity insight ("wisdom of simplicity").
6. Negative reactivity coefficients (power, steam. temperature coefficients) - power self-restriction in course of reactivity accident.
7. Integral layout - provides the inherent safety conditions, conserves the geometry and excludes the primary circuit branching out.
8. Shutdown and heat removal systems' variety.
9. Primary coolant natural circulation in the whole range - reliable heat removal in all regimes.
10. Low working pressure - reduces the potential energy of coolant.
11. Low power density oi fuel elements greatly improves the fuel elements' retaining capability.
12. Core is under water during all loss-of-coolant accident conditions (reactor vessel and pipelines' loss of integrity).

13. Passive localization system - the second strong vessel, additional safety barrier, includes RP.

14. Containment - encloses all the systems important for safety, provides protection against external impacts (air crash).

15. Emergency blackout conditions are sustained during some days without personnel intervention.

16. Three circuit heat transfer scheme at reduced heating medium pressure ($P_1 > P_2 < P_3$) excludes any possibility of radioactivity ingress into the heating grid.

17. Primary circuit leaktightness - eliminates steam-gas radionuclides' release.

18. Radiological consequences of any severe accident are limited by background fluctuation level.

REACTOR PLANT CHARACTERISTICS

Main Parameters	AST-200	AST-500
Thermal power, MW	200	500
Number of loops	2	3
<u>Primary Circuit</u>		
Coolant temperature, °C outlet/inlet	206/135	208/131
Pressure, MPa	2.0	2.0
Coolant flowrate, kg/s	642	1500
Reactor water inventory, m^3	75	175
<u>Intermediate Circuit</u>		
Coolant temperature, °C, inlet/outlet	140/80	160/90
Pressure, MPa	1.2	1.2
<u>Heating Grid Circuit</u>		
Water temperature, °C direct/return	130/60	150/70
Pressure, MPa	1.6 - 2.0	2.0
<u>Reactor</u>		
Reactor size, mm:		
Diameter	4290	5320
Height	17000	18370
<u>Core</u>		
Equivalent diameter, mm	2300	2800
Height, mm	1700	3000
Power density, average, kW/l	27.1	26.9
Fuel assemblies' number	85	121
UO_2/U inventory, t	19.3	48
Fuel element diameter, mm	13.6	13.6
Linear heat, rating, average, W/cm	97	96

SAFETY AND LICENSING OF NUCLEAR HEATING PLANTS

V.G. SNELL, J.W. HILBORN,
G.F. LYNCH, S.J. McAULEY
Chalk River Nuclear Laboratories,
Atomic Energy of Canada Limited,
Chalk River, Ontario,
Canada

Abstract

World attention continues to focus on nuclear district heating, a low-cost energy from a non-polluting fuel. It offers long-term security for countries currently dependent on fossil fuels, and can reduce the burden of fossil fuel transportation on railways and roads. Current initiatives encompass large, centralized heating plants and small plants supplying individual institutions. The former are variants of their power reactor cousins but with enhanced safety features. The latter face the safety and licensing challenges of urban siting and remotely-monitored operation, through use of intrinsic safety features such as passive decay heat removal, low-stored energy and limited reactivity speed and depth in the control systems. Small heating reactor designs are compared, and the features of the SLOWPOKE Energy System, which is in the forefront of these, are summarized. The challenge of public perception must be met by clearly presenting the characteristics of small heating reactors in terms of scale and transparent safety in design and operation, and by explaining the local benefits.

---

1. THE NEED FOR NUCLEAR HEATING

The increasing demand for economic and reliable energy supply is driven both by the growth in the world's population and by the essential role that energy plays in industrial development. With the global energy requirements expected to double over the next 40 years [1], all supply sectors will be seriously challenged in their ability to meet the demand.

The oil price shocks of the 1970s changed energy economics to the point that nuclear technology can now offer economically competitive energy sources in much smaller sizes that meet a broader range of applications. One such application of particular interest is building heating.

Many countries in the northern hemisphere consume in excess of 25% of their primary energy supply to satisfy their building heating requirements [2] Since the majority of the population lives in urban centers, a significant fraction of these heating requirements can be satisfied by central heating systems that use low-cost heat sources. Unlike transportation, this is an important energy sector which is readily amenable to the application of small-scale nuclear technology.

The current trend in building heating technology is towards hot water rather than steam. Consequently, in specifying a nuclear heat source, existing power-reactor technology is neither required nor appropriate. For example, a nuclear heating system can operate at significantly lower temperature and pressure, thereby eliminating much of the complexity that is associated with the production of high-pressure steam for electricity generation.

An analysis of the annual load curves for stand-alone heating systems in buildings in several countries has concluded that a nuclear heating system satisfying approximately 50% of the peak heat demand and used in a base load capacity could provide up to 90% of the annual heat requirements. By using a low-capital-cost, fossil-fired boiler to satisfy the peaking requirements, and acting as a backup to the more capital intensive nuclear heat source, the overall reliability requirements can be met at a cost which is competitive with fossil fuels.

For those countries with district heating networks which interconnect several load centers with a series of heat sources (much like established electrical grids), the potential for nuclear heating is even more attractive. In such cases, the nuclear heat source can be operated with much higher load factors, satisfying not only the base load requirements for heating but acting also as a source of heat for domestic hot water. In such circumstances, load factors of 80% can be expected with a corresponding improvement in the economic advantages.

In summary, nuclear heating offers the following advantages:

- low cost energy from a non-polluting fuel,
- long-term fuel security for countries currently dependent on imported fossil fuels, and
- reduced need for rail and road transportation of fossil fuels.

2. CHALLENGES AND REQUIREMENTS FOR LOCAL DISTRICT HEATING

Nuclear district heating plants must satisfy three very different "clients". The most obvious client is the customer who uses the heat - he demands safety, reliability, and acceptable costs. These demands become technical requirements on the design. The second client is the general public, who must balance the real benefits of the facility with their perception of the risk. The third client is the regulator, who demands licensability based on national experience with which he is familiar, and an assurance that he will not be faced with contamination of a populated area as a result of an accident. All three types of requirements are described in this section.

2.1 Design Requirements

To meet the essential requirements of public safety, plant reliability and low cost, the following factors must be considered:

(i) There is a balance between unit size, coolant pressure, siting and safety characteristics. In our view, it is uneconomic to build a plant with a pressurized water coolant below a power of about 200 MWt. Similarly, it is uneconomic to build a plant with an atmospheric pressure coolant above a power of about 50 MWt. This results in two classes of heating plants: large, pressurized units and small unpressurized ones. For the former, the combination of size and pressure gives a mechanism for dispersal of fission products beyond the immediate plant surroundings and therefore, certain mitigation measures are employed: containment/confinement and siting some distance away from dense populations.

For small nuclear heating plants, the economics of heat distribution by pipeline requires them to be located near the load; the low-pressure and small size preclude widespread fission product dispersal, and in addition, the chance of even local effects must be made very small by means of exceptionally benign safety characteristics. Current designs cover both types and range from 10 MW to 500 MW, where the 10 MW design is intended for urban sites, and the first twin 500 MW unit is located 7.5 km from the city of Gorky in the U.S.S.R. [3].

(ii) Existing large-scale district heating networks generally require a supply temperature of 120°C or higher.

(iii) Small-scale distribution systems can be designed to use water below 100°C.

(iv) Heat demand changes slowly with outside air temperature.

(v) Since the capital cost of nuclear reactors is significantly greater than the capital cost of fossil fuel boilers, the fuel and operating costs of nuclear heating plants must be minimized.

It is concluded that nuclear heating plants should be designed in small, unpressurized unit sizes if they are sited close to population centers, and even the largest plant will be much smaller than the average nuclear plant for electricity production. Nuclear heating plants should operate at the lowest temperature and pressure appropriate to the heat distribution system. They should be capable of automatic load-following for extended periods with a minimum of operator intervention. Control and safety systems can be slow in response and therefore relatively simple. For unit sizes at the low-end of the range (e.g., 10 MW to 50 MW) the ultimate goal is to minimize the need for operator attention. In that mode, a number of small units in various urban districts would be monitored at a central location, and at each site local power plant staff would carry out limited surveillance and maintenance.

The rest of this section discusses public perception and licensing issues for heating plants. The emphasis will be on local district heating, since large heating plants are viewed by the public, and treated by regulatory authorities, as being similar to power reactors.

2.2 Public Perception and Public Acceptance

Local district heating brings nuclear energy "home" in a more direct way than central nuclear electricity generation. Economics requires that the nuclear heat source be located close to the load, which means close to the general public. The plant is a neighbour, must be a good neighbour, and above all must be perceived to be a good neighbour. An accident in which no-one was hurt but which contaminated part of an urban area, could jeopardize an entire heating reactor program. While the risk of accidents can never be eliminated, the chance of an accident having significant off-site effects must be greatly reduced relative to alternative heating systems. Thus the design and operation should be transparently safe - simple and understandable enough that people can make an informed judgement. Routine effects from normal operation must be clearly trivial - at the level of the "noise" in the natural background radiation - and abnormal events expected to occur even once in the life of the plant should give insignificant incremental risk to an individual outside the building.

With respect to communicating an understanding of such risk, one of the goals in achieving public acceptance is to explain the small scale, and hence the small hazard, of a local district heating reactor. Clearly nuclear opponents will want to de-emphasize the small scale, to mix in nuclear weapons, and to raise the spectre of Chernobyls whenever nuclear power of any type is being discussed. The public does distinguish scale as an important factor in other technologies; for example, propane tanker trucks versus propane barbecue tanks, and small forgiving nuclear reactors should receive the benefit of the same distinction. This is in fact true for the SLOWPOKE-2 research reactors, whose benign characteristics have been clearly enough understood by the public, and have thus been accepted by the public in an urban environment. There are seven of these located and operating in cities in Canada, plus one overseas.

On the benefit side, there must indeed be a local, observable benefit - through lower heating bills, stable heat prices, reliability of supply, and through recognition that small heating reactors play an important role in reducing use of fossil fuel with its acid rain and uncontained waste products.

2.3 Safety Principles and Licensing

As noted earlier, licensing for large heating plants has generally evolved from the practice for their power reactor cousins. The Soviet Union, for example, has developed specific requirements for licensing large heating plants that permit location within 5 km of a city if certain additional safety requirements are met. Section 3 discusses some of the safety enhancement characteristics of these designs.

Local nuclear district heating is not new, but as noted in Section 2, the use has not been widespread, particularly of small heating plants located near the general public. Thus the major licensing challenge is the lack of direct precedent, either through long experience or regulations, to which the regulator can turn. Two related experience bases can bias the way licensing is done: these are research reactors, and power reactors.

Research reactors are generally the right scale. They are characterized by relatively low fission product inventory and low stored energy, easy access to the core and flexibility in core configuration, and "hands-on" operation. Safety is achieved both by engineered safety features, and a reliance on highly-skilled people reviewing proposed experiments and core changes, and following administrative procedures in performing them. Remote siting can be a further defence where a mechanism for dispersal of fission products exists. Thus if one views elements of safety as inherent design characteristics, process systems, engineered safety features, containment/siting and human intervention, most research reactors are more oriented toward the latter elements than the former.

Power reactors are orders of magnitude larger in scale. They have large fission product inventories and high stored energy; core access is difficult and highly controlled; core configuration changes are not permitted except under unusual circumstances; routine operation is continuously monitored by on-site operators but for the most part automatically controlled; automatic safety systems remove the immediate need for operator intervention; and the plant is normally provided with an exclusion zone but can be sited modest distances away from urban areas. Power reactors thus rely more on engineered safety features than on inherent design characteristics and human intervention.

Desirable safety-related characteristics for small heating reactors can be stated as follows:

1. The power, and hence the fission product inventory, are generally low.

2. There is highly restricted access to, and infrequent changes to, the core. The control devices for load-following are slow-moving and stability is aided by negative reactivity coefficients.

3. All the reactor safety systems are automatic or self-actuating. Effects of failures in the safety systems are mitigated by inherent properties or self-actuating processes. Automatic initiation of a safety system cannot be easily disabled by an operator. Safety devices are testable on power, without risk of a spurious shutdown. All critical components of a safety system are fail-safe or have independent back-up. Two independent and diverse shutdown systems are provided unless automatic shutdown can be guaranteed by inherent physical or chemical properties.

4. The mechanism for removal of decay heat has the same reliability and effectiveness as an automatic safety system for several days after shutdown. Passive decay heat removal is the usual approach.

5. The stored energy in the coolant is low. A sudden loss of coolant is prevented, usually by double barriers. Following a small loss of coolant, there is no need for an external supply of water, nor for human intervention, for several days,

6. The plant can withstand credible external events typical of an urban industrial environment, such as severe natural phenomena, industrial accidents in nearby facilities, and the consequential effects of natural and man-made disasters on nearby facilities.

7. The water pool provides significant retention of fission products released from the pool.

8. Storage of used fuel is on site, usually in the reactor pool or vessel, so that shipments of used fuel are infrequent or absent.

All these characteristics mean that the plant can operate with no need for routine operator intervention or presence.

It is clear from this list that the safety of small heating reactors relies much more on inherent design characteristics, and to a lesser extent on shutdown systems, than on engineered heat removal, siting or human intervention.

Figure 1 shows how safety is achieved by balancing prevention, protection, mitigation, and siting and how each reactor type uses a different "mix" of these aspects to ensure public safety. Thus for small heating reactors, licensing should not only choose from the appropriate elements of existing research and power reactor philosophies, but recognize and credit the increased emphasis on preventing an accident, as opposed to containing it after fuel has been damaged. Swiss regulations for small heating reactors reflect much of this thinking [4].

It is the emphasis on accident prevention which permits both urban siting and remotely-monitored operation. They are not new concepts by themselves - both have been accepted for a number of years in Canada for the 20 kW

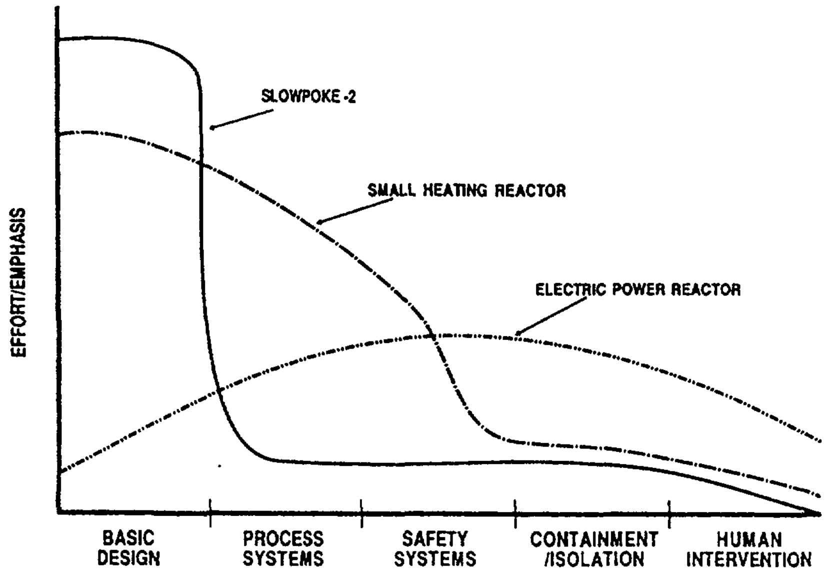


FIGURE 1: REACTOR SAFETY CURVE

SLOWPOKE-2 research reactors, on the basis of an inherent design characteristic - because of the limited amount of reactivity available to the control system, and the negative temperature coefficients of reactivity, they do not need an engineered shutdown system, and can be left unattended for periods of up to 24 hours. The SLOWPOKE Energy Systems 10 MW heating reactor retains many passive safety characteristics - for example, decay heat removal is passive - but because it operates at higher power, requires an engineered shutdown mechanism and in fact is provided with two separate, independent, and diverse shutdown systems, to eliminate the potential of failure to shutdown for an abnormal event. This redundancy reflects a philosophy pioneered by CANDU nuclear generating stations. Thus the issues raised by small heating reactor licensing are not novel by themselves, although the combination is.

In Canada an inter-organizational Small Reactor Criteria (SRC) working group was formed in 1988 to propose criteria for all small pool-type reactors [5]. The group comprises four people from organizations in Canada responsible for reactor licensing or involved in the development or operation of small reactors: the Atomic Energy Control Board, Atomic Energy of Canada Limited and McMaster University. Two levels of criteria have been proposed: the first level forms a safety philosophy and the second, a set of criteria for specific reactor applications. These criteria are not regulatory requirements but are being issued for peer review and for consideration by the sponsoring organizations [6]. The work should be of value in helping these organizations design and licence small heating reactors.

3. APPLICATIONS: LARGE CENTRALIZED PLANTS

This section reviews some of the experience with large heating plants and summarizes actual operation and selected designs. The small heating reactor experience is covered in Section 4. The discussion is restricted to water-cooled reactors.

Use of nuclear power for district heating is not new, although most large facilities to date have been co-generation, supplying both heat and electricity. In Sweden, a prototype nuclear district heating plant at Agesta supplied a Stockholm suburb (Farsta) with 55 MW of heat from 1963 to 1973; in addition a turbine could supply about 10 MW of electricity ([7],[8]). The Stade PWR in West Germany and the Gösgen PWR in Switzerland, provide low-temperature process heat for industrial purposes ([9],[10). The Beznau nuclear power station in Switzerland supplies nuclear-generated district heat to a number of communities within a seven kilometer radius ([10],[11]). In Canada, the Bruce Nuclear Power development, with eight CANDU reactors, can supply 5,350 MW of medium-pressure process steam to the nearby heavy-water plants, and for industrial uses to the Bruce Energy Centre Industrial Park [12]. Co-generation has likewise been used in nuclear electric power plants in the U.S.S.R. - the four-unit Bilibino plant in Siberia has supplied electricity and heat since 1974; co-generation is used at both PWR and RBMK-type reactors [10].

Such co-generation facilities have generally followed the safety and licensing practices of electric power reactors. Of more interest are large nuclear plants, currently in design or construction, dedicated to district heating. The ACT-500 program in the U.S.S.R. is the most advanced: the twin 500 MW unit at Gorky is in the latter stages of construction, and will supply hot water to about half the city [10]. Kraftwerk Union AG in the Federal Republic of Germany has designed a 100-500 MW district heating reactor [13]. Other designs include the THERMOS 100-200 MW French reactor [14]; the 100-400 MW Swedish SECURE reactor, a forerunner of the PIUS concept [15]; and the 64 MWt TRIGA power system. A 5 MW experimental reactor prototype of a 450 MW demonstration reactor is under construction in the People's Republic of China [10].

These newer designs have improved safety to reflect their siting near urban areas. They have more forgiving characteristics, and in general feature natural circulation, lower fuel ratings and lower stored energies. The Soviet and German designs are doubly contained in two pressure-vessels, the outer of which acts as both a double barrier to escape of primary system fluid (so the core is kept covered even if the first barrier fails) and as a containment; this is achieved in the SECURE concept by a thermally-coupled pool in which the reactor is immersed. They emphasize passive decay heat removal for hours and less reliance on prompt human action.

4. SMALL HEATING REACTOR EXPERIENCE

4.1 SLOWPOKE Heating Reactor as an Example

To illustrate how the small reactor safety principles discussed in Section 2 are incorporated in a design concept, the Canadian SLOWPOKE heating reactor will be used as an example.

The main protection against a major release of radioactivity from the 10 MW core is the fuel itself. By restricting the maximum fuel temperature in normal operation and in accidents, most of the fission products are retained within the uranium oxide pellets, and only a small fraction of the fission product gases escape to the narrow gap between the ceramic pellets and the metal sheath. If the sheath should fail, iodine would remain in the large volume of pool water and a small quantity of radioactive xenon and krypton could escape to the cover gas above the pool surface. The ultimate release to the environment from a single sheath failure would be well within regulatory limits for normal operation.

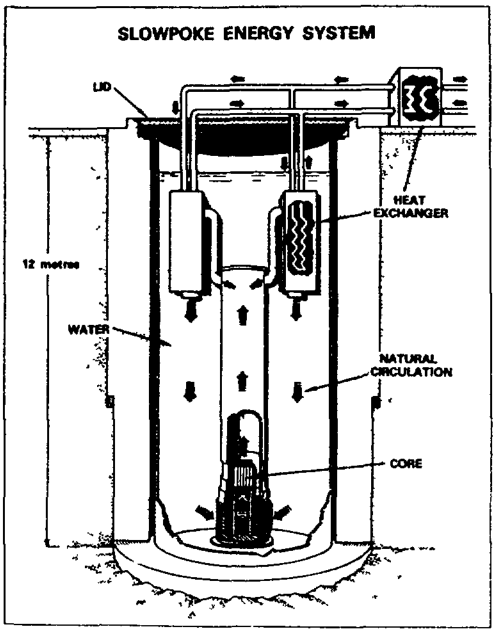


FIGURE 2 SCHEMATIC DIAGRAM OF THE SLOWPOKE ENERGY CONCEPT

Other important safety features of the SLOWPOKE concept (Figure 2) are listed below:

- A pool type reactor avoids the need for a nuclear pressure vessel and high pressure piping system.

- Operation below 100°C and near atmospheric pressure avoids a large source of stored energy and loss of coolant by depressurization.

- Natural circulation of primary coolant in the pool avoids a loss-of-primary flow accident.

- Double containment of the pool in a steel vessel and concrete vault prevents loss of coolant by leakage. An air gap between the two containers permits both detection and control of leakage.

- Slow-moving control devices permit slow-response safety systems.

- The negative reactivity effects of coolant density and fuel temperature attenuate the power transient following control system faults.

- The large heat capacity of the pool delays the core temperature rise following loss-of-secondary coolant flow.

- The top surface of the pool is not open to the reactor building as in many pool-type reactors, but is enclosed with a steel cover plate and concrete shield. The vapour space between the pool surface and the cover plate is used to monitor and control gases released from the pool.

- A mechanical shutdown system and a liquid shutdown system are provided. Both systems are actuated by gravity and each system has separate dedicated instrumentation for detecting potentially hazardous conditions.

- Long-term decay heat removal is by conduction to the ground through the concrete wall of the pool.

From this example, we now survey world experience in small reactors.

4.2 Worldwide Small Heating Reactors

A survey of proposed small heating reactors in the rest of the world shows similar trends to SES-10. Six proposed designs were examined, as an example of current international trends. Five of the six reactors are based on standard designs with safety-related modifications; the sixth, GEYSER, is a departure from contemporary designs in that it does not use conventional engineered safety systems or controls. The reactors examined are listed in Table I. SES-10 is included again, as a reference point.

Table I

Small Heating Reactors

Designer Country	Reactor Name	Type
Canada	SES-10	Cover Pool Absorber Rod Control
Russia	RUTA [16]	Covered Pool Be Reflector and Absorber Rod Control
Switzerland	Swiss Heating Reactor SHR [16, 17, 18, 19, 20]	Pressurized BWR Absorber Rod Control
Switzerland	GEYSER [17, 21]	Covered Pool Chemical Control
West Germany	High Temperature Gas Cooled Heating Reactor GHR [17, 22]	Pressurized Helium Cooled Reactor Absorber Rod Control
United States (General Atomics)	TPS [17, 23]	Pressurized TRIGA Absorber Rod Control

The features of most interest are the following:

(i) Negative reactivity coefficient

All six designs take advantage of fuel temperature feedback. SES-10, RUTA, and SHR use UO_2 fuel; GHR uses TRISO coated UO_2 fuel; GEYSER may use either UO_2 or Uranium Zirconium Hydride (TRIGA) fuel; and the TPS uses TRIGA fuel. The SES-10, RUTA, SHR, and TPS also take advantage of the negative reactivity effect of the light water moderator temperature and void to mitigate reactivity transients.

(ii) Shutdown heat removal

Five of the designs have taken advantage of a large volume, low temperature pool (GHR excepted) and natural circulation capability to remove decay heat without the need for emergency power sources. Either the pool is a part of the primary heat transport system with natural circulation as the normal operating cooling mode (SES-10, RUTA, GEYSER), or a passive connection is made to the pool on loss of the normal heat removal and natural circulation used to transfer heat to the pool. Heat is removed from the pool via normal pool heat loss (SES-10, SHR and GEYSER) or via natural circulation to a passive heat removal system (RUTA, GHR and TPS).

(iii) Low operating temperatures

All six designs operate with normal fuel temperatures well below their failure limit allowing them to take maximum advantage of the negative fuel temperature reactivity feedback without endangering the fuel. The presence of a large volume, low temperature pool has the additional benefit (SES-10, RUTA and GEYSER) of mitigating a loss of heat removal such that inherent features and the normal control system can cope with the event without the need for a safety action.

(iv) Loss of coolant susceptibility

As mentioned in (ii) above, five of the designs use the low-pressure pool as part of the primary coolant system or provide passive connection to a pool on loss of the primary coolant system to prevent a loss of coolant accident. All six designs are inground facilities. Those incorporating the pool as part of the primary heat transport system have double-lined pools (concrete with steel liner), which combined with the inground location and the low-pressure, ensures that rapid pool water loss is incredible. The sixth, GHR, has been designed with a low enough power density such that a loss of the helium coolant will not result in an unacceptable overheating of the fuel.

(v) Radioactivity confinement

All six designs operate their fuel at temperatures well below the point where significant fission product release from the fuel matrix can occur. Failure of a fuel cladding will not result in a significant fission product release. Five of the designs take advantage of the radioiodine and particulate retention capabilities of a water pool. The RUTA reactor also uses fuel with double cladding to reduce the probability of cladding failure. In the non-pool reactor, GHR, the fission products are retained in the fuel up to a fuel temperature of 1800°C and in the accidents considered fuel temperatures remain well below that level. All six designs provide some form of confinement for fission gas release, either in the form of a covered pool (SES-10, RUTA and GEYSER), or a separate concrete structure surrounding the reactor (GHR, SHR and TPS).

(vi) Safety shutdown systems

Four of the designs have two separate safety shutdown systems with varying degrees of independence and diversity. The SES-10 and SHR have a dual purpose control and safety absorber rod system and a separate liquid absorber insertion system. The GHR and the TPS have a dual purpose control and safety absorber rod system and a dedicated safety absorber rod system. The RUTA design currently has a dual purpose control and safety absorber rod system but is considering the addition of a separate liquid absorber system. The GEYSER uses flooding of the core from the highly borated pool. The flooding is passive due to a pressure imbalance between the core and the pool when reactor power exceeds a predetermined level.

(vii) External hazards protection

An effort has been made in all designs to protect against external hazards. The protection varies from a concrete cover (RUTA and GEYSER), to a concrete cover plus hardened control room (SES-10), to the emplacement of the facility and all essential equipment underground in a concrete structure.

(viii) Available excess reactivity

To minimize operating cost an extended core life is a desirable feature in these reactors. The life varies from 3 to 5 years for the TPS, RUTA and SES-10 and from 12 to 15 years for SHR, GHR and GEYSER. A considerable amount of excess reactivity is required to achieve these targets and an effort has been made to reduce the amount of this reactivity under the control of movable absorbers. The designs normally use burnable absorber material to do this. Efforts have also been made to reduce the size of individual absorbers to reduce the consequence of a single absorber removal.

(ix) Long period for corrective action

The designs considered have succeeded to varying degrees in achieving this goal by incorporation of these features.

5. CONCLUSIONS

Small heating reactors offer a safe and economic alternative to fossil fuel for local municipal and institutional district heating. As a replacement for fossil fuel, they reduce the damage due to acid rain and hydrocarbon wastes.

The requirements for urban siting and remotely-monitored operation lead to design requirements such as slow rates of change in power aided by stabilizing reactivity characteristics, natural circulation and passive decay heat removal, modest performance requirements for shutdown, low fuel ratings and low free fission product inventories, tolerance to upsets in operation and minimal dependence on people to ensure safe operation.

Licensing innovation is required, but modest: precedents from licensing both power reactors and research reactors can be used in developing a sensible approach to small heating reactors, and already exist for items such as unattended operation and urban siting.

When comparing the nuclear option with other energy options, environmental and safety issues have become as important as cost. Moreover, the public perception of these two issues has tended to discredit nuclear power and indirectly add to the cost through increasingly stringent regulations. The present challenge is to convince the public that the long-term advantages of an economic non-polluting heat source far outweigh the risks of nuclear technology.

REFERENCES

[1] Frish, J.R., ed., Energy 2000-2020: World Prospects and Regional Stresses, London, Graham & Trotman, 1983.

[2] Lynch, G.F., et al., Unattended Nuclear Systems for Local Energy Supply, Paper 4.2-2, Thirteenth Congress of the World Energy Conference, Cannes, 1986.

[3] Baturov, B.B., et al., The Use of Nuclear Reactors for Central Heat Supply and District Heating, Proceedings International Conference on Nuclear Power and its Fuel Cycle, Salzburg; May 1977.

[4] Swiss Regulatory Commission, Protection Targets and Design Rules for a Swiss District Heating Reactor with Small Power, September 1988.

[5] French, P.M., Ernst, P.C., Axford, D.J., and Snell, V.G., Recent Initiatives at the IAEA and Within Canada to Develop Small Reactor Safety Criteria, Proceedings of the 10th Annual Conference of the Canadian Nuclear Society, Ottawa, June 1989.

[6] Ernst, P.C., French, P.M., Axford, D.J., and Snell, V.G., Development of Small Reactor Safety Criteria in Canada, paper to be presented at the International Symposium on Research Reactor Safety, Operations and Modifications, 1989 October 23-27, Chalk River Nuclear Laboratories.

[7] Nuclear Heat Application, Proceedings of a Technical Committee Meeting and Workshop, Cracow, December 1983; International Atomic Energy Agency; from Summary Report.

[8] Hannerz, K. and Larsson, Y., Reactor Waste Heat Utilization and District Heating Reactors, Proceedings International Conference on Nuclear Power and its Fuel Cycle, Salzburg; May 1977.

[9] Schutz, E., Grosstechnische Lieferung von Prozessdampf aus dem Kernkraftwerk Gösgen Daniken (Schweiz). Siemens Energietechnik 7 (1981), 219.

[10] Low Temperature Nuclear Heat Applications: Nuclear Power Plants for District Heating, Report of an Advisory Group Meeting on Low-Temperature Nuclear Heat Applications, Prague, June 1986; International Atomic Energy Agency publication IAEA-TECDOC-431.

[11] Handl, K.H., Fernwarme fur acht Gemeinden vom Kernkraftwerk Beznau, Fernwarme International 14 (1985), 46.

[12] Morgan, A.V. and Dias, F.E., The CANDU Nuclear Reactor and Process Heat, in Nuclear Heat Application, Proceedings of a Technical Committee Meeting and Workshop, Cracow, December 1983; International Atomic Energy Agency; paper IAEA-TC-483/26.

[13] Bitterman, D., et al., Design Aspects and Pertaining Development Work for the KWU 200 MW(th) Nuclear Heating Reactor, Nuclear Engineering and Design, 108 (1988), 403-417.

[14] Girard, Y., Centrales Nucleaires Francaises pour la Production de Chaleur, in Nuclear Heat Application, Proceedings of a Technical Committee Meeting and Workshop, Cracow, December 1983; International Atomic Energy Agency; paper IAEA-TC-483/11.

[15] Pedersen, T., The SECURE Reactor, in Nuclear Heat Application, Proceedings of a Technical Committee Meeting and Workshop, Cracow, December 1983; International Atomic Energy Agency; paper IAEA-TC-483/19.

[16] Artamkin, V.N., Passive Safety of Water-Cooled Pool Type Reactor for Nuclear Heating Plants, Research and Development Institute of Power Engineering, 1988.

[17] International Atomic Energy Agency, Small Reactors for Low-Temperature Nuclear Heat Applications, IAEA-TECDOC-463, 1988 June.

[18] Brogli, R., et al, Design Aspects of a Small District Heating Reactor, Paul Scherrer Institute, Wurenlingen, Switzerland, 1988 June.

[19] Burgsmuller, P., et al, The Swiss Heating Rector (SHR) for District Heating of Smaller Communities, paper presented at the IAEA Advisory Group on Small Reactors for Low-Temperature Nuclear Heat Applications Meeting, Winnipeg, Canada, 1987 June.

[20] Foskolos, K.G., et al, Solutions of Neutronic Design Problems of Small Heating Rector Cores Based on the BWR Principle, Nuclear Engineering and Design, 108 (1988), 419-427.

[21] Doroszlai, P.G.K., and Vecsey, G., GEYSER, a Simple New Heating Reactor of High Inherent Safety, see [19].

[22] Ribbat, B., and Sommer, H., GHR 10 MW: The Technical Concept of the Gas Cooled Heating Reactor, see [19].

[23] Schleicher, R.W., TRIGA Power System: A Passively Safe Cogeneration Unit for Electric Power and Desalination for Small Communities, GA Technologies, 1987 June 23.

SAFETY ASPECTS OF NEW DESIGNS AND PROCESSES FOR THE NUCLEAR FUEL CYCLE

(Session VIII)

Chairmen

Y. KISHIMOTO
Japan

W. STOLL
Federal Republic of Germany

SAFETY ASPECTS OF THE UO_2 FUEL CYCLE

R. LALLEMENT
Commissariat à l'énergie atomique,
Paris, France

Abstract

The nuclear fuel cycle entails several necessary steps from the ore mining to the final disposal of the fission products.

The public acceptance of the nuclear energy option depends on the safety of all the technological steps of the cycle.

This paper intends to assess the main safety issues of enrichment, fuel fabrication, fuel reprocessing, transportation and waste disposal.

It is shown that the safety problems in the fuel cycle are milder and easier to control than for the reactor case, because the amount of radioactivity involved in any step of the cycle is generally rather low.

It does not mean than nothing has to be done to improve safety of the cycle.

In the future, one can foresee a general trend to reduce the effluent release from the reprocessing plants and a steady effort to solve the problem of long term storage of high activity - long life wastes.

I - INTRODUCTION

The decision to establish nuclear reactors as a source of energy entails many other technological obligations than the mere construction and operation of the reactor itself. It is clearly evident that it is necessary to transform uranium ore into a suitable fuel for the reactors and that one must take care, one way or another, of the irradiated fuel and its associated fission products.

Those several technological necessary steps from the ore to the final disposal of the fission products are called the nuclear fuel cycle.

The safety of the nuclear cycle has to be assessed and controlled as well as the safety of the reactor itself in order to allow a comprehensive judgment on the safety of nuclear energy.

This is true whether the cycle is "open", that is to say when irradiated fuels are not reprocessed, as well as when the cycle is "closed", that is to say when irradiated fuels are reprocessed and uranium and plutonium are reintroduced in the cycle.

The general feeling of the non specialist is that the main safety problems lie in the reactor itself, where an enormous amount of energy is concentrated in a small volume, compared to the fuel cycle where either there are only natural fissile materials at a low enrichment, or "cooled" irradiated products in a rather non concentrated form.

This paper intends to specify those global and simple judgments in more details.

II - GENERAL RULES AND METHODOLOGY

II.1. In evaluating the safety of the several steps of the cycle some general rules are followed. They concern the safety of the workers and the safety of the public.

The type of risks which are of concern are either conventional (chemical risks, mechanical risks, fires), natural (earth quakes, wind, storms) or nuclear (irradiation, criticity, contamination), or a combination of all of them.

In all cases, the technical activities within the fuel cycle must, as a principle rule, comply with the statutory limits on dose uptake, be as safe as possible when conventional industrial risks are involved, and must entail the minimum reasonable radiation level on the workers.

The public is concerned directly in case of accidents which can induce immediate risks, and also in case of discharge to the environment where the consequences can be more diffuse and of longer term. Those accidents have to be identified as best as possible, their consequences assessed, and measures have to be taken in order that the radiation level to the public remain in all cases below the level recommanded as safe by the competent authorities.

As far as the discharges to the environment are concerned, which are of ecological nature, they have to be evaluated carefully, and minimised as much as possible.

This is well known, has been debated and discussed at length, and the discussions will continue in order to reach "reasonable" rules, based on sound assessments and results, which must, at the same time, protect the workers and the public and maintain the nuclear cycle in operation. Excess and disequilibrium in any direction have to be carefully avoided.

II.2 A systematic methodology has been adopted by the safety authorities and the industrial companies involved in the cycle, in order to analyse thoroughly all the activities implied in all the steps of the cycle.

Schematically the methodology is the following :

a) general analysis of all the activities,

b) research and identification of all the causes of danger,

c) definition of the accidents of most significance,

d) evaluation of the probability of those accidents,

e) evaluation of the consequences of thoses accidents,

f) actions to prevent those accidents,

g) actions to minimise the consequences of those accidents, should they occur, and maintain those consequences within the "authorised level", when radiation is concerned.

III - THE TECHNOLOGICAL STEPS OF THE CYCLE BEFORE THE REACTOR

III.1 Several technological steps are necessary before uranium ore is transformed into a suitable fuel. They are : the mining and ore processing, the refining of uranium and its conversion to hexafluoride, the enrichment of uranium and the fabrication of the fuel.

All those technological steps deal only with natural radioactive nuclei, namely uranium isotopes U238, U235 and U234.

It is convenient to separate the analysis of these activities from those after the reactor, namely reprocessing, waste treatment, and plutonium fuel fabrication, which involve artificial radioactive nuclei, because the level of radioactive risk of the first category of activities is obviously much lower.

We will not discuss the mining, ore processing and conversion to hexafluoride in this paper, because it is a very specific subject. Nevertheless it must be known that the mining industry involves very important radiological problems, and it would be very useful to assess how a closed cycle, with the use of uranium and plutonium, can reduce the need for mining and milling, and to compare the resulting radiation dose uptake in both scenarios.

III.2 Enrichment of uranium

The most utilised process to enrich natural uranium is gaseous diffusion.

The principle of the process is to force gazeous uranium hexafluoride (UF6) to diffuse through poreous ceramic barriers. Three main steps are necessary for the process : first a compression to raise the pressure of UF6 to the required value, then a heat exchange to dissipate the heat produced by the compression of UF6, then the diffusion process itself.

The safety of gaseous diffusion plants is correlated to the classical risks (fires, handling, electricity supply), to the nature and to the quantity of the substances circulating in the plant which are mainly fluorides, and to the presence of uranium. One should note that for the Eurodif plant in Pierrelatte the hold up is around 3000 t of UF6.

III.2.1 Nuclear risks

a) Criticality : UF6 is always non critical for the maximum enrichment foreseen in the plants. However the presence of impurities containing hydrogen (HF, water), or hydrocarbon (oil), as well as the possibility to form uranium compounds different from UF6 (oxyfluoride as an example) makes necessary some special rules. For example :

- strict control of U235 and HF concentrations,

- addition of neutron absorbing compounds at the heat exchange stage, after compression of UF6,

- systematic water leak detection,

- choice of favourable geometry for the process equipment to prevent neutron moderation,

- many heat transport fluids are chosen to be chlorine compounds,

- systematic neutronic poisoning of uranium solution tanks.

b) Loss of radioactive substances

The possibility of a leak of UF6 is real and leaks have already occurred in all the enrichment plants.

Those incidents have no damaging consequences when they are quickly detected and when the leak can be stopped rapidly.

We recall that the danger of a release of UF6 is more linked to the presence of HF formed by reaction with water than to the presence of uranium. All the precautions are taken to confine and control the volumes where UF6 is treated (tanks, compressors, collectors) in order to isolate them in case of leak. It is the reason why the leak of the totality of the hold up of an enrichment plant is considered as impossible.

In one of the worst accidents of this type which occured in the past, several tons of UF6 escaped from a container. The worst cast could be the leak of the totality of a container (12 tonnes). In all cases the consequences can be controlled and are small for the public.

III.2.2 Non nuclear risks

Fires : The possibility of fires exists, due to the presence of oil for the compressors, and of electric cables. This type of risk is conventional and the ways to handle it are well known.

Chemical risks : As we have already said the major risk coming from enrichment plant is the chemical risk coming from the presence of HF when UF6 is released to the atmosphere.

One must add that some compounds utilised in the process (chlorine trifluoride for example) can react explosively with carbon containing compounds. This risk is taken into account in the conception of the plant and very strict measures are taken to control the presence of those compounds.

Other risks : The other natural risks (earth quakes, floods etc...) are taken in account in the design of the plants.

Conclusions: On the whole the risks linked to a gas diffusion enrichment plant are very low compared to the other risks in the cycle. The main risk is of chemical nature and related to the production of HF if a UF6 leak occur. The maximum quantity of UF6 susceptible to escape is low and cannot affect seriously the environment.

III.2.3 Centrifuge plants compared with diffusion plants

- The in-process inventory of a centrifuge plant is very much lower than in a diffusion plant ; typically the inventory is of the order of 10 kgU in a unit of 100 t SW per annum. It follows that that the hazard in the event of a plant leak is much reduced. Also the general levels of radiation in the plant are lower.

The inventory of the feed, tails and products stations will depend on the throughput, and will be similar for both types of processes. If UF6 is to be held in the liquid rather than the solid state at these stations, special attention is required in design and operation to ensure containment.

. Centrifuge plants are designed on a zero maintenance philosophy. This results in reduced radiation exposure of the workforce.

. The sensitivity of the centrifuge machines to earth-quakes does not present a hazard ot the operators or the public as there would be no significant release of process gas.

On the whole, the risks linked to a centrifuge plant are even much lower than for a gaseous diffusion plant.

III.3 Fuel fabrication

The fuel fabrication process comprises several steps :

- conversion of UF6 into UO2,
- pellet fabrication,
- pin fabrication,
- fuel assembly fabrication.

Non nuclear risks :

Two steps imply chemical risks. The first one is linked to the presence of UF6, which as well as in enrichment plants, can lead to the production of HF in case of significant leak. The second one is linked to the explosion risk linked to the utilisation of hydrogen in the reduction - sintering process of the pellets. All those risks are controlled by strict operational rules during the plant operation.

Nuclear risks :

The nuclear risks are low :

- criticality is controlled by the geometry of the equipment and by a strict control of the masses of UO2 involved, which is generally of low enrichment (~3,5 %)

- the dissemination of radioactive material is avoided by special confinement and ventilation measures in the plant.

A special care has to be taken for the wastes and effluents produced in the process in order to minimise them and to recycle uranium in the plant as much as possible.

Conclusion :

In a fabrication plant of UO2 fuel for PWR, the main chemical risk comes from the presence of UF6 at the beginning of the process. The other risks (criticality and dissemination of radioactive materials) are controlled by specific designs of the equipment and of the plant itself.

In the future, when uranium coming from reprocessing is widely utilised in fabrication plants, new problems might occur due to a higher specific activity of the fissile material, which could lead to a higher risk of irradiation for the workers. In particular, one must recognise that U234 (α emitter) is enhanced in recycled uranium, and that the presence of U232, and specifically its decay product thallium 208 which is a hard gamma emitter, increases the level of radiation in the fabrication step. There can also be transuranic elements (Pu isotopes and Np) as well as residual fission products (Tc 99, Rh 106) contamination.

Those problems do not raise unknown and unsolvable problems, according to the first manufacturing campaigns carried out all over the world.

IV - THE TECHNOLOGICAL STEPS OF THE CYCLE AFTER THE REACTOR

IV.1 Reprocessing

IV.1.1 All the reprocessing plants in the world utilise the Purex process and the technological steps in those plants are very similar.

The irradiated fuel assemblies are transported to the plant, then stored in huge pools (in La Hague the storage capacity is 10 000 tons of uranium). Then after a rather long cooling time, generally a few years chosen to allow the decay of short lived fission products, the fuel assemblies are introduced in the process line, where they are cut, and dissolved.

The solution is then clarified, fission products separated from uranium and plutonium by solvent extraction, and then plutonium and uranium are separated from each other.

All the steps produce radioactive waste (gases, fines, technological waste, fission products, transuranium nuclei) or valuable fissile material (uranium and plutonium).

The secret of a safe reprocessing plant is to take care of all the questions in a comprehensive and coherent way, by thorough analysis, deep evaluation and appropriate measures, no question being deferred and delayed. A reprocessing plant has to be considered from the beginning as a plant which produces plutonium, uranium and wastes of all kinds, which have to be taken care of in the right way ab-initio.

IV.1.2 This being said, a general assessment of the safety of a reprocessing plant can be made by comparison between such a plant and a reactor, knowing that :

- the power per volume in a reprocessing plant is much lower than in an operating reactor (1/1000 less).

- the pressures in the circuits are near atmospheric pressures.

- the slow evolution of the process give time to control hazardous situations.

On the other hand the radioactive species are more easily dispersable (gaz, liquids, powders) ; some chemical products (like nitric acid) are rather agressive and may induce corrosion ; the confinement barriers are large and have many discontinuity and holes ; chemical hazards are to be considered due of the presence of nitrates, solvents, hydrogen and chemical products ; and last but not least, a great variety of geometrical configurations of the apparatus, tanks and pipes have to be checked again the risks of criticality.

IV.1.3 As a consequence, eventhough the positive factor (power per volume) is very important, a great care has to be taken to minimise all the risks.

A general approach is to look carefully in all the systems contributing to safety.

Four groups of safety related functions can be identified.

- The confinement functions for gases, radioactive liquids, radioactive solids, and chemical products.

- The structures themselves (building, supporting of the equipment, shielding).

- The auxiliary structures, like ventilation, energy and fluid supply, fire protection, handling and maintenance devices.

- the control functions, like the information on the operation of the plant and the radioprotection system.

They all contribute to the general safety of the plant. None of them can be neglected. The specific measures are difficult to describe in detail, they are the fruit of the operating experience, and they are as important (may be more) than the specific analysis of selected reference accidents.

IV.1.4 This being said, it is nevertheless important to point out where are the main points of concern in a reprocessing plant.

a) Storage of the fuel

The quantity of fuel stored in a big reprocessing plant is high (10 000 tons for La Hague) representing several megawatts of residual heat.

A prolonged loss of cooling of the pool cannot be tolerated. However as the volumic power in the fuel is low, the consequences of a loss of cooling are radically different from the LOCA in a reactor. Several hours or days are needed to reach dangerous situations. All the necessary measures are taken to insure a permanent cooling of the storage pools and the risks are judged as non significant.

b) Storage of the fission products

The other places where a great quantity of radioactive materials exists are the tanks where fission products are stored in the liquid form. To day, several tanks are in use in the existing plants in order to store the fission products which have been produced from the past activities and which are not yet vitrified. They will be progressively emptied and their content sent to vitrification, and all the reprocessing plant will be operated in such a way that the number of storage tanks will be a minimum. The fission products will be eventually incorporated in glasses "on line".

The loss of cooling of those storage tanks has been taken by the French authorities as a reference accident in a reprocessing plant, because the source term can be significant (of the order of 2-5 10^8 Cie per tank) and because the heat emitted is high (1,2 MW per tank).

The result of the loss of cooling scenario would be that the solution might boil after 6 hours ; that some aerosols would be emitted during the next 20 hours ; then ruthenium would be emitted more and more. After two days, 80 % of the solution would be evaporated.

In this case the time scale for significant safety problem to occur is much longer than for the reactor case.. It is reasonable to think that there is time enough to establish some cooling system before significant release of radioactivity occurs, tanks to redundancy in power supply and also to the availability of spare tanks..

c) Criticality

Criticality accidents may occur in reprocessing plants because fissile material is now in aqueous solution (or extracted into organic solvent) in which moderation can occur - unlike the cases with UF6 or UO2.

The complexity of the piping and tank system in a reprocessing plant, the diversity of the liquids and solids, make possible a criticality accident, if great care is not taken. Several accidents have already occurred in the past in reprocessing plants.

Safe geometry has to be imposed in the maximum of cases, and if it is impossible to have an all safe geometry, special rules have to be imposed for quantity and quality of fissile materials as well as operational procedures. It is felt that with care for this problem from the conception stage and good operational rules, the criticality problem can be mastered.

IV.1.5 The other conventional accidents which can occur in any chemical plants, like fires, explosions, handling problems, are also taken into consideration with great care. They all can create conditions where some radioactivity can be released in the plant. It is true that the quantity of radioactivity susceptible to be released is rather small in each case, because radioactivity is not very concentrated in a reprocessing plant, apart from the two cases described above.

Nevertheless, all the measures are taken to avoid dissemination of any radioactivity liberated by those classical accidents. Several barriers are established to avoid dispersion of radioactivity in the zones where workers operate.

The barriers are the circuits and apparatus themselves, the shielded cells, and the buildings around the cells.

A system of controlled depression is generally established in the plants to insure that the pressure decreases from the outside towards the inside.

It is highly improbable that significant radioactivity can be released in the environment due to classical accidents.

IV.1.6 "Normal" release of radioactivity

During the process, and in accordance with the accepted regulations, some radioactivity is released to the environment.

Those releases concern gaseous effluents (Krypton 85, iodine 129, carbon 14, tritium) and liquid effluents containing alpha, beta and gamma emitters, tritium, Cs and Sr.

The trend of all the existing or future plants is to decrease drastically all the released quantities. Variations among the reprocessing plants (La Hague, Sellafield, JNFS) may be observed due to the site selection and to the critical group of the public concerned by those releases.

Some targets set up for the new projects are challenging for all of us.

The future will tell us where is really the "As Low As Reasonably Achievable" target. I think that nobody should forget that reasonably implies "technically and economically reasonable". I believe also that reasonable means "compatible with the known radiological standards".

IV.1.7 In line waste treatment

A reprocessing plant produces continuously uranium, plutonium, gazeous and liquid effluents, technological wastes, fissions products of all kinds.

A reprocessing plant must be organised to process all those products continuously, on line, without undue accumulation.

This is a key point of the safety of reprocessing plant.

It is fair to say that the waste treatment methods and technologies are an integral part of the reprocessing system and the clue to a safe operating plant.

IV.1.8 Conclusion :

The safety of reprocessing is well assessed and controlled and does not raise problems of the same order of magnitude as for the reactors.

Great care has any way to be maintained to guarantee the good operation of the equipments of the plant, to maintain the tightness of the cells and buildings, to process the waste in line and quickly, and to train all the workers in the plant to reach excellent exploitation in normal and incidental cases.

IV.2. Waste disposal

In the closed cycle, all the materials produced by fission are extracted and treated according to their nature, risk and value.

All the waste produced are processed according to their nature and incorporated in glass, bitumen or concrete, in order to be temporarily or definitely stored.

Plutonium and uranium are reintroduced in the cycle.

The main problem which has to be solved is the answer to the following questions : Is it possible to find a solution for final disposal of long life nuclei ? Is it possible to establish that a special confinement (glass, concrete etc...) in a chosen geological environment will be safe during the thousands of years which correspond to the radioactivity contained in the wastes.

The question is studied thouroughly all around the world. It does not raise immediate concern. No doubt that in the future decades there will be an agreed technical solution.

IV.3. MOX fuel fabrication and reprocessing

The reintroduction of plutonium coming out from reprocessing in the fabrication line of reactor fuels introduces some changes in the safety analysis of fabrication and reprocessing.

- In the fabrication line the new risks are linked to the presence of plutonium which imposes the utilisation of tight confinement (glove boxes), strict α control of α contamination, and separation of the steps of the process in specialised cells, which help to control dissemination of radioactive materials in case of incidents.

- In the future, the greatest problem of the fabrication of recycled fuel will come from the irradiation risks induced by the transuranium nuclei (Am 241, Pu 238 etc...) which will be abundant in the plutonium coming from PWR fuels reprocessed in reprocessing plants around the world.

The Mox fabrication plants will need more shielding and automatisation than the existing fabrication plants for PWR fuels.

- The introduction of MOX fuels in reprocessing plants has not raised major problems. The questions of solubility of the fuels , of criticity linked to the higher Pu content, of the higher transplutonium content and of the higher neutronic emission of the fuel, have been studied and solved for the existing plants without major difficulties.

IV.4. Radioactive material transportation

The cycle includes many technological steps, which implies uranium, uranium compounds, plutonium and fission products, which circulate from one point to the other.

This is done safely now since decades, on road, rail, and sea.

The transport industry has designed and demonstrated the strength and tightness of many containers adapted to all the materials to be transported through the cycle, in a variety of possible acidental situations (collisions, falls, fires etc...).

There is no doubt on the safety of transportation.

One must care anyway about the importance of the absolute safety of this part of the cycle, because it is the most "media-sensitive" one, especially when associated with the risk of "diverting" fissile material and the non proliferation questions.

V - GENERAL CONCLUSION

The establishment of nuclear energy demands the establishment of several industrial activities in support of the reactors themselves.

Those activities imply conversion and enrichment of uranium, fabrication of fuel, and, in the case of the closed cycle, the reprocessing of irradiated fuel and the reintroduction of uranium and plutonium in the cycle.

Careful examination of the safety questions induced by the cycle shows that they are less important than the safety problems of the reactors themselves ; and can be mastered through normal sound and careful industrial practice.

In the future, one can foresee some general trends in the technology of the cycle :

a) introduction of plutonium in the fabrication activities. This does not introduce major changes in the safety analysis.

b) reduction of the release of effluents from the reprocessing plants. This imply in particular careful in line treatment of the wastes.

c) general efforts to solve the problems raised by long term storage of high activity-long life wastes.

ACKNOWLEDGEMENTS

The author is greatly indebted to those who have accepted to help him and to review this paper, namely :

Dr. Takashima from Institute of Research and Innovation, JAPAN

Mr Boehm from KFK, GERMANY

Mr Allardice and Tanner from BNFL, UNITED KINGDOM

Mr Rougeau from COGEMA FRANCE

MMr Devillers et Puit from CEA-IPSN, FRANCE

SAFETY ASPECTS OF THE IFR PYROPROCESS FUEL CYCLE

R.J. FORRESTER*, M.J. LINEBERRY*, I. CHARAK**,
J.H. TESSIER**, C.W. SOLBRIG*, J.D. GABOR**

*Argonne National Laboratory-West,
Idaho Falls, Idaho

**Argonne National Laboratory,
Argonne, Illinois

United States of America

Abstract

The Argonne National Laboratory Hot Fuel Examinations Facility-South (HFEF/S) located at the Idaho National Engineering Laboratory was designed more than 30 years ago to remotely reprocess and refabricate fuel elements for the Experimental Breeder Reactor-II (EBR-II). It is currently being modified and will be equipped with newly developed equipment to reprocess and refabricate EBR-II fuel elements that are a key part of the DOE Integral Fast Reactor (IFR) Program. This paper deals with the safety aspects of operating the HFEF/S as a major development facility in the IFR program.

Facility modifications presented a great challenge to the analysts and designers since DOE required that such modifications meet current industry and DOE standards. One major result of this requirement was the design of a new safety-grade argon cell exhaust system that will assure that all accidental radionuclide releases from that cell are first filtered. Another significant effort was associated with seismic analyses required to assure the basic integrity of the structure following a design basis earthquake, even though the original facility was designed for minimal earthquake resistance using conventional building codes.

A spectrum of credible accidents of varying likelihood was analyzed in order to estimate potential accidental radionuclide releases to the environment and assess their consequences to the public and facility workers. All such accidents were shown to have negligible consequences when credits for mitigative features are applied.

Finally, criticality safety has received considerable attention. The project is attempting to design process equipment and procedures so that criticality-safety goes beyond current DOE and industry standards for highly-

shielded operations. Project efforts are being directed toward ensuring that a criticality event is incredible. Nevertheless, the consequences to the public of an accidential criticality were evaluated and shown to be negligible.

This paper addresses the important safety considerations related to the unique Integral Fast Reactor (IFR) fuel cycle technology, the pyroprocess. Argonne has been developing the IFR since 1984. It is a liquid metal cooled reactor, with a unique metal alloy fuel, and it utilizes a radically new fuel cycle. An existing facility, the Hot Fuel Examination Facility-South (HFEF/S) is being modified and equipped to provide a complete demonstration of the fuel cycle. This paper will concentrate on safety aspects of the future HFEF/S operation, slated to begin late next year. HFEF/S is part of Argonne's complex of reactor test facilities located on the Idaho National Engineering Laboratory.

HFEF/S was originally put into operation in 1964 as the EBR-II Fuel Cycle Facility (FCF).[1] From 1964-69 FCF operated to demonstrate an earlier and incomplete form of today's pyroprocess, recycling some 400 fuel assemblies back to EBR-II. The FCF mission was then changed to one of an irradiated fuels and materials examination facility, hence the name change to HFEF/S. The modifications consist of activities to bring the facility into conformance with today's much more stringent safety standards, and, of course, providing the new process equipment. The pyroprocess and the modifications themselves are described more fully elsewhere.[2],[3]

The HFEF/S consists primarily of two hot cells (air and argon atmosphere cells, Fig. 1), a contaminated equipment wash/repair area (Fig. 2), support areas, and associated equipment. Fuel assemblies are received from the EBR-II reactor in an inter-facility shielded cask which is transported through an airlock (Fig. 3) that connects the reactor and the hot cells. In the air cell, fuel assemblies are dismantled into individual fuel elements, and are then transferred through a small air/argon lock to to the argon cell. The following operations all take place within the argon atmosphere cell: fuel element chopping, high temperature (500°C) electrorefining, distillation of cadmium and salts from the electrorefiner product, fuel injection casting, processing of the cast fuel rods into finished rods, and reassembly of the new fuel rods, new cladding, and fuel assembly hardware into a new fuel assembly. Operations in the air atmosphere cell are limited to only those with fuel having intact cladding, i.e., disassembly and reassembly of fuel assemblies containing 61 individual elements.

Both HFEF/S hot cells are surrounded by operating areas that are served by an exhaust ventilation system that is separate from the hot cell ventilation exhaust and off-gas systems. This results in a minimum of two separate confinement barriers. The hot cell atmosphere pressures are maintained negative with respect to the operating areas to prevent the backflow of contamination. In addition, all ventilated areas containing loose contamination are provided with high efficiency filters at ventilation inlets. The argon cell is cooled with recirculated argon that is refrigerated in the out-of-cell portion of recirculation loops. There are two such cooling loops each with a flow rate of 4.72 m^3/s. The loops contain High Efficiency Particulate Attenuation (HEPA) filters. Since the volume of the cell is 1870 m^3, the atmosphere volume is exchanged every 6.6 minutes; therefore, the filtration in the cooling loops maintains suspended particulates in the argon

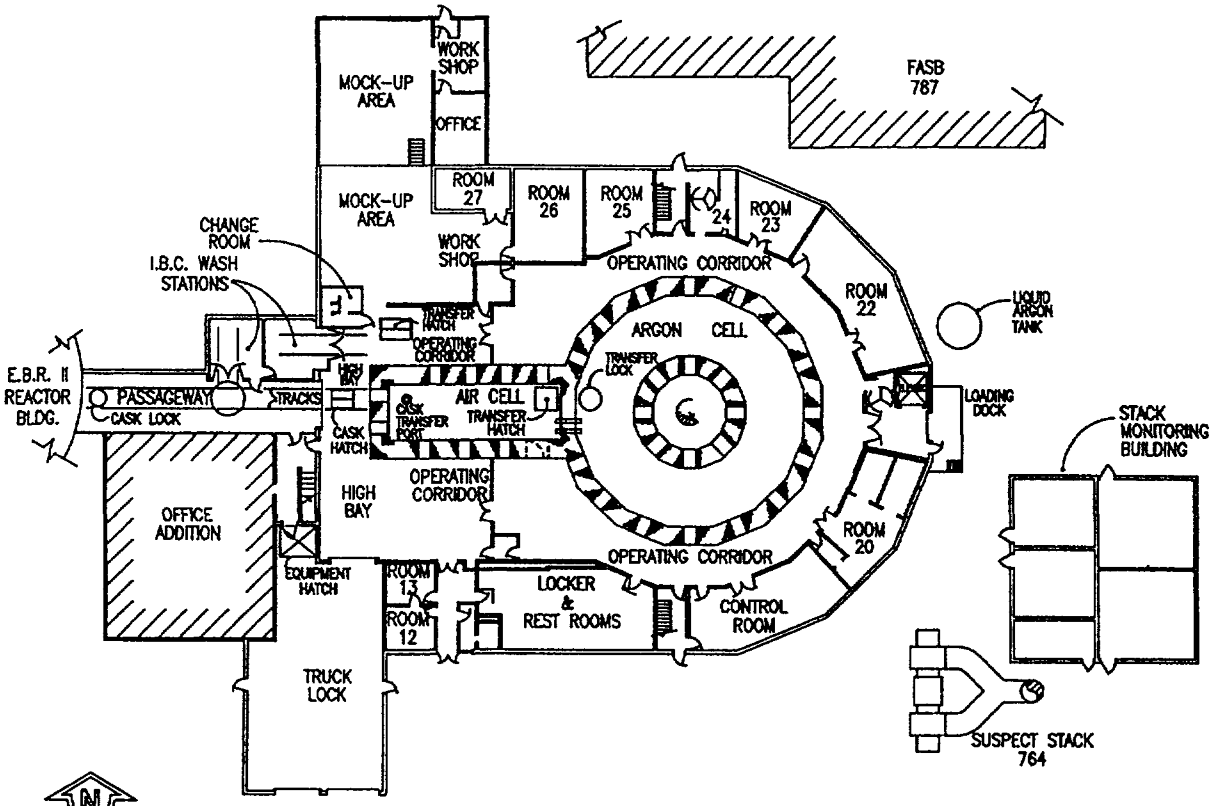


FIG 1. HFEF/S operating floor plan with conceptual modifications.

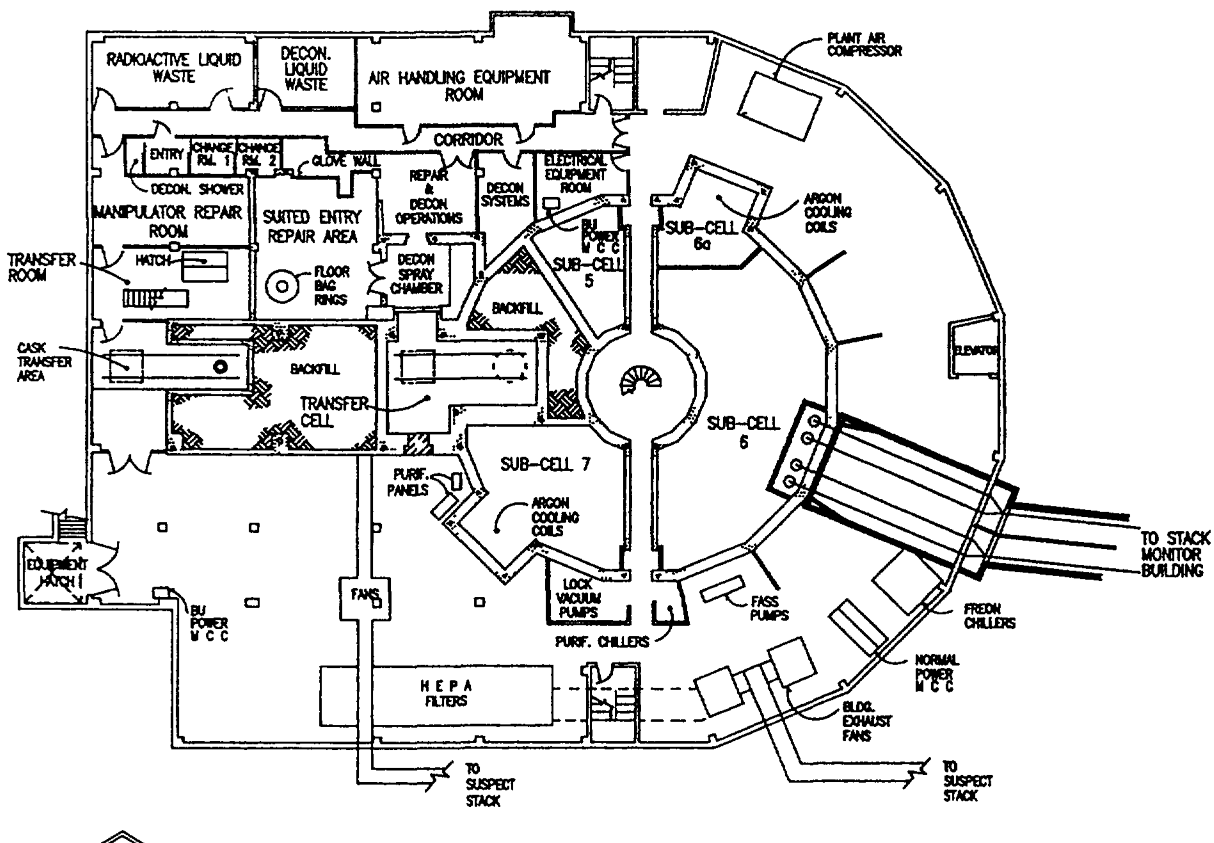


FIG. 2. HFEF/S basement floor plan with conceptual modifications.

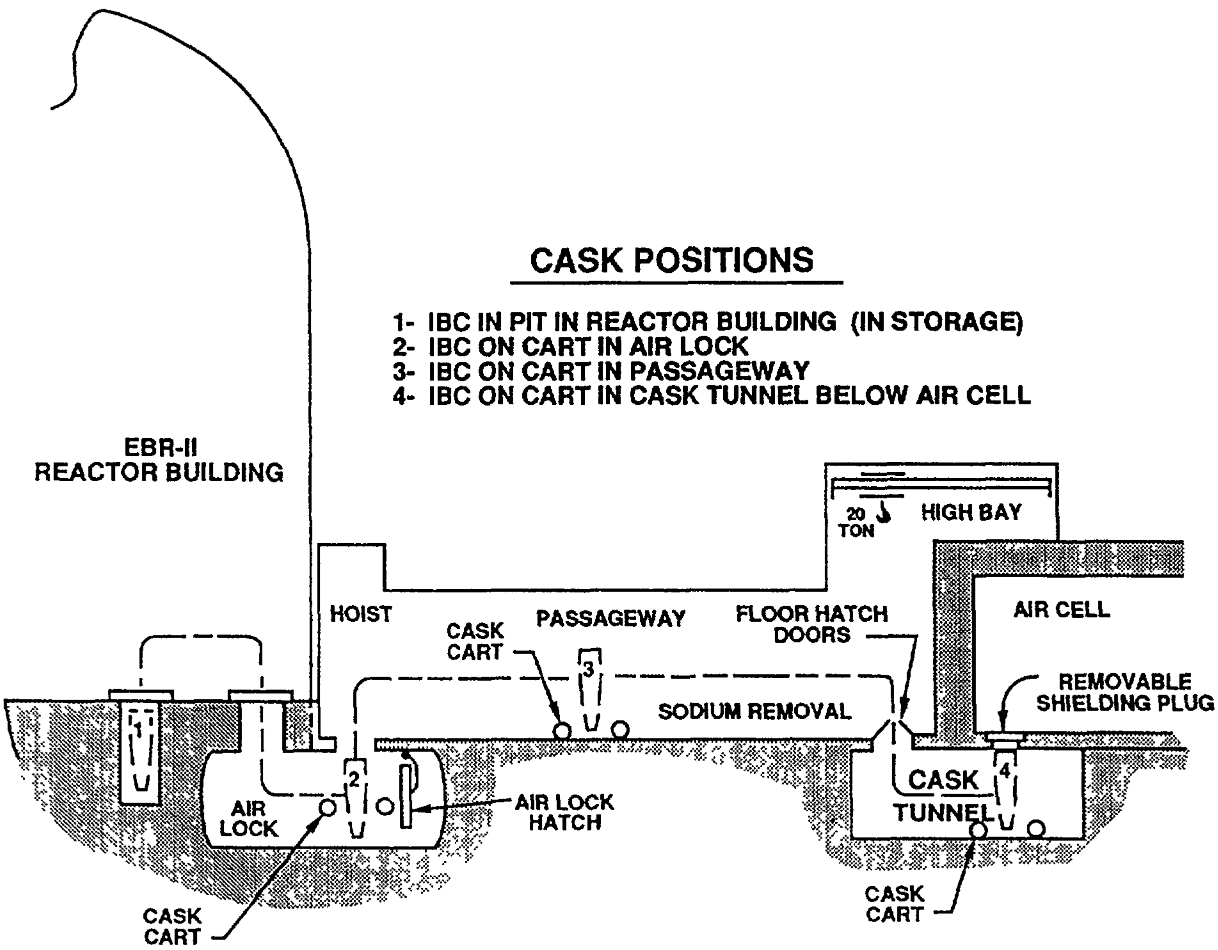


FIG. 3. Interbuilding fuel cask transfers.

cell atmosphere at very low levels. This is important in minimizing the particulate release that accompanies a small purge of argon atmosphere necessary to control nitrogen levels for fuel reprocessing.[1]

Modifications to the HFEF/S facility are being conducted in accordance with the earlier draft versions of the Department of Energy (DOE) general design criteria manual[4], the codes and standards guide developed by the Brookhaven National Laboratory (BNL)[5], and the mandatory DOE standards.[6] Earthquake analyses of the cells, foundations, and building, i.e., the new hot repair area and other critical items, have been, or are being conducted by dynamic methods using the finite element ANSYS code.[7] Department of Energy-sponsored guidelines for site-specific natural phenomena[8] are being utilized in this effort. Although the HFEF/S facility is presently classified as moderate hazard under DOE guidelines for hazard classifications, it is being modified in accordance with high hazard natural phenomena guidelines. The design basis earthquake has a zero-period asymptotic acceleration of 0.21g. The design basis wind is 42.5 m/s.

[1]Any air ingress to the argon cell has oxygen removed in a O_2-H_2 catalytic combiner, nitrogen is untreated. To control nitrogen buildup, the argon cell atmosphere is continuously purged with a small flow of fresh argon.

The HFEF/S hot cells were originally analyzed by static methods, and with less severe earthquake accelerations than presently required for nuclear facilities. It has been necessary to reanalyze their seismic performance using dynamic analysis methods, as now preferred by the DOE. These new analyses have shown that the basic structural integrity of the cells and their foundations are adequate. However, it is not practical, and might not be possible, to show that the argon cell remains leak-tight following occurrence of the design basis earthquake. This has resulted in a requirement for the installation of a Safety Exhaust System (SES), to maintain adequate inward flow through any breaches that might occur in the cell boundary. This special exhaust system (Fig. 4) is being designed to applicable safety-class standards.

Following a postulated breach in the HFEF/S argon cell boundary the SES must maintain particulate capture velocities (>0.635 m/s) across the breach area. To assure this capability under the accident condition of a cell boundary breach and subsequent in-cell metal fire, the exhaust system must remove cell atmosphere at a rate that provides this minimum flow, in addition to removing cell atmosphere at a rate that accommodates expansion of cell gas due to heatup (i.e., from the sensible heating effects of the in-cell metal fire, radioactive decay of fuel and waste in storage, and heat transfer from the cell liner). In evaluating sources of heat and their potential to cause atmosphere expansion, it is not necessary to consider continued electric power input to the furnaces or cell lighting, since they are to be automatically disconnected from the power source when the argon cell pressure rises.

The HFEF/S will contain a "hot repair" area in the basement, with two confinement levels, in which equipment can be washed/decontaminated and subsequently repaired, either by suited-entry hands-on maintenance, or by use of a glove wall to protect the operator from excessive radiation exposure. All contaminated waste water from washing (and all other minor streams of contaminated water generated in the facility) are evaporated so that no contaminated liquid waste will be released to the environment.

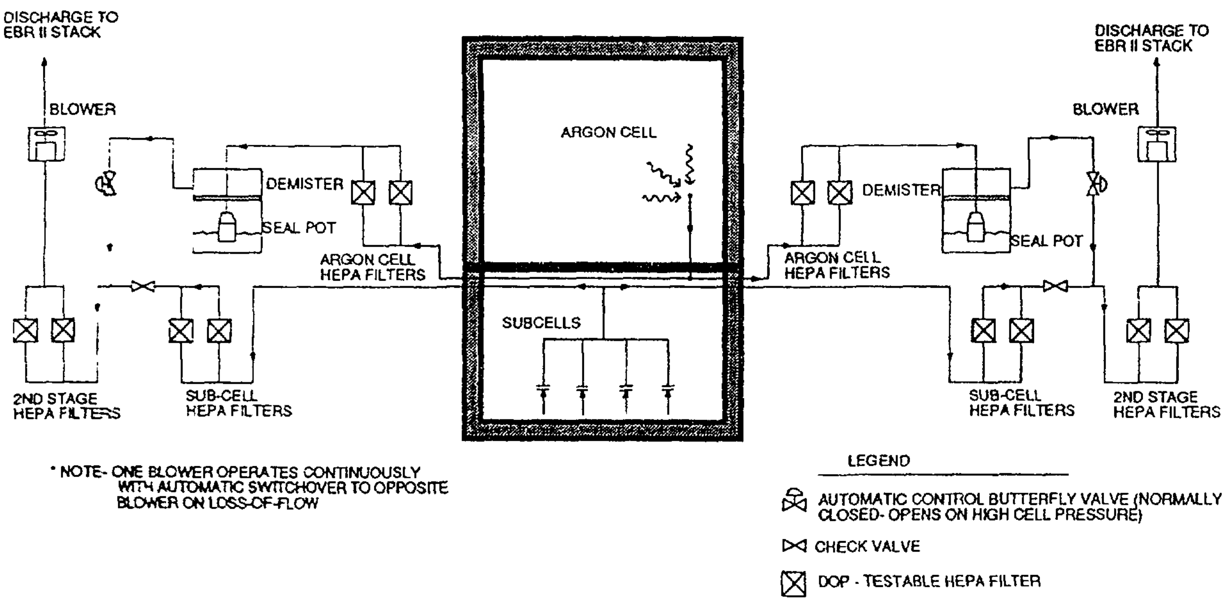


FIG. 4. Simplified conceptual schematic of argon cell exhaust system.

Fuel assemblies, both prior- and post-processed, may be stored in cylindrical holes or "pits" in the floor of the air cell. Waste cans are stored in similar pits in the argon cell.

Passive safety in the HFEF/S facility has been a primary objective. The protection provided personnel by the highly shielded hot cell walls, natural-circulation/radiation coolability of all fuel and waste in storage, natural-circulation/radiative cooling of fuel assemblies if forced cooling is lost, and finally passive cooling of process equipment such as the electrorefiner (even if argon cell cooling is lost) are major aspects of passive safety. The passive cooling of waste cans, located in the pits in the argon cell is a particularly difficult requirement to address. The desire to maximize heat in the can, in order to minimize storage volume, requires accurate heat transfer analyses under conditions which are difficult to analyze; conditions of combined natural convection and radiation. The can, when removed from the argon cell, must also be able to meet acceptance criteria of a local temporary dry-tube storage facility. These acceptance criteria also impose a passive cooling requirement that cadmium metal wastes remain in a solid state, which places additional constraints on the waste can design.

To ensure passive cooling when received in HFEF/S, an EBR-II fuel assembly must be cooled approximately 100 days or longer for the anticipated fuel burnup. This cooling period will also allow adequate time for decay of the Iodine-131 and other short-lived fission product contributors to accidental radiological doses. The primary remaining gaseous radioisotope is Kr-85. Initial plans were to collect a portion of the Kr-85 gas at the fuel chopping station at time of fuel element puncturing. In addition, a recovery system was planned for Kr-85 released to the cell atmosphere. Subsequent analysis has established that the Kr-85 radiological doses are sufficiently low, for the approximate 3.7×10^{14} Bq annual normal release, that the recovery of Krypton is unnecessary. Therefore fission gas recovery is being treated only as a desirable option, to be implemented as a demonstration after initial startup if funding is available.

The basic process hazards that have been identified in HFEF/S are similar to those that would be found in a future commercial IFR-type facility -- although the method of mitigation may differ because of the difference in confinements. Preliminary analyses were conducted without credit for mitigation features. This allowed direct comparison with accident dose limits, to determine whether or not safety-class mitigation systems were required.

The events that lead to site-boundary radiological dosages are described below.

Fission Gas Release Due to Loss of Cell Atmosphere

There are several events that might lead to abnormal release of fission gas. These are:

1. Over-pressurization of the argon cell due to loss of cell cooling and subsequent heatup of cell atmosphere, with the pressure buildup relieved by activation of the safety exhaust system.

2. Over-pressurization of the argon cell due to failure of the controls for the normal argon supply (a large dewar containing 2.6 cell volumes of argon).

3. Over-pressurization of the argon cell due to failure of the controls for the emergency argon supply (a bottled supply containing 0.033 cell volumes of argon).

Although detailed analyses of each event are being performed, the radiological consequences of all the above events can be "bounded" by a hypothetical event in which all cell atmosphere is released. Radiological consequences are shown in Table I. For this accident and in the following accident discussions, site boundary doses are evaluated at the point of nearest boundary location with respect to the facility, a distance of 5000 m from the facility. Meteorlogical dispersion parameters were derived from Regulatory Guide 1.145.[9] In preliminary analyses all doses were evaluated for a ground level release, even though the release would actually be at the 61-meter stack exhaust point. The calculated meteorlogical dispersion factor is 2.1×10^{-3} s/m^3.

Fission Gas Release from Kr-85 Recovery System

Although the HFEF/S project does not intend to install a fission gas recovery system for initial operations, an accident in this system is included because of possible future installation, and its possible application to commercial concepts. For this accident, it is assumed that Kr-85 has been collected into a bottle over a period of one year and that during changeout the bottle is dropped, possibly resulting in valve failure. This results in a release of approximately 3.7×10^{14} Bq.

Metal Fire in Argon Cell

The processing of hot metals in the argon cell leads to the possibility of spontaneous ignition and a metal fire if sufficient air leaks into the cell. An initiator of this event is loss of inert atmosphere due to an earthquake-related breach in cell boundary. As previously discussed, the SES is being installed as a safety class system to filter any airborne particulate products that result from this postulated event. In addition, as a "defense-in-depth" measure, confinements for individual process furnaces are being designed to survive a design basis earthquake.

A load drop from the in-cell crane onto the large equipment transfer lock in the floor of the argon cell might be another initiator of this event. In HFEF/S, the use of this lock for potentially damaging loads is to be limited to times when hot metals are inside the process confinements.

Failure of a floor penetration is considered another possible initiator of a metal fire. There are many small flanged penetrations for electrical and other services that penetrate the cell floor. Although these penetrations are passive and rugged, it is considered possible that an operator mistake, during changeout of a service, could cause an inadvertent opening into the cell. In addition an earthquake might result in an unevaluated failure mode in these penetrations.

In preliminary analyses, both large and small breaches of the HFEF/S argon cell boundary were analyzed. Failure and complete opening of the argon cell large equipment transfer lock (1.83 m diameter) in the floor of the cell was assumed for the large breach. Failure and complete opening of a 0.126 m diameter penetration of the cell boundary was the assumed small breach.

A chopped fuel batch containing 10 kg of heavy metal was assumed to be exposed and burned as a result of the ingress of air into the cell. The remainder of the hot fuel was assumed to be inside process confinements. The assumed chopped fuel composition prior to irradiation was 71 w/o U, 19 w/o Pu, 10 w/o Zr. The accident sequence involves initially inertia-dominant slug flow through the breach due to the density difference between the argon cell atmosphere and the ambient atmosphere. The cell pressure therefore began to rise. At -25 mm wg differential pressure, the cell safety exhaust system began to operate and exhausted at a rate of 0.236 m^3/s.[1] The modeling predicted that, for the large diameter breach, the time to reach atmospheric pressure in the cell was a very short time (less than one second). For the large breach, the time to reach 4% oxygen concentration in the cell, i.e., an amount that might support combustion of hot metals, was estimated to be about 3 minutes; whereas for the small breach this time was estimated as 25 minutes.

The relationship between burning rate and oxygen concetration was based on the data of Baker and Fischer[10] for ternary U-Pu-Mo alloy. Once burning is established, the rate of burning would be controlled by oxygen diffusion through the oxide layer that is formed. The burning rate is therefore dependent upon the partial pressure of oxygen, the diffusion coefficient for the layer of oxide buildup on the surface of the fuel, and the temperature of the layer. Assuming diffusion through a porous oxide layer, so that the diffusion is described by Knudson flow, the diffusion coefficient[11] is taken as proportional to the one-half power of the average oxide layer temperature.

The heat transfer coefficient in the oxide layer was taken as constant, dominated by conduction, and not by gas convection. This coefficient was empirically derived. For these preliminary analyses some additional assumptions were necessary, the most important of which are listed in the following.

1. No credit was taken for heat transfer to the cell boundary or to cell equipment.

2. Air/Oxygen was assumed to have access to the interior of the bed of chopped fuel (pellets) so that burning was uniform through the pellet bed.

3. The burning surface area was assumed constant and taken as the exposed ends of the chopped pins in their container.

With these assumptions, it was found that for the large and small breach approximately 70 and 130 minutes, respectively, would elapse before complete oxidation of the 10kg fuel batch.

The transient temperature of the cell atmosphere was calculated using an energy balance that included the effects of the addition of heat due to the burning of the fuel, the energy input and output from the cell due to air exchange, and the enthalpy increase of the cell atmosphere. The temperature transient, from initial to maximum, was less than 30°C for the most conservative (large breach) case. This transient poses no significant stress on the cell confinement.

For radiological dose calculations, an airborne fractional release of 0.0005 (from the fuel) was assumed for plutonium and solid fission products.

[1]This was the design flow rate at time of these preliminary analyses. The flow rate in the latest safety exhaust system design has been increased by about a factor of 3.0 in order to maintain particulate capture velocities across assumed breaches in cell boundary.

This was based on measurement.[12,13] For consistency with previous HFEF safety analyses,[14] cesium was assumed to have a fractional release of 0.35, conservatively high compared to a more recently recommended value of 0.01[15] for volatile fission products. Credit for fallout/plateout was conservatively taken as a factor of 0.5. Because of the greater-than-100 day fuel cooling time, the iodine and xenon inventories are negligible.

More detailed transient analyses are planned for the Final Safety Analyses. The unmitigated radiological doses from preliminary analysis of this metal fire event are summarized in Table I. In final safety analysis, credit will be taken for the safety-class filtration of aerosols, to be provided by the Safety Exhaust System. This will reduce calculated radiological doses by several orders of magnitude.

Wastecan Spill or Meltdown

Although the issue of a wastecan meltdown in the argon cell is minimized by the presence of the argon atmosphere, these cans must eventually be transferred into the air cell for loading from a port in the floor into a cask, with subsequent transport to an acceptable storage facility. The hypothetical consequences of a dropped can was addressed. It was assumed that the can was dropped in a manner that results in loss of can confinement, possibly by can damage or by loss of passive cooling capability.

Two general types of radioactive wastes are to be produced by the IFR processes. These are 1) metal wastes and 2) salt wastes. These wastes are produced primarily by the electrorefining and cathode processing operations. The metal wastes are primarily cathode and anode wastes (cadmium and fission products), and the salt wastes derive from the electrolyte. The salt contains the more active fission products (e.g., rare earths) and the metal waste contains primarily the noble metal fission products dispersed in a cadmium metal matrix.

The fission product contents of one subassembly were assumed to be contained in the cans, along with 1% of the heavy metal. The results are easily extrapolated to a higher can loading by estimation of the number of subassemblies processed per waste can. The one-subassembly loading corresponds approximately to the decay heat limit imposed at the assumed waste repository. Further refinement of can loading was not warranted due to the conceptual nature of the process the time of the analyses.

Release fractions and meteorlogical dispersion parameters assumed for this accident were the same as discussed previously for the argon cell metal fire. The calculated unmitigated radiological dose from this preliminary analysis is shown in Table I.

Meltdown of Fuel Assembly in a Storage Pit

At the time of preliminary safety analyses, it was planned that only post-processed fuel assemblies would be stored in the air cell floor pits. Pre-processed assemblies, which have a much higher heat load, were to be stored in racks on the air cell floor to allow for passive cooling by radiation and natural convection. Each floor pit can accept four post-processed fuel assemblies. This accident assumes that a single pre-processed fuel assembly is mistakenly placed into a pit that contains three freshly processed assemblies. The heat load from the "hot" assembly is assumed to cause melting and/or a metal fire in all four assemblies. Based on results of recent experiments performed a EBR-II in which flow was stopped to a subassembly contained inside a shroud, this accident might be eventually classed as incredible. Nevertheless, the preliminary analysis is summarized here, with-

TABLE I

Major Accidents Considered for HFEF/S Facility
and Site Boundary Radiological Dose
from Preliminary Analyses

Accident Descriptors	Radioactive Source	Unmitigated Radiological Dose at Site Boundary, Sv	Mitigation Features Available, But Not Credited[a]
Fission Gas Release			None
• All of cell atmosphere	<2.52×10^{13} Bq, Kr-85	Skin - 1.3×10^{-5} EWBE[b] - 1.3×10^{-7}	
• Fission gas bottle	3.61×10^{14} Bq, Kr-85	Skin - 2.2×10^{-4} EWBE - 2.1×10^{-6}	
Metal fire in argon cell	10 kg heavy metal burned	• large breach - 5×10^{-3}, EWBE • small breach - 7×10^{-4}, EWBE	SES Filters
Waste can spill or meltdown	Fission product content of one fuel assembly	• cadmium waste - ~0.0, EWBE • salt waste - 2.7×10^{-3}, EWBE	Air cell exhaust filters
Placement of pre-processed fuel assembly in storage pit	One pre-processed, three post-processed fuel assemblies	9×10^{-5}, EWBE	Air cell exhaust filters
Wastebox fire	3700 Bq (alpha) per gram of wastebox material	2×10^{-6}, EWBE	Air cell exhaust filters
Criticality[c]	1×10^{18} fissions	1×10^{-4}, EWBE	

[a]Will be credited in final safety analysis.

[b]EWBE - Effective Whole Body Equivalent, 50-year dose commitments, based on ICRP-30[15] techniques.

[c]Beyond-design-basis accident; credit taken for exhaust HEPA filters.

out regard to the probability of occurrence. The assumed release fractions for this accident were the same as for the in-cell metal fire previously discussed, with one exception. The exception is that the effects of local fallout/plateout inside the storage pit were credited in the overall release fraction. A local (pit) confinement release fraction of 0.01 was assumed, based on assumptions from similar, previous HFEF/S safety analyses[14] in which data from aerosol tests sponsored by the Atomic Energy Commission were utilized. The unmitigated radiological doses are reported in Table I. It should be noted that an existing mitigation system, the air cell exhaust system, a highly reliable system with two stages of high efficiency particulate attenuation filters, was not credited for these preliminary analyses.

Wastebox Fire

Miscellaneous contaminated wastes removed from the hot cells and items such as polyethylene sheeting, wipedown rags, boots, etc., are used in the hot repair facility are collected in large (1.2 x 1.2 x 2.4 m) wooden boxes. The wooden box structure, although painted with fire resistant paint, leads to the postulate that a box could be involved in a fire. The alpha curie content of these boxes is limited to 3700 Bq per gram of material; consequently the box can be disposed of as non-transuranic waste. In addition, the fission product content of the box is limited to an amount such that a dose rate of 5 mSv/h at 1 m from the box surface will not be exceeded. The assumed accident involves complete burning of the box when loaded to the limit of both alpha and gamma activity. Calculations indicate that the fission product radiological dose would be negligible compared to the dose from the transuranics. The fractional release of transuranics from the box was taken to be 0.0005 of the of the box contents, as assumed for non-volatiles in similar analyses.[16]

Dispersion and meteorlogical assumptions were the same as for the in-cell metal fire. The calculated unmitigated radiological dose is summarized in Table I. It should be noted that a mitigation system, the air cell exhaust system, which includes two stages of HEPA filtration, will protect against the effect of this accident; even though the unmitigated radiological doses are very small.

Facility Fires and Explosions

IFR fuel processing involves the handling of metals; there are no organics or solvents used in, or required to support the process. This results in mimimum concern regarding fires in facility processing or storage areas.

The facility is constructed primarily of concrete and steel and therefore most portions are considered non-combustible. However the DOE is presently applying "improved risk" insurability criteria, based largely on monetary value rather than a detailed analysis of the potential for a large fire. These criteria, applied in this manner, would require a full facility wet-pipe sprinkler system, except in inerted areas. The HFEF/S modifications project is installing such systems in all areas in which any significant combustible loading is anticipated, and where criticality is not a consideration. This will result in fire-sprinkler protection for essentially all areas of the facility except the hot cells.

The only identified potential for a significant explosion, from preliminary analysis, was in the argon cell atmosphere purification system. This system is installed to remove oxygen impurities from the cell atmosphere. A small, substoichometric flow of hydrogen gas is combined with a small flow of argon atmosphere in the presence of a palladium catalyst. Water vapor is formed and collected in dryers. The presence of hydrogen leads to the possibility of leakage due to pipe or joint failure. Of particular concern is the possibility of an explosion during hydrogen supply bottle changeout. To alleviate these concerns supply bottles are being relocated outside the facility, and a system is to be installed to detect supply line failure and to isolate the line if such failure occurs. In addition, the supply line is being routed within a secondary pipe and the annulus between the two pipes will be vented to a highly reliable exhaust system.

Another possible explosion potential arises from the current concept of a fission gas recovery system. Recent design studies for HFEF/S have established that, if installed, this system should have a cryogenic distillation column, as presently used on the EBR-II fission gas recovery system. The cryogenic column introduces some potential for ozone collection and explosion, although more studies are required to evaluate this potential. These studies are presently inactive due to the decision not to initially install a fission gas recovery system.

Nuclear Criticality

The IFR fuel process is basically a batch process in which the amount of fuel introduced and leaving each step can be accounted for, before placing fuel in the equipment for the next step. This reduces the concern over occurrence of criticality. Nevertheless, the project is attempting to design equipment and procedures so that no credible combination of normal or off-normal events can lead to a nuclear criticality.

A hypothetical criticality event, assumed to result from overloading of the fuel pin casting furnace, has been analyzed for HFEF/S. Analysis of this event, assumed to involve plutonium bearing fuel, uses the guidance in Regulatory Guide 3.35[17] to establish the total number of fissions (1×10^{18}) involved. It was conservatively assumed that all of the fission energy was initially directed toward vaporization of the fuel, and that the latent heat of the vaporized fuel was subsequently transferred to the argon atmosphere, due to near-instantaneous fuel condensation. The result was an over-pressure of approximately 7000 N/m^2 in the argon cell. This pressure would be passively relieved through a seal pot and two stages of HEPA filtration in the safety exhaust system. Because of the previously-discussed project efforts toward rendering a criticality event incredible, criticality has been initially treated in HFEF/S safety analysis as a Beyond-Design-Basis-Event, with protective/mitigative features. Release from cell-to-atmosphere was taken to be identical to fractional cell atmosphere release under assumption of uniform mixing. For these initial analyses, 100% of the fission products was assumed to be released. Radiological doses are shown in Table I.

Other Accidents

Many other accidents were considered in preliminary safety analyses, including a dropped subassembly, ventilation flow anomalies, and personnel evacuation with preprocessed fuel pins in the small equipment argon/air lock. These accidents were either benign or there was considered to be adequate time available for operator action to prevent accident progression or significant radiological dose.

One potential accident, the overheating and rupture of a fuel assembly in the HFEF/S-EBR-II interbuilding fuel transfer cask, has been addressed in previous safety analyses. Since the safety envelope providing for usage of this cask has not been significantly changed by the new program, this accident is not presently being re-addressed. However, recent experiments, in which the cooling flow to a subassembly was interrupted, point to the possibility of providing for passive fuel assembly cooling in the cask by allowing for the radioactive heat to sufficiently decay before transfer from the reactor. Further tests are planned.

A comparison of the major confinement features of a future facility, designed specifically for pyroprocessing with those of HFEF/S is given in Table II. The future facility would have several safety advantages over HFEF/S, since it would be a new facility in which modern safety-related design criteria could be more easily implemented than in retrofitting the 30-year old HFEF/S facility.

The IFR concept, although not necessarily tied to co-location of the reactor and the fuel cycle facility, offers both fuel theft and diversion

TABLE II

Comparison of Confinement Features and Hardening for Natural Phenomena-- Future Facility* vs. HFEF/S

	Future Facility	HFEF/S
Number of confinement levels	2	2
Confinement structurally hardened for earthquake?	Yes, both confinement levels	Yes, both confinement levels
Argon cell leak tight after earthquake?	Yes	No, requires safety exhaust system (SES) to maintain inflow through breaches in cell penetrations.
Confinement structurally hardened for missiles?	Yes, outer confinement provides first level allows location of critical equipment at any building level.	Yes, but relies on inner barrier (hot cells), and location of critical equipment in basement to minimize hazard.
Outer confinement structurally hardened for high winds and tornado?	Yes	Yes, but for high wind forces only-relies on site location.
Can failure of penetrations into argon cell (for support of process equipment) result in rapid loss of cell atmosphere?	No, penetrations are in top of cell -- argon is heavier than air. Also in-cell coolers are used to avoid external recirculation loops.	Yes, penetrations are below cell, in to subcells. Requires SES connection to the subcells to remove any leakage from argon cell.

*Future facility assumed to be designed specifically for pyroprocessing.

advantages when the fuel cycle building is located on-site with the reactor. Because all operations are performed with the fuel under heavy gamma-ray shielding, the diversion or theft of fuel is unattractive. Also the transportation of fuel between the fuel cycle building and the reactor is all within the site, making security protection easier.

To a large degree, the advantages of the co-located concept accrue to minimizing fuel transportation of fuel to offsite locations. This advantage is apparent in the case of HFEF/S where, if fuel were not to be processed on-site, more off-site transportation of makeup material, processed fuel, and especially of unreprocessed fuel with high heat loads would be necessary (Fig. 5).

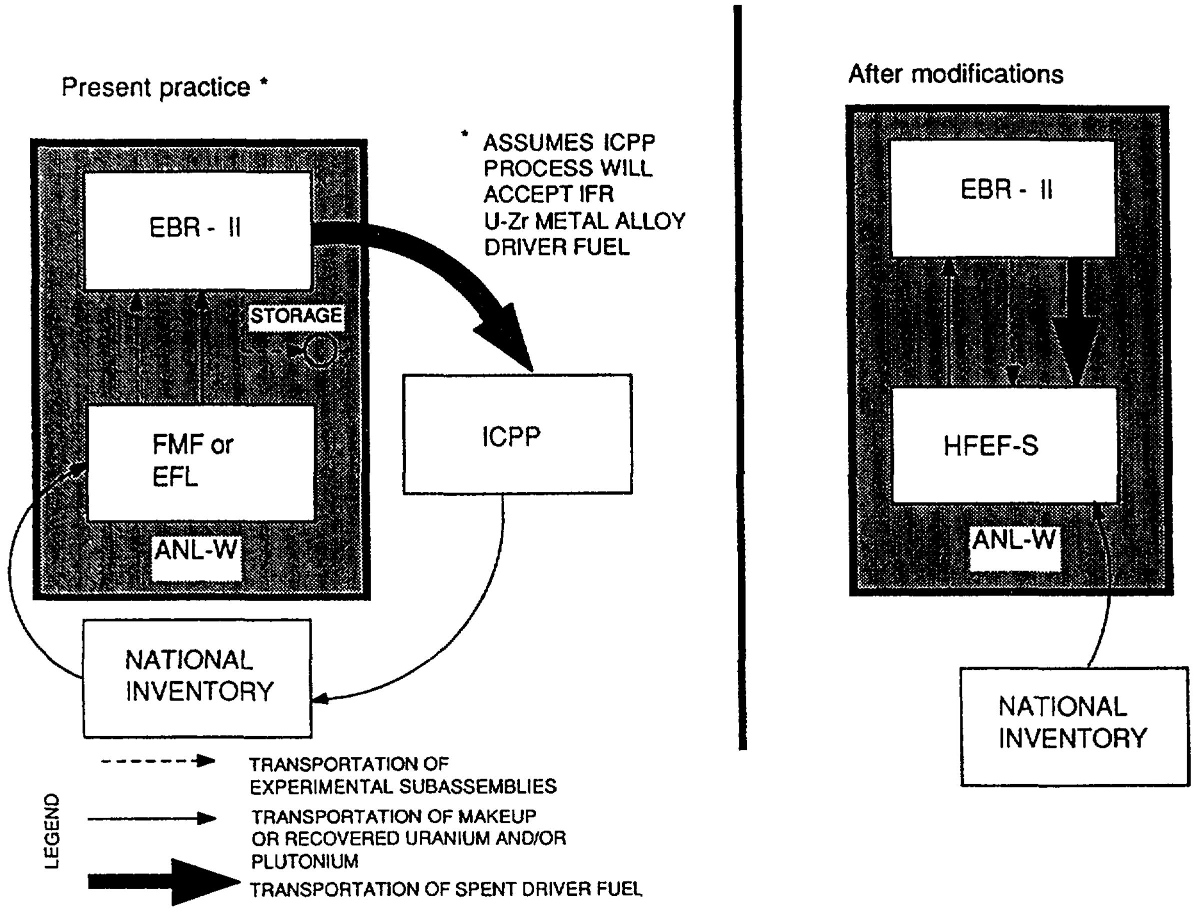


FIG. 5. Comparison of transportation requirements.

Summary

The HFEF/S modifications are being designed in accordance with the recent revisions in DOE general design criteria, including hardening against the effects of natural phenomena. Radiological doses from "unmitigated" accident releases are in the trivial-to-minor range, and likely would have been acceptable in prior regulatory eras without installation of mitigation systems. However, the most recent DOE general design criteria are invoking an "ALARA" concept to accident releases. For this reason the HFEF/S Project is installing a safety exhaust system to provide inward flow through all credible cell breaches and to HEPA filter all exhaust. It is expected that this system will allow for large reductions (a factor of at least 1×10^{-4}) over "unmitigated" metal-fire radiological doses as reported herein. Also, in final safety analyses credit will be taken for the air cell exhaust system -- a non-safety class, but highly reliable system, also with two stages of tested HEPA filtration. With the above credits it is expected that accident consequences, as related to the operation of HFEF/S modifications, will easily meet DOE regulations and "ALARA" goals.

In a future facility several of the HFEF/S design deficiencies, such as the floor penetrations, which can allow argon to drain from the cell, and the possible lack of argon cell seal following a design basis earthquake, can be easily avoided.

The co-located concept offers significant fuel theft/diversion improvements because of decreased transport of fuel offsite and the continual high radioactivity of the fuel prior to, during, and after processing. Also, the concept essentially eliminates off-site transport of fuel with high internal heat source.

REFERENCES

[1] STEVENSON, C.E., The EBR-II fuel cycle story, American Nuclear Society (1987).

[2] LINEBERRY, M.J. and PHIPPS, R.D., "A demonstration facility for the IFR fuel cycle," Proc. International Conference on Nuclear Fuel Reprocessing and Waste Management, Paris, France (1987).

[3] CHANG, Y.I., LINEBERRY, M.J., BURRIS, L., and WALTERS, L.C., A Closer Look at the IFR Metallic Fuel Cycle, Nucl. Eng. International Journal, (1987).

[4] U.S. DOE Order 6430.1A, General design criteria manual," (1989).

[5] BRYNDA, W.J., SCARLETT, C.H., TANGUAY, G.E., and LOBNER, P.R., Nonreactor nuclear facilities: standards and criteria guide, BNL 51444-Rev. 1, (September, 1986).

[6] U.S. DOE Order 5480.4, Environmental protection, safety, and health protection standards, (1984).

[7] (b) ANSYS Finite Element Computer Analysis Code, Rev. 4, Swanson Analysis Systems, Inc., Houston, PA.

[8] KENNEDY, R.P., et al., Design and evaluation guidelines for department of energy facilities subjected to natural phenomena hazards, (May, 1989) (draft no. 4).

[9] U.S. NRC Regulatory Guide 1.145, Rev. 1, Atmospheric dispersion models for potential accident consequence assessments at nuclear power plants, (1983).

[10] BAKER, L. Jr., and FISCHER, D.F., Burning Tests with Uranium-Plutonium-Molybdenum and Uranium-Plutonium-Titanium Ternary Alloys, Argonne National Laboratory Report, ANL-7225, (November, 1966).

[11] PETERSEN, E.E., Chemical reaction analysis, Prentice-Hall, Englewood Cliffs, New Jersey (1965).

[12] MISHIMA J., Plutonium release studies II, Release from ignited bulk metallic pieces," BNWL-357 (Nov. 10, 1966).

[13] MISHIMA J., and SCHWENDIMAN, L.C., "The amount and characteristics of plutonium made airborne under thermal stress," Proc. Symp. on Health Physics Aspects of Nuclear Facility Siting, Eastern Idaho Chapter Health Physics Society, Idaho Falls, (1971).

[14] COURTNEY, J.C., FERGUSON, K.R., and BACCA, J.P., "Radiological safety analysis of the hot fuel examination facility/south", Nucl. Tech., Vol. 73, (1986).

[15] ELDER, J.C., et al., "A guide to radiological accident considerations for siting and design of DOE nonreactor nuclear facilities," LA-10294-MS (January, 1986).

[16] SUTTER, S.L., MISHIMA, J., Ballinger, M.Y., and Lindsey, C.G., Emergency preparedness source term development for the office of nuclear material safety and safeguards-licensed facilities," NUREG/CR 3796, (1984).

[17] U.S. NRC Regulatory Guide 3.35, Assumptions Used for Evaluating the Potential Radiological Consequences of Accidental Nuclear Criticality in a Plutonium Processing and Fuel Fabrication Plant, Rev. 1 (1979).

[18] (b) International Commission on Radiological Protection (ICRP), Limits for Intakes of Radionuclides by Workers, ICRP Publication 30, Pergamon Press, New York (1978).

SAFETY ASPECTS OF DISPOSAL OF SPENT NUCLEAR FUEL IN SWEDEN

N. RYDELL
National Board for Spent Nuclear Fuel,
Stockholm, Sweden

ABSTRACT

The KBS-3 repository design from 1983 is used as reference in a brief review of safety aspects of spent fuel disposal in Sweden. The presentation follows the customary division of a repository system in barriers and is concluded by chapters on safety criteria and safety assessment. The strategy of the design is to reduce the impact of uncertainties about detailed geosphere properties by the use of corrosion resistant copper canisters to protect the spent fuel from contact with the groundwater for a considerable length of time and by distribution of the fuel packages in the bedrock so that temperatures in the rock always are kept below 100 C. Recent data from laboratory studies of radionuclide leaching from high burn-up fuel samples indicate that the fuel matrix alone is a highly efficient barrier against release of actinides. Practical tests made in the Stripa underground research facility with seals for boreholes and shafts gave good results. Uncertainties remain about details in the contribution of the geosphere to the overall safety of the repository system. Progress has been made in development of criteria adressing specific long term aspects such as assessment of rare, but over long time periods possible, extreme events and of exposure of man to radionuclides in the distant future. Old data are used to illustrate repository safety as no recent update has been made.

---

1. INTRODUCTION

Domestic political decisions on utilisation of nuclear power, the available geology, and Sweden´s geographical location at latitudes of recurrent glaciations have shaped the outlines and much of the details in the Swedish approach to disposal of residues from the nuclear fuel cycle. This should be kept in mind by anyone who compares own ideas and experiences with these snapshots of the state of the art in Sweden.

Safety aspects of our disposal scheme are here discussed following the customary division of the repository and its host rock in separate barriers against migration of radionuclides. The repository is, however, a combination of barriers with interactions which have to be studied in comprehensive system analyses. The results of such analyses have to be evaluated against safety criteria. These aspects are covered in the concluding sections.

2. REPOSITORY CONCEPT

It is an unprecedented requirement on the development of novel technology that its first industrial product shall function flawlessly over a virtually unlimited service period. This requirement must, however, be satisfied by our spent fuel repository, which will be sized to accomodate all fuel spent in our nuclear power programme. Our approach to this requirement was already at the outset a conservative design which minimises the impact of uncertainties on the assessment of repository performance and safety. This is exemplified by our intentions to use fuel canisters which have a very long service life as barriers against contact between groundwater and the fuel, and to distribute the fuel packages so that temperatures in the bedrock shall everywhere and at all times stay below 100 C.

The reference repository concept KBS-3 [1] and its predecessor KBS-1 were developed by the Swedish Nuclear Fuel and Waste Management Co (SKB) to satisfy requirements that HLW-disposal in Sweden shall be shown feasible. They have been submitted for generic safety approval as part of the procedure to obtain fuelling permission for new nuclear power plants. Their designs were on these occasions reviewed by Swedish and foreign experts, their safety was assessed by our nuclear safety authorities, and they were approved as feasibility demonstrations by our government.

We are also studying other repository concepts, e g the WP-Cave, and disposal methods, e g deep boreholes, but the KBS repository is the most thoroughly elaborated and is therefore here used to exemplify safety aspects of spent fuel disposal in Sweden.

Figure 1 illustrates the radionuclide source strengths per metric ton of U in the fuel and their variation over the time during which the source strength of spent fuel is greater than the source strength of U-nat ($1.8X10^{11}$ Bq/ton U). Figure 3 gives an overview of the KBS-3 repository. Figure 2 shows the design of the engineered barriers. The repository will be installed at a depth of somewhere between 500 and 1000 m in Precambrian rock.

3. FUEL MATRIX

The fuel matrix material, uranium dioxide, is a ceramic, which is also found in nature as mineral ore, often with ages of more than a billion years. The corrosion of uranium dioxide in the bedrock can thus be extremely small under favourable, i. e. chemically reducing, conditions . These favourable conditions may, however, not exist in the immediate vicinity of the spent fuel uranium dioxide surface, since radiation from the fission products and the transuranium elements may oxidize the groundwater by radiolysis once the fuel canister has been penetrated.

The corrosion of the fuel matrix and the leaching of radionuclides have therefore been studied experimentally at the Studsvik Research Centre since 1982 on samples from low and high burn-up BWR fuel and high burn-up PWR fuel. Distilled water and artificial groundwater have been used as leachants. The artificial groundwater is representative of granitic bedrock at intermediate depths - a few hundred meters. More saline groundwater which is typical of coastal sites and may be found at greater depths inland, have not yet been tried.

Results so far are encouraging [2]. The corrosion rate of the matrix appears to be controlled by the solubility of uranium which, again, is low in reducing groundwater typical for our bedrock. Radiolytic oxidation of

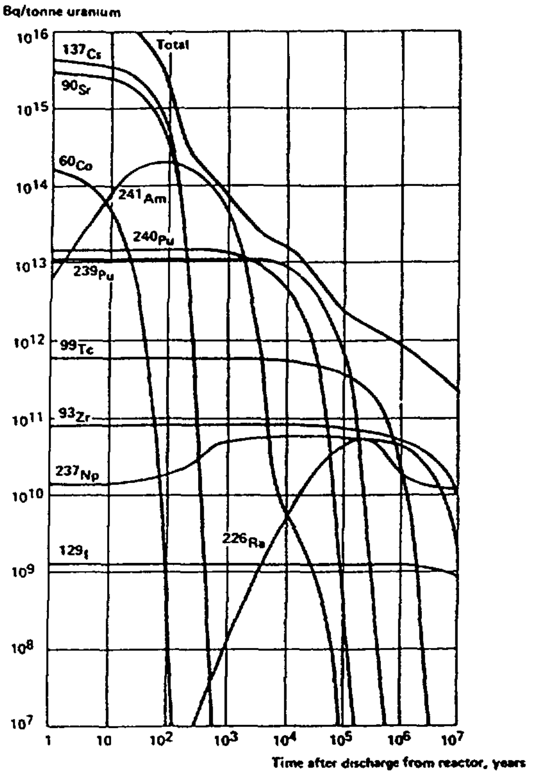


Figure 1. Radioactivity in spent fuel. Burn-up 38000 MWd/t U.

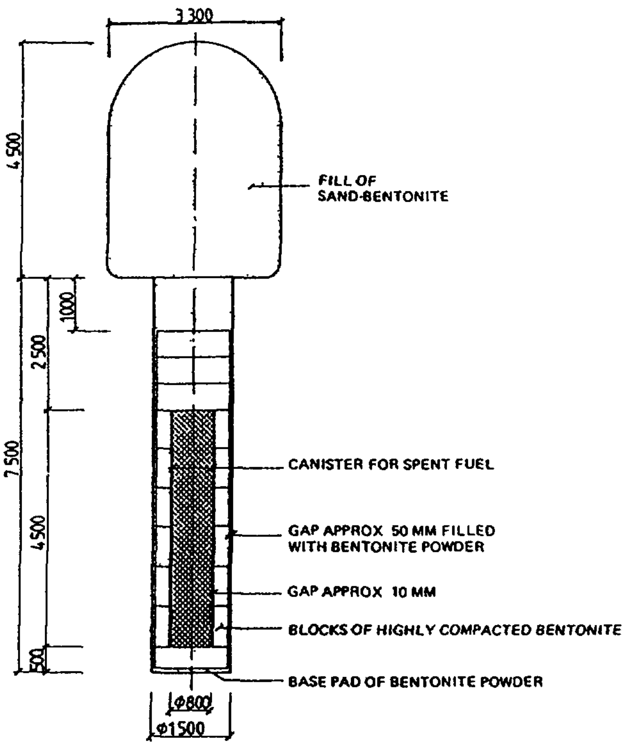


Figure 2. Deposition hole with canister and backfilling of tunnel.

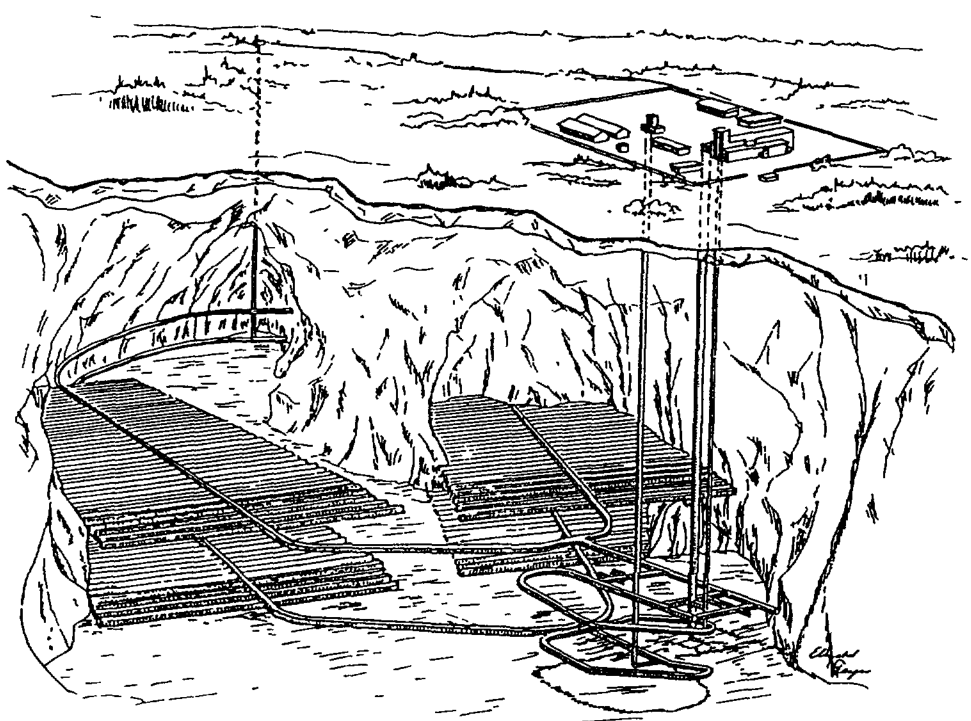


Figure 3. Tunnels and shafts in the KBS repository.

the groundwater seems not to have significant influence on the fuel corrosion. Congruent dissolution, at least of the actinides, is indicated by the results. Enhanced leaching has been observed for cesium as expected, but also for strontium and some of the refractory transition metals like molybdenum and technetium. This appears to come from enrichments at grain boundaries and other segregatory processes during in-core irradiation. The leaching of actinides has been so low in laboratory that their concentrations in the leachant would allow its use for consumption based on ALI-values for radiation workers.

These studies also aim at the development of a mathematical model of the corrosion processes. With improved understanding of leaching mechanisms also leaching in saline waters should be investigated since saline groundwaters exist at depth in coastal regions and may ingress into the repository host rock in inland locations from above or below depending on climatic variations and bedrock subsidence and rebound during the continuation of the Quaternary.

4. FUEL CANISTERS

Copper is the preferred choice of canister material since general corrosion of copper proceeds extremely slowly in groundwaters of chemical compositions which are typical in our bedrock. The earliest penetrations should be caused by pitting corrosion, but are not expected during the first several hundred thousand years as shown in an assessment by the Swedish Corrosion Institute [3]. This assessment was based on available data for groundwater composition and turnover rate in the repository and assumed a homogeneous quality of the canisters as made. The fuel corrosion should thus start at a time when the alfa and gamma radiation of the fuel matrix stems mainly from the uranium decay chains and is of similar intensity as in natural uranium dioxide ores. The subsequent penetrations should take place over a time period of similar length, and thus disperse in time any bursts of volatile radionuclides as Iodine-129 which may have accumulated in the fission gas spaces inside the fuel cans.

Design, manufacturing and quality assurance of canisters have so far only been tried for production of prototypes. The step to industrial production scale remains to be taken.

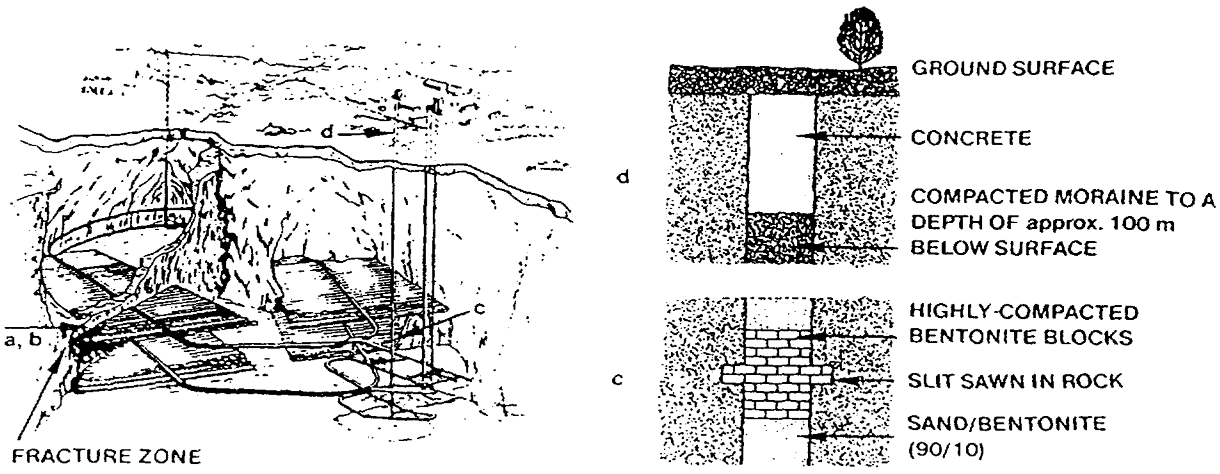
5. BUFFER, BACKFILL, AND SEALING OF REPOSITORY

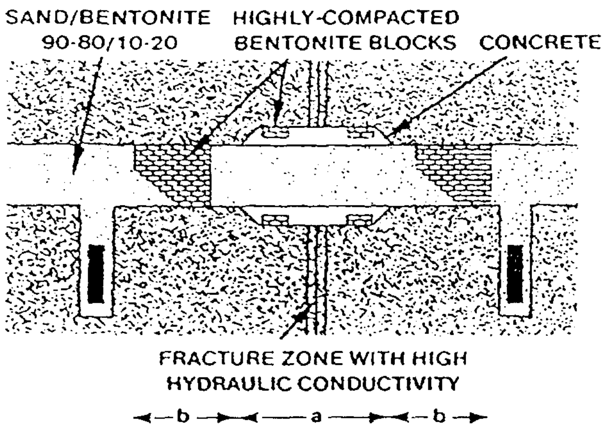
A swelling clay, bentonite, was proposed as buffer material already in the first KBS conceptual design. The buffer shall keep the fuel canisters centered in their pits, dissipate the decay heat from the fuel, restrict the groundwater flow to the canister, and protect the canister from anisotropic mechanical forces, e g due to rock movements.

Bentonite and granitic rock do not form an inherently stable chemical system. Its thermodynamics and reaction kinetics must therefore be investigated. Bedrock where bentonite, a weathering product of volcanic ash, is found has during some time of its geologic history been geothermal. Studies of bentonite ores have given insight into processes by which bentonite is transformed to a non-swelling clay. This transformation is observed only where the bedrock temperature has been above 100 C and accelerates with increasing temperature. The swelling properties of bentonite are desirable, although not vital, for the safety. Consequently the fuel will be distributed in the repository so that the temperature of the bentonite everywhere and always stays below 100 C.

The small mass of the buffer in comparison with the surrounding rock and tunnel backfill should make its influence on groundwater chemistry and radionuclide retardation correspondingly small, but its location in contact with the canisters warrants further studies of its impact on near field processes.

Bentonite will also be used in the backfill of the tunnels and shafts and to seal drillholes (Fig 4). This use of clays to prevent rapid ingress of infiltrating surface waters to the depths of the disposal area has analogues in nature. Clay fillings of fractures in hard rock are common and have often proved to be less permeable to water than the surrounding rock. Tests of tunnel, shaft, and borehole sealings by sand and bentonite and with concrete plugs for mechanical support have been made in Stripa with promising results [4].





a) Isolation of fracture zone with high hydraulic conductivity from tunnel in final repository. The tunnel permits transports during the deposition period and is backfilled after deposition has been completed in the tunnel.

b) Backfilling with plugs of highly-compacted bentonite blocks that are stacked in connection with layer-by-layer compaction and spraying of sand/bentonite mixture.

c) Backfilling of shafts with plugs of highly-compacted bentonite blocks that are stacked in connection with layer-by-layer compaction of sand/bentonite mixture.

d) Backfilling of upper part of shaft with layer-by-layer compaction of moraine and with plug of concrete.

Figure 4. Sealing techniques.

6. ROCK STABILITY AND GROUNDWATER MOBILITY

Sweden is at present a low seismicity country. There are, nevertheless, major fault scarps in Sweden which appear to have originated at the time of the deglaciation from the last ice age. Opinions differ as to the character of these events, whether they occurred as major thrusts or developed gradually. This question remains to be resolved. During the present interglacial, however, the probability is exeedingly small that the hypocenter and the fault extension of a major earthquake should hit the disposal area, provided that the repository is constructed so that it does not in itself constitute a fracture initiator.

The existence of creep motions, micro-plate tectonics, in the Swedish bedrock is more widely accepted [5]. Such creep might also be initiated by the thermal expansion and subsequent contraction of the host rock during the thermal transient around the disposal volume, or by the loading and unloading of the bedrock during an ice age. Even though major fracture zones are considered the most likely sites for these movements, some investigators do not exclude that minor fractures in the host rock of a repository could be affected and new pathways for groundwater be opened.

It is difficult, if not impossible, to map the groundwater flow pathways through our Precambrian bedrock. Therefore, in the early attempts to calculate ground water flow and transport times, the host rock was treated as a homogeneous medium with an evenly distributed permeability for water. The homogenised permeability was calculated from frequencies and permeabilities of discrete fractures observed in boreholes. An equivalent permeability calculated in this way can give reasonably correct values for the volume flow of water, but not for the water velocity in a discrete fracture, which is one of the factors determining the transport times of radionuclides once they are released from the fuel.

Models of the rock as a heterogeneous matrix for water flow are therefore being developed as complements to the homogeneous model. They are based on observations of water carrying fractures in tunnels and boreholes. A stochastic rather than a deterministic representation of the fracture system is preferred since data from fractures are at best statistically representative and since properties of individual fractures may change with time due to creep motions, weathering and sedimentation or mineralisation of weathering products.

The water velocity in a fracture is only one of the factors determining the transport times of radionuclides dissolved in the water. Radionuclides find their way into microfractures in the rock where the water is stagnant or become adsorbed on the fracture walls. Also these factors need to be considered and have to be treated on a stochastic basis due to lack of complete data.

Knowledge about the groundwater transport properties of the host rock can thus only be approximate. This may seem an essential limitation in the assessment of repository safety, since groundwater transport is the only credible mechanism - beyond human action - by which radionuclides in a repository can find their way back to the biosphere. The characteristics of the man-made barriers - the late and time-dispersed penetrations of the canisters and the low solubility of the fuel matrix - however, delay, restrict and disperse the supply of radionuclides to the groundwater in a way that reduces the sensitivity of the safety to details of the transport through the geosphere.

7. BIOSPHERE

The time scale for changes in the biosphere including the food chains to man is much shorter than for changes in the geosphere and in well selected materials in the engineered barriers. Studies have been and are made on enrichment and transfer coefficients in the biosphere of radionuclides released from nuclear power plants, but such data are of limited value to analyses of the biosphere link in the transport chain from fuel to man in the distant future.

The release of radionuclides from spent fuel is bound to be distributed over a very long time period. The dilution of the leachate from the fuel on its way to the biosphere will also contribute to ensure that radionuclides will enter the biosphere in very low concentrations. Significant radiation doses within a lifetime can only be experienced if radionuclides have accumulated over longer periods in some biosphere compartment and subsequently been mobilised by biosphere processes.

Research items of particular importance for disposal are therefore processes by which those radionuclides which reach the biosphere at all are trapped there and recirculated instead of being dispersed and transported to their ultimate sinks in the sea.

8. SAFETY CRITERIA

Safety criteria for repositories may include requirements on components of the repository system but the ultimate aim of the criteria is to limit individual radiation doses to the public now and in the future. This limit is in Sweden, as in some other countries, set at the same level as design limits for doses from nuclear power plants, in our case 0.1 mSv/a. There is a proposal for more detailed criteria, which have been worked out in Nordic collaboration. These criteria are largely qualitative and based on the criteria recommended by IAEA and on principles developed by ICRP.

The individual dose limit is difficult to apply on predicted exposures of man to radionuclides in the distant future, say during the next interglacial, when the biosphere and the nutritional habits of man may be totally different from at present. An alternative proposed by the Swedish Institute of Radiation Protection [6] is to set a limit on the predicted influx of radionuclides to the biosphere from a repository. This limit should be a fraction of the influx of radionuclides from natural weathering processes over the same time span, which in Sweden could conveniently be a glacial-interglacial cycle.

Individual doses calculated with present biosphere-food chain conditions are, nevertheless, useful for assessments of early exposures assuming that a few canisters have manufacturing defects.

Special consideration must be given to the application of the dose limit on extreme accident scenarios, e g destruction of a repository by a meteorite impact. Such an event could cause high individual doses (in addition to other more severe consequences) but one feels intuitively that the probability of the event is too low to merit any measures specified to protect the repository against meteorites. The ICRP has proposed [7] that a quantitative risk criterion is used to determine the maximum probability of a destructive event which can be accepted, implying that countermeasures are not required. Accidents are stochastic events and so is cancer incidence from low level radiation exposures. The annual risk that an individual gets cancer from a continuing exposure at the dose limit 0.1 mSv/a is of the order of 10^{-6}. An accident, even if it gives lethal doses, does not appreciably increase an individuals risk if the frequency is less than a fraction of 10^{-6} per year. Doses from accidents thus need not be assessed provided it can be shown that their probability is sufficiently low.

9. SAFETY ASSESSMENT

Deterministic safety assessments were made for each of the KBS concepts. Figure 5 shows the calculated radiation dose at different times in the future to a member of the critical group who takes his household water from a well downstream from the KBS-3 repository[1]. The first penetration of canisters has been set to 100 000 years.

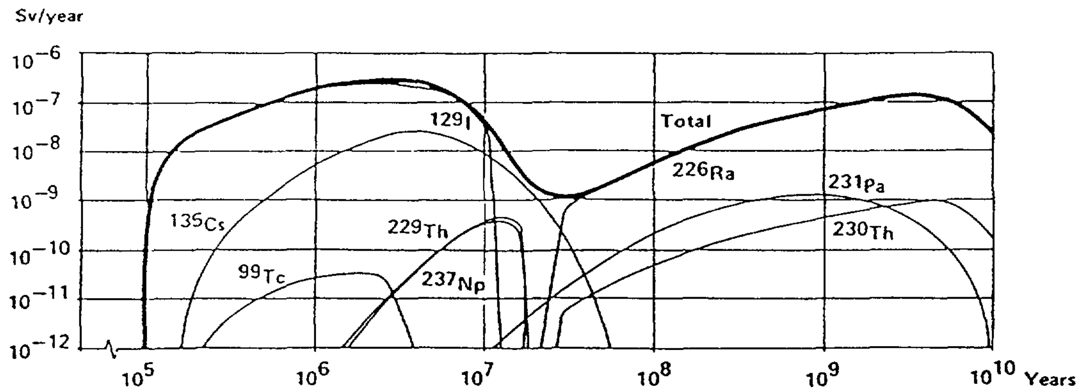


Figure 5. Dose versus time; indicating repository safety.

The curves illustrate some of the features of a repository with late release of radionuclides. Only a few long-lived nuclides contribute to the dose. Iodine-129, which follows the water without delay, arrives instantaneously to the biosphere in this time scale. The other nuclides are delayed by interactions with microfractures and minerals in the wetted fracture walls. This delay in combination with radioactive decay reduces the doses from these nuclides. The dose levels are satisfactorily low.

It takes upwards of 10 million years for the fuel to entirely "forget" that it was once irradiated in a nuclear reactor. The very late doses from radium etc are essentially independent of the irradiation of the fuel. They are due to ingrowth in the fuel of the daughter products of U-238 and U-235 which were removed from the natural uranium feed when it was prepared for fuel production. The calculation should have been terminated after the first maximum of the curve, since calculations of doses from natural uranium for the remainder of the history of the Earth are meaningless.

This safety assessment is presently being updated for publication in 1991. The recalculated doses should not increase appreciably as long as the present observations and assessments of spent fuel solubility and copper corrosion remain valid. These two features are at the heart of the safety of this repository.

REFERENCES

[1] "Final storage of spent nuclear fuel - KBS-3." SKB, Stockholm (1983)

[2] WERME, L., FORSYTH, R. , "Spent UO_2 fuel corrosion in water; Release mechanisms" Mater. Res. Soc. Symp. Proc., Vol 112 (1988)

[3] The Swedish Corrosion Institute and its reference group. "Copper as canister material for unreprocessed nuclear waste - Evaluation with respect to corrosion. Final report 1978-03-31." SKB, Stockholm (1978)

[4] PUSCH, R., BÖRGESSON, L., "Final report of the borehole, shaft and tunnel sealing test. Vol I, Borehole plugging. Vol II, Shaft plugging. Vol III, Tunnel plugging." Stripa project Technical Reports 87-01, 87-02, 87-03. SKB, Stockholm (1987)

[5] "Management and disposal of spent nuclear fuel. Review of a programme for research, development and other measures" p 66. Ibid, App 1 p 22-24 (in Swedish). SKN, Stockholm (1987).

[6] BERGMAN, C., BOGE, R., JOHANSSON, G., "Review of KBS-3." SSI - Report a 84-05. SSI, Stockholm (1984)

[7] "Radiation protection principles for the disposal of solid radioactive waste." ICRP Publication 46, Pergamon Press (1985).

THE CANADIAN APPROACH TO SAFE, PERMANENT DISPOSAL OF NUCLEAR FUEL WASTE

W.T. HANCOX, K. NUTTALL
Whiteshell Nuclear Research Establishment,
Pinawa, Manitoba,
Canada

Abstract

The assessment of nuclear fuel waste disposal deep in plutonic rock of the Canadian Precambrian Shield is now well advanced. A comprehensive understanding has been developed of the chemical and physical processes controlling the containment of radionuclides in used fuel. The following conclusions have been reached.

- Containers with outer shells of titanium or copper can be expected to isolate used fuel from contact with groundwater for at least 500 years, the period during which the hazard is greatest.

- Uranium oxide fuel can be expected to dissolve at a rate less than 10^{-8} per day, resulting in very low rates of radionuclide release. This is consistent with observations of uranium oxide deposits in the earth's crust.

- Transport of radionuclides away from the containers can be significantly delayed by placing a compacted bentonite-clay based layer between the container and the rock mass.

- The granite plutons of interest consist of relatively large rock volumes of low permeability separated by relatively thin fracture zones. The low permeability volumes are sufficiently large to accommodate a vault design that will ensure radionuclides do not reach the surface in unacceptable concentrations.

Our field and laboratory investigations, together with assessments of conceptual disposal vault designs, give us confidence that the combination of engineered barriers and a technically suitable plutonic rock site will meet the requirements for safe disposal of nuclear fuel wastes in Canada.

---

1. INTRODUCTION

Disposal deep in rock of a continental land mass is the most practical means to ensure permanent safety of nuclear fuel waste with today's technology [1]. A number of suitable geologic media have been identified and most countries are focussing their research on the geologic medium that is most appropriate for them: West Germany is studying salt, the United States is studying volcanic tuff, Belgium is studying clay, and Sweden, Finland, Switzerland and Canada are studying granite. A multi-barrier containment system has been universally adopted in which the intrinsic containment provided by the geologic medium is supplemented by passive engineered barriers such as leach-resistant waste forms, corrosion-resistant containers to isolate the waste from contact with groundwater, and swelling clays to backfill and seal openings excavated in the geologic medium.

Canada generates about 15% of its electricity from nuclear power, using CANDU heavy-water moderated reactors. There are 13 GWe installed and 3 GWe under construction. There is about 13,000 Mg(U) of nuclear fuel waste in storage at reactor sites, all in the form of intact used natural uranium fuel assemblies. Additional used fuel is produced at a rate of about 1,800 Mg(U) per year. Although it is well established that used fuel storage is safe and reliable, and can continue for many decades, it is recognized that storage is not a permanent solution. In the 1970's, it was decided that disposal should be the final step in the nuclear fuel cycle. The objective was to isolate the nuclear fuel waste from the biosphere in such a manner that no responsibility or burden would be passed on to future generations. Canada does not reprocess used fuel and, consequently, the direct disposal of fuel is the primary focus of the fuel cycle. However, there is an international consensus that both used fuel and immobilized waste from reprocessing are acceptable waste forms for disposal, so that there are no major technological barriers to implementing reprocessing in Canada.

Since 1978, Atomic Energy of Canada (AECL) has been carrying out a generic research and development program to assess the concept of nuclear fuel waste disposal deep in plutonic rock of the Canadian Shield. The results of this generic research will be reviewed under the Federal Environmental Assessment and Review Process. The Environmental Impact Statement for this review will be submitted by AECL in 1991 for an in-depth scientific and technical review followed by public hearings. No screening or selection of potential disposal sites can be undertaken before a decision is made by the governments following the hearings.

The research and development program has had three primary goals:

- to develop and demonstrate technology to site, design, build and operate a disposal facility in plutonic rock that will satisfy Canadian regulatory safety criteria,

- to develop and demonstrate a methodology to evaluate the performance of a disposal system against the safety criteria, and

- to show that suitable sites in plutonic rock are likely to exist that, when combined with a suitably designed facility, would meet the safety criteria.

In Canada the nuclear regulatory agency is the Atomic Energy Control Board (AECB). In addition to the regulatory requirements that apply to existing nuclear facilities, the AECB requires that following closure of the disposal facility no individual should receive an annual radiation dose greater than 0.05 mSv (compared to the 1 mSv received annually from natural sources). It must be shown quantitatively that the safety criteria would be satisfied for a period of 10,000 years [2].

The Canadian decision to focus on plutonic rock of the Precambrian Canadian Shield as the disposal medium was made in the late 1970's [3]. The rationale was as follows. The Canadian Shield has been relatively stable for at least 600 million years, and most of the Shield has not had major orogenic activity for 2.5 billion years. Therefore, it is reasonable to infer that the region would remain stable for the required lifetime of a disposal vault. Also, regional topographic gradients in the Shield are low, about 1 m/km. As a result, the natural driving force for groundwater flow deep in the rock should be weak. Further, it is believed that there are large volumes of plutonic rock with extremely low porosity and permeability. These characteristics would serve to limit access of groundwater to the waste, thereby slowing its deterioration and inhibiting movement of radionuclides through the rock. Also, minerals in plutonic rock are known to react with many of the radionuclides in nuclear fuel waste, further retarding their movement.

The research program is now well advanced and a comprehensive understanding has been established of the performance of the various barriers [4]. This paper describes our reference concept for disposing of used CANDU fuel and highlights our understanding of the performance of the system components, including the used-fuel container, the used fuel, the clay layer surrounding each container, and the plutonic rock mass. Evidence is also presented of long-term performance gained from natural systems.

2. CHARACTERISTICS OF USED CANDU FUEL

A typical CANDU fuel bundle is shown in Figure 1. The uranium oxide fuel is in the form of ceramic pellets that are sealed inside zirconium alloy tubes to form individual fuel rods.

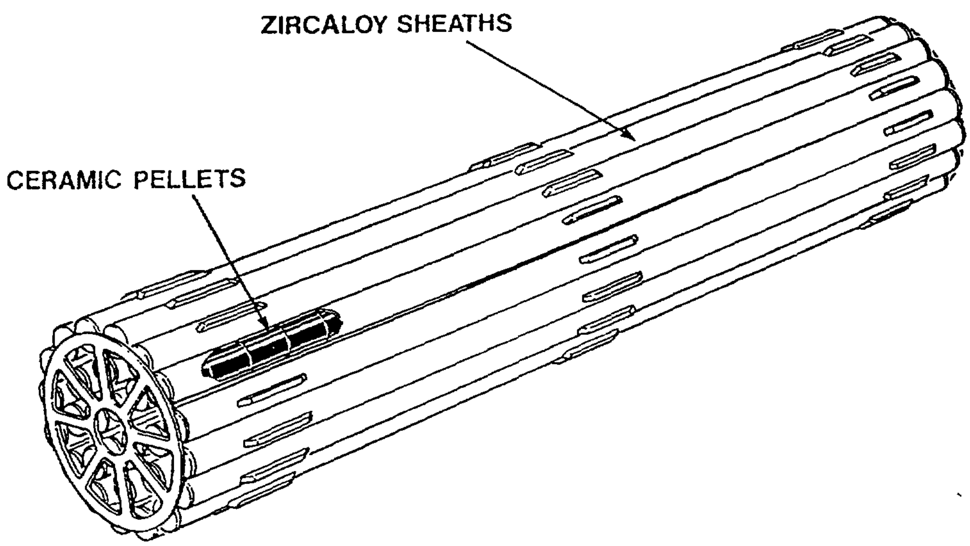


Figure 1: A Typical CANDU Fuel Bundle Assembly

Table 1 shows the composition of a typical bundle ten years after removal from the reactor (after a burnup of 685 GJ/kg). When the uranium oxide is "burned" in the reactor, almost 99% of the original uranium oxide is unchanged, and 0.65% of it is changed to stable elements. Only 0.65% of the fuel becomes new radioactive material, all of which is contained within the individual fuel elements, most within the uranium oxide grains.

Of the uranium isotopes, the uranium-235 content has been reduced from 0.7% to 0.2%, which is about the same level as that in the tails from a uranium enrichment plant. The plutonium (of which about 3 g/kg is fissionable) could be recovered by reprocessing and recycled with fresh natural uranium in a CANDU reactor, thereby producing about twice the energy output available from the natural uranium alone. However,

TABLE 1

USED CANDU FUEL COMPOSITION (%)

Element	Weight %
Uranium isotopes	98.78
Plutonium isotopes	0.40
Other actinides	0.01
Radioactive fission products	0.16
Non-radioactive fission products	0.65

plutonium-enriched natural uranium fuel is not economical today: it would cost about 3.5 mils/kWh in comparison to 0.6 mils/kWh for natural uranium fuel. The price of natural uranium would have to increase by a factor of about six to make plutonium recovery and recycle economic.

Figure 2 shows how the radiation dose 30 cm from a typical used-fuel bundle decreases with time. Used-fuel bundles are likely to remain in the water-filled storage bays at the reactor sites for at least 20 years. Twenty years after the bundle is removed from the reactor, the radiation dose at a distance of 30 cm is 2.5 Sv/h. After 500 years, most of the short-lived radionuclides have decayed to negligible levels and the radiation dose has decreased to less than 1 mSv/h.

Although the hazard from penetrating gamma radiation is relatively small after about 500 years, the long-lived radionuclides iodine-129, cesium-135, technetium-99 and plutonium-239 must be isolated from the

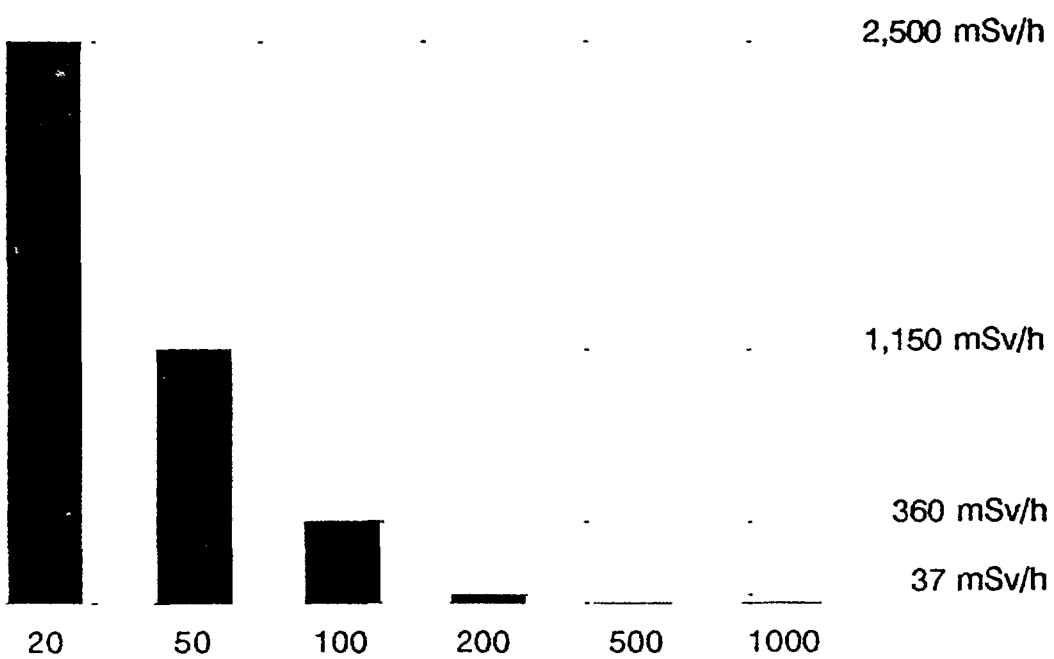


Figure 2: Radiation Dose from a Used CANDU Fuel Bundle at 30 cm

biosphere for tens of thousands of years. They can do harm only if they are ingested. However, they are mainly contained within the uranium oxide grains and will be released only if the grains are dissolved in groundwater.

3. CHARACTERISTICS OF PLUTONIC ROCK MASSES

The hydraulic, geochemical and structural characteristics determine the containment capacity of a rock mass and, thus, the containment requirements of the system of engineered barriers. Developing the technology needed to gain a detailed understanding of plutonic rock masses has therefore been a major thrust of our research.

Figure 3 shows a conceptual model of a typical plutonic rock mass indicating the scales of major fracturing in relation to the size of a disposal vault. The methodology that we have developed to derive the conceptual model has four main steps.

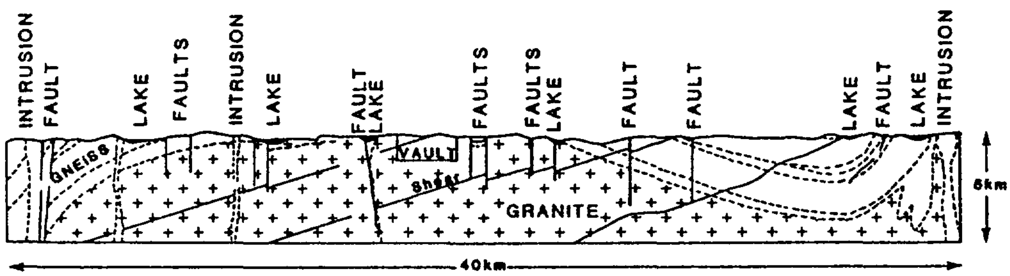


Figure 3: Schematic cross-section showing the general nature of structural and lithological features anticipated in association with granitic plutons in the Canadian Shield of Ontario. The approximate size and depth of a disposal vault is shown for comparison.

First, the surface of the site is carefully studied to map the location of features that are the surface expression of faults and fracture zones in the underlying rock mass. Airborne measurements of magnetic and density variations are interpreted to define the boundaries of the rock mass. And, at selected locations, seismic and electromagnetic waves are transmitted from the surface into the underlying rock and analyzed to infer the presence and orientation of zones of fracturing.

Second, guided by the results of the surface studies, cored holes are bored into the rock mass at selected locations to depths up to 1,000 m. Examination of the rock cores removed from the holes and the interior surface of the holes provides information on the distribution of fractures within the rock mass. Usually the fracturing is concentrated in narrow zones (about 1 m thick) that are hydraulically active. Steel casings fitted with valves and sealing systems are inserted in the holes to isolate the fracture zones and allow the hydraulic properties of the zones to be monitored. The chemical composition of water samles taken from the fracture zones also provides information on the origin of the water.

Next, the isolated intervals within the boreholes are used to determine the interconnections between fracture zones and the hydraulic properties of the interconnecting flow paths. This is accomplished by either injecting or withdrawing water from an isolated interval while monitoring isolated intervals within neighbouring boreholes. By repeating this procedure at a number of intervals a picture can be developed of the three-dimensional character of the flow paths, and their hydraulic characteristics.

Finally, a three-dimensional mathematical model is used to describe water movement within the flow paths. Predictions by the model are tested against measurements of natural flow system changes made in the network of isolated intervals. Refinements are made in both the model and the description of the flow paths until agreement is attained. The model then provides a basis for analyzing the containment potential of the rock mass.

We have used this methodology to characterize the Lac du Bonnet Batholith, which is located in the Whiteshell region of southeastern Manitoba (Figure 4). It is a large granite pluton similar to many found in the Canadian Shield. The pluton was intruded over 2,500 million years ago into the rocks existing at the time. The pluton itself, the surrounding rocks and the interfaces between them have been the subject of extensive field investigation over 10 years.

Our field research indicates that the plutons of interest can be conceptualized as relatively large rock volumes with low permeability,

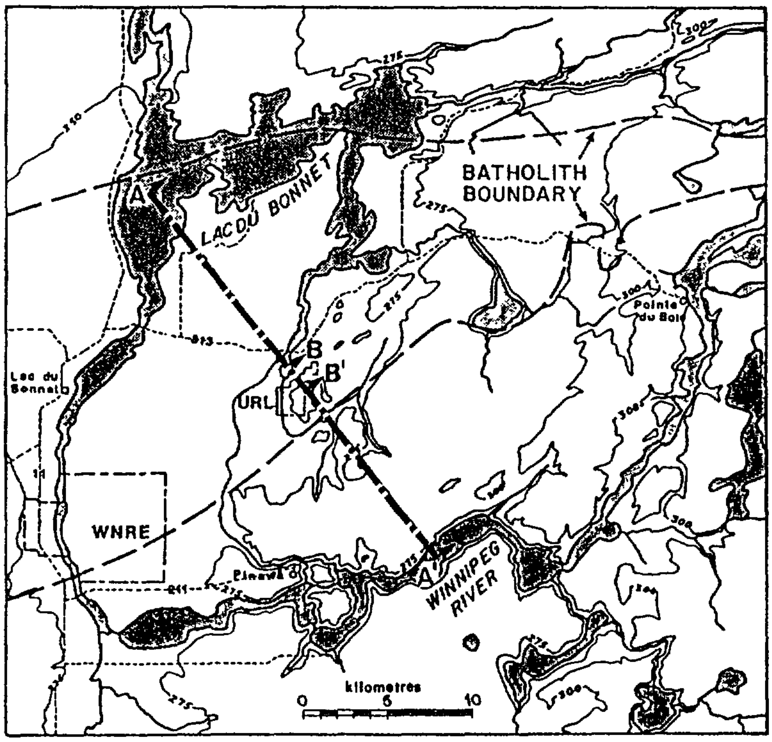


Figure 4: Location of Whiteshell Research Area showing the Lac du Bonnet granite batholith, surface topography (25 m contour interval), drainage and the location of the cross sections in Figure 5.

separated by relatively thin planar fracture zones. A vertical cross section (through AA[1] on Figure 4) showing our conceptual understanding of the fracture and permeability characteristics of the Lac du Bonnet Batholith is shown in Figure 5 [5]. The fracture zones are much more conductive than the background rock, and control the groundwater flow. The flow is primarily driven by topographic gradients, which in the Canadian Shield are small on a regional scale. Outside the fracture zones, the rock is relatively unfractured, except for networks of near-vertical fractures that extend from the surface to depths of about 250 m.

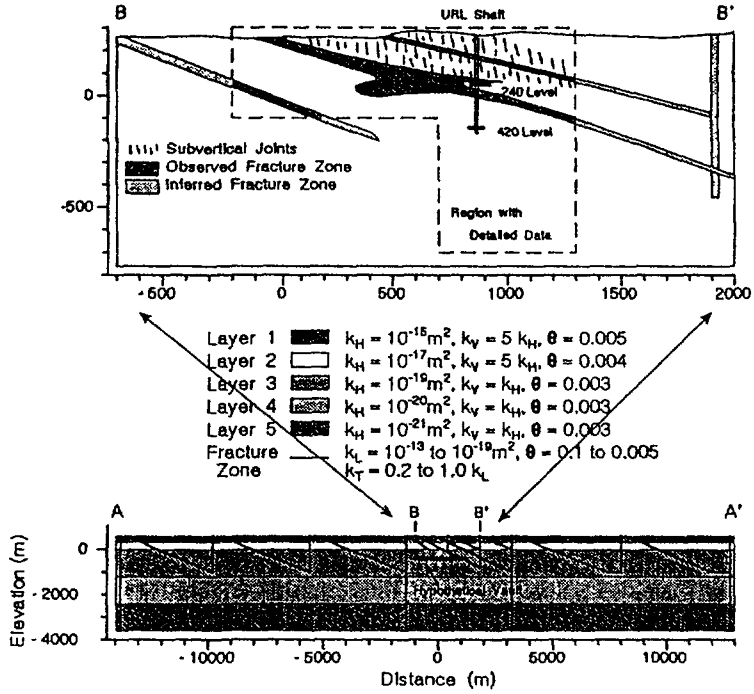


Figure 5: Conceptual cross-section (A-A') used for mathematical modelling of groundwater flow at the Whiteshell Research Area based on detailed investigations at the Underground Research Laboratory (B-B'). Patterns in section A-A' represent the distributions of horizontal and vertical permeability (k_H, k_V) and porosity (θ) employed. The ranges of lateral and transverse permeability (k_L, k_T) are also given for the fracture zone.

This conceptual groundwater flow model is described mathematically by a finite-element computer model called MOTIF [6,7]. It represents the relatively unfractured background rock by an equivalent porous medium, composed of three-dimensional continuum elements. The high conductivity zones are represented by special planar elements, which are embedded in the background porous medium. The flow within these planes is dominant along their axes. The three-dimensional flow field within this assembly of blocks and planar elements is described by porous medium flow equations.

The pathways with the shortest transit time to the surface are fracture zones, as might be expected. Once radionuclides reach such a zone where the direction of groundwater flow is toward the surface, the transit time could be of the order of a thousand years. However, the hydraulic conductivity of the relatively unfractured background rock is such that radionuclide migration occurs mainly by diffusion. Transit times of the order of 1,000 years per metre would be expected. Therefore, radionuclide transit times to the surface will be determined by the location of the disposal rooms relative to the fracture zones.

4. DISPOSAL CONCEPT

Prior to disposal, the used-fuel bundles would be sealed in corrosion-resistant containers. Our design target is to isolate the used fuel from contact with groundwater for at least 500 years, the period during which the most of the radionuclides decay to negligible levels. Figure 6 shows a conceptual design for a thin-walled container for 72 CANDU fuel bundles. Support against external pressure is provided by packing glass beads in the spaces between the fuel assemblies and the outer wall. Prototype containers of this design, with a 5-mm thick titanium alloy outer shell, have withstood external pressures greater than 10 MPa at 150 C, during hydrostatic tests. Thus, they meet the primary structural requirements for disposal in a vault at a depth of 1,000 m [8].

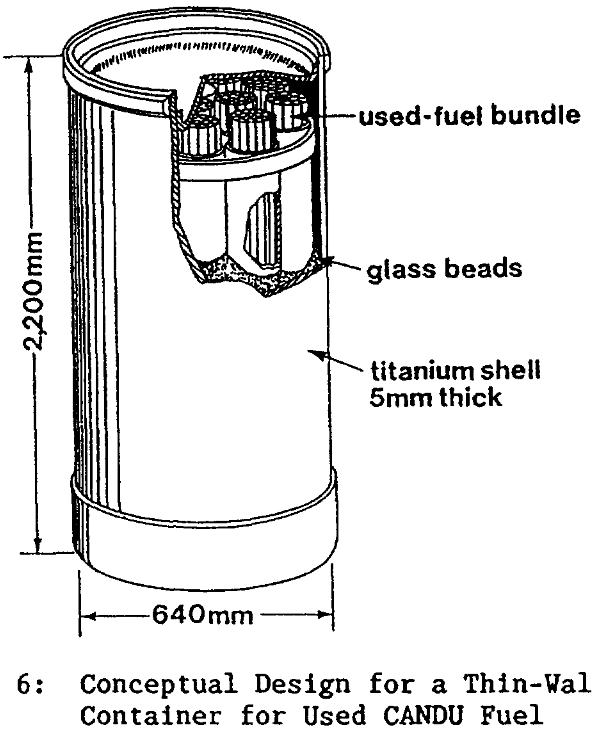


Figure 6: Conceptual Design for a Thin-Walled Container for Used CANDU Fuel

The reference layout of a single-level disposal vault is shown in Figure 7, as well as details of a typical disposal room [9]. The vault would consist of 480 disposal rooms, each 220 m long, 8 m wide and 5.5 m high, and would have a plan area of about 4 km^2. It would be excavated at a depth between 500 m and 1,000 m, depending on the characteristics of the host rock mass. There would be sufficient capacity to dispose of about 190,000 Mg of used CANDU fuel (about 135,000 containers).

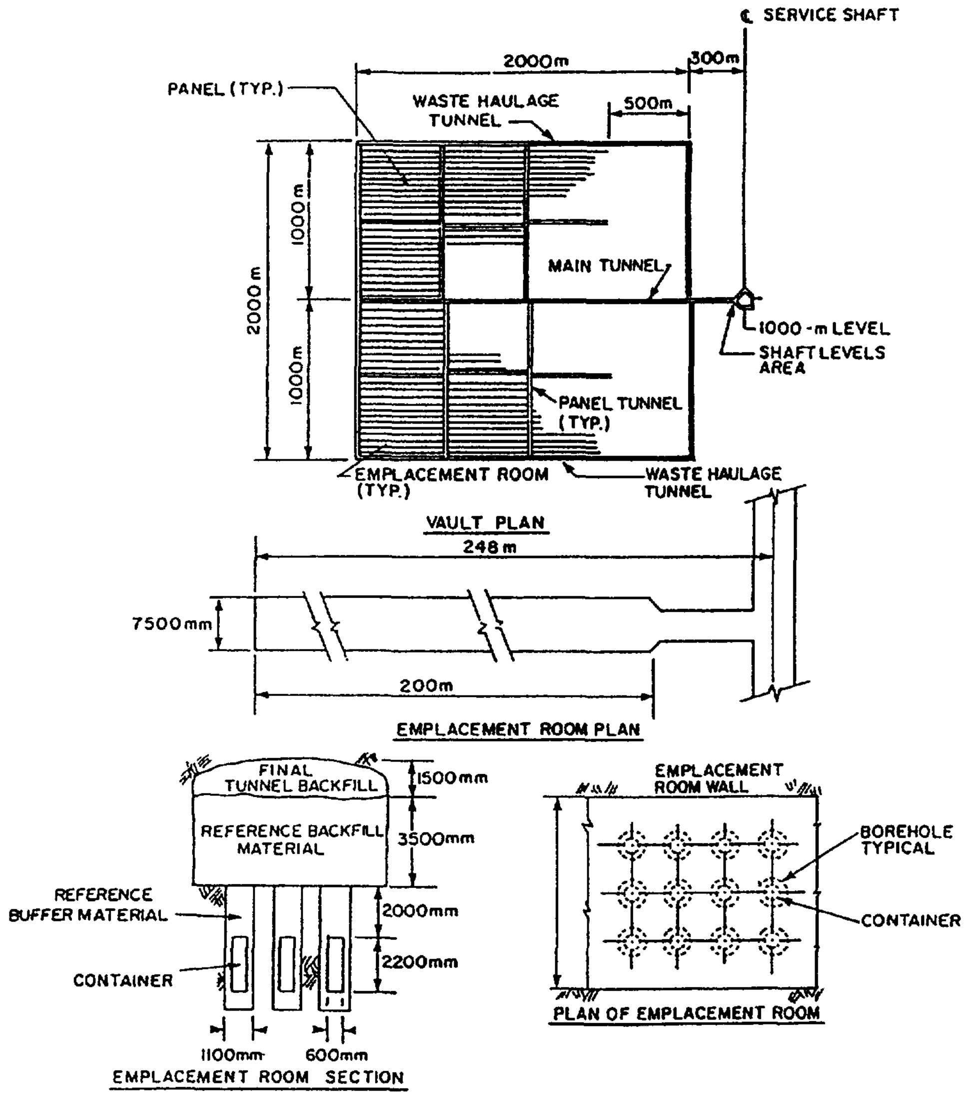


Figure 7: Reference Layout of a Single-Level Disposal Vault

Figure 8 indicates the reference backfilling materials in a disposal room. The used-fuel containers would be lowered through a vertical shaft, transported to the disposal rooms, and placed in holes (1.2 m in diameter and 5 m deep) bored into the floor of the rooms. Prior to receiving the waste containers, the holes would be filled with a mixture of sodium-bentonite clay and sand, mechanically compacted and then rebored to provide a central hole (700 mm in diameter and 4.2 m deep). The 250-mm thick bentonite-sand layer would act as a diffusion barrier to the movement of groundwater, inhibiting the transport of radionuclides away from the container. The spacing between containers would ensure that the maximum temperature of their out shells would not exceed 100 C.

When filled with containers, each room would be backfilled and sealed. The backfilling would be done in two stages: first, the lower

CROSS SECTION THROUGH A TYPICAL DISPOSAL ROOM

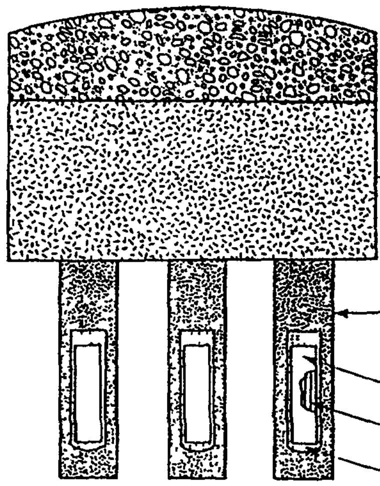


Figure 8: Cross-Section Through a Typical Disposal Room

portion of the room would be filled with a mixture of clay and crushed granite, which would then be mechanically compacted; second, the remaining space would be filled pneumatically with a mixture of granite aggregate and bentonite. Additional sealing would be provided by concrete bulkheads at the ends of the rooms. To close the vault, the access tunnels would be backfilled in a manner similar to the disposal rooms. The access and ventilation shafts would also be backfilled with a compacted mixture of clay and crushed granite and supported with a series of concrete bulkheads. The bulkheads could be located so as to mitigate the effects of excavation damage or fracture zones, should this prove necessary.

5. BARRIER PERFORMANCE

5.1 The Used-Fuel Container

Container integrity will be determined primarily by the corrosion resistance of the outer-shell material. Our design target is to isolate the used fuel from contact with groundwater for at least 500 years. For the chloride-rich groundwater found deep in the Canadian Shield, we have focussed our research on titanium alloys and copper.

Our studies on titanium alloys [10] demonstrate their corrosion rate would be less than 1 μm/a under the conditions expected in the disposal vault; that is, groundwater at less than 150 C with a chloride content less than 1 mol/L. This extremely low corrosion rate is a result of a protective, passive oxide film. However, breakdown of this film can make titanium susceptible to localized corrosion processes, such as crevice corrosion. We have used an electrochemical approach, which forces crevice corrosion to initiate, to demonstrate that both grade 12 and grade 2 titanium are capable of preventing the propagation of crevices by re-establishing their protective oxide films. Thus, a 5-mm thick titanium outer shell would be sufficient to isolate the used fuel from groundwater for at least 500 years.

If copper is used for the outer shell, only uniform corrosion is expected to play a role. We have studied the dissolution of copper metal in chloride solutions and in the presence of compacted bentonite [11]. The experiments show that the corrosion rate is limited by the rate at which dissolved metal species are transported away from the corroding surface. We conclude that the 25-mm thick outer shell of copper required for structural support, would provide an effective barrier to the release of radionuclides for at least 5,000 years.

5.2 The Uranium Oxide Fuel

Once groundwater breaches the container shell, the zirconium alloy fuel sheaths (see Figure 1) are not expected to provide significant protection. Because of the high chloride content of the deep groundwater, the zirconium may be attacked by crevice corrosion. However, the uranium oxide is expected to provide highly effective containment of radionuclides.

Our research shows that there are three principal mechanisms by which radionuclides are released in groundwater [12]:

1. About 2% of the iodine and cesium are released rapidly once the zirconium alloy fuel sheath is breached.

2. An additional 6% of the iodine and cesium are released slowly by preferential dissolution at the grain boundaries.

3. The remaining fission products and actinides trapped within the uranium oxide grains are released extremely slowly as the grains dissolve.

Under the reducing conditions expected in a disposal vault, experiments with used fuel show that uranium concentrations in low to moderately saline groundwater would be in the range 1-100 $\mu g/L$. Dissolution rates are observed to be less than 10^{-8} per day.

The stability of uranium oxide in groundwater has been confirmed by studies at the Cigar Lake uranium deposit in northern Saskatchewan [13]. The deposit, shown in Figure 9, is situated at a depth of 430 m at the interface between the host sandstone formation and the underlying basement rock. The ore body is 2,000 m long, 100 m across, and 20 m thick at mid-length and contains about 150,000 Mg of high-grade ore. It is surrounded by a clay-rich layer that varies in thickness from 5 m to 30 m. An iron oxide/hydroxide-rich zone forms the contact between the high-grade ore and the clay layer.

The ore body consists mainly of individual grains of uranium oxide mixed with clay minerals; the average concentration of uranium oxide is 12%, with local concentrations as high as 60%. Since the ore body was formed about 1.3 billion years ago, there have been several episodes of groundwater interaction with the ore body. Despite this interaction, there has been no significant movement of uranium. Water samples taken only 5 m from the ore body have a uranium concentration less than 20 $\mu g/L$ which is below the levels specified for drinking water.

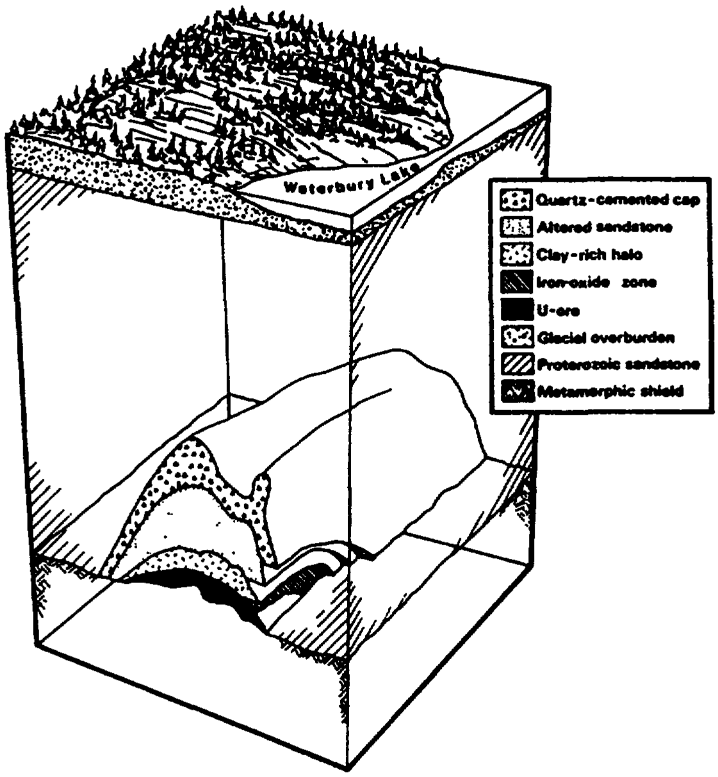


Figure 9: Schematic of Cigar Lake Uranium Deposit

Although the groundwater flowing toward the deposit is oxidizing in nature, oxygen is removed by iron minerals and organic materials within the ore body and the surrounding clay layer. The iron is oxidized more easily than uranium and acts as a scavenger for oxidizing species. Examination of samples from the ore body show that the surface oxidation state of the uraninite grains is less than U_3O_7 [14]. Compositions less than U_3O_7 are consistent with the observed reducing condition of groundwater samples from the ore zone and with laboratory observations of the dissolution behaviour of uranium oxide fuel.

5.3 The Sealing and Backfilling Materials

The principal function of the bentonite-sand layer surrounding each container (see Figure 8) is to inhibit the movement of radionuclides. Our research shows that radionuclide movement in compacted bentonite-sand mixtures would occur only by diffusion [15]. Layer thicknesses of only 250 mm can delay movement of dissolved and suspended radionuclides for thousands of years. Laboratory studies indicate that bentonite clay is expected to remain stable for long periods of time under the geochemical conditions in a disposal vault in the Canadian Shield. Recent field and laboratory studies of natural bentonite deposits in southern Saskatchewan confirm that this clay has maintained an acceptably high swelling potential and low permeability millions of years after its deposition [16]. Mechanically compacted clay backfilling materials have similar properties to the buffer, providing the potential for diffusion rates of the order of 1,000 years per metre.

6. CONCLUSIONS

Containers with titanium and copper outer shells can be expected to isolate used fuel from contact with groundwater for at least 500 years, the period during which the hazard is greatest. The used fuel has also been shown to be highly resistant to dissolution under the groundwater conditions expected in a disposal vault. Dissolution rates less than 10^{-8} per day have been determined for used fuel in the laboratory experiments and are consistent with observations of uranium ore deposits in the earth's crust.

The movement of radionuclides dissolved in groundwater can be further retarded by placing a compacted clay layer between the container and the rock mass. Delay times of thousands of years can be attained.

Thus, the combination of the container, used fuel and clay layer can be expected to delay the release of radionuclides into the deep groundwater system for several thousand years and to maintain their concentrations at low levels.

Our field investigations in the Canadian Shield, supported by assessments of conceptual disposal vault designs, give us confidence that there are a large number of locations which, after detailed examination, will provide disposal sites that meet safety requirements.

REFERENCES

[1] OECD/NEA, "Nuclear Spent Fuel Management: Experience and Options", Organization for Economic Development and Cooperation, Nuclear Energy Agency, Paris (1986).

[2] AECB, "Regulatory Objectives, Requirements and Guidelines for the Disposal of Radioactive Wastes - Long Term Aspects", Atomic Energy Control Board Regulatory Document, R-104 (1987).

[3] AIKEN, A.M., HARRISON, J.M., and HARE, F.K., The Management of Canada's Nuclear Wastes, EP-77-6, Energy, Mines and Resources Canada, (1977).

[4] DORMUTH, K.W. (Editor), Canadian Nuclear Fuel Waste Management Program, Special Issue, Radioactive Waste Management and the Nuclear Fuel Cycle, 8 2-3 (1987).

[5] DORMUTH, K.W., HANCOX, W.T. and WHITAKER, S.H., "Geological considerations for disposal of nuclear fuel wastes in Canada", Proc. 28th International Geological Congress, Washington (1989), to be published.

[6] GUVANASEN, V., Development of a Finite-Element Code and Its Application to Geoscience Research, TR-299*, Atomic Energy of Canada Limited Technical Record (1985) 554-66.

---

* Unrestricted, unpublished report available from SDDO, Atomic Energy of Canada Limited Research Company, Chalk River, Ontario K0J 1J0.

[7] DAVISON, C.C., CHAN, T., and SCHEIER, N.W., "Experimental activities of the Canadian Nuclear Fuel Waste Management Program to validate geosphere models", Proc. Geoval-87, Stockholm (1987) 401-422.

[8] TEPER, B., Feasibility Assessment of the Particulate-Packed, Thin-Walled Container, TR-350*, Vol. 1, Atomic Energy of Canada Limited Technical Record (1985) 21.

[9] BAUMGARTNER, P., and SIMMONS, G.R., Disposal centre engineering for the Canadian Nuclear Fuel Waste Management Program, Special Issue, Radioactive Waste Management and the Nuclear Fuel Cycle, 8 2-3 (1987) 219-239.

[10] IKEDA, B.M. and CLARKE, C.F., "Titanium corrosion under Canadian nuclear waste disposal conditions", Proc. 2nd International Conference on Radioactive Waste Management, Winnipeg, Canadian Nuclear Society (1986) 605-610.

[11] KING, F. and LITKE, C.D., "The corrosion behaviour of copper under simulated nuclear fuel waste disposal conditions", Proc. 2nd International Conference on Radioactive Waste Management, Winnipeg, Canadian Nuclear Society (1986) 593-596.

[12] JOHNSON, L.H., SHOESMITH, D.W., and STROES-GASCOYNE S., "Spent fuel: characterization studies and dissolution behaviour under disposal conditions", Scientific Basis for Nuclear Waste Management Vol. XI, Pittsburgh, MRS (ATED, M., and WESTERMAN, R., Ed.) (1988) 99-113.

[13] CRAMER, J.J., "A natural analog for a fuel waste disposal vault", Proc. 2nd International Conference on Radioactive Waste Management, Winnipeg, Canadian Nuclear Society (1986) 697-702.

[14] SUNDER, S., TAYLOR, P., and CRAMER, J.J., "XPS and XRD studies of uranium rich minerals from Cigar Lake, Saskatchewan", Scientific Basis for Nuclear Waste Management, Vol. XI, Pittsburgh, MRS (ATED, M., and WESTERMAN, R., Ed.) (1988) 465-472.

[15] CHEUNG, C.H., "Evaluation of methodologies for determining ionic diffusion coefficients in clays", Proc. of the Canadian Engineering Centennial Convention, Montreal (1987) 195-224.

[16] OSCARSON, D.W., DIXON, D.A., and GRAY, M.N., Swelling capacity and permeability of an unprocessed and processed bentonite clay, Journal of Eng. Geology (in press).

PANEL PRESENTATION

FUEL CYCLE SAFETY EVALUATION

J.M. MORELLE
Belgonucléaire SA,
Brussels, Belgium

The numerous steps of the fuel cycle each have their own technicalities and for each of them safety evaluations have been conducted. However, the fuel cycle should be seen as a whole, i.e. as one single "system", not only as a sequence of steps. A technical optimisation of this unified "system" is most likely to lead to changes in the definition and the technicalities of several of its individual steps.

A similar observation applies to the safety evaluation which has not reached the same level of synthesis and depth as that of the nuclear power plant. Furthermore, an update of existing work would be appropriate. Such an update should include the steadily widening experience resulting from operating numerous fuel cycle facilities.

The present lack of synthesis is due not only to the subdivided nature of the fuel cycle, but also to the diversity of its individual actors. More interplay between actors is desirable and each actor should look beyond his part. Hence to arrive at a proper safety evaluation of the fuel cycle as a whole, a "stage director" should be needed to coordinate the safety evaluation of the various individual actors.

As mentioned at several occasions during the workshop for the long term energy supply and to counter the greenhouse effect only the breeder can provide an adequate solution. Therefore, the safety evaluation for the long term option should also be conducted on the breeder fuel cycle. Such an evaluation should rest on as much experimental evidence as possible and the question is then how to acquire a proper evaluation of the safety of the breeder fuel cycle. This aim is complicated by the fact that the experimental data related to the fuel cycle are by their very nature lagging behind those related to the power stations using this fuel cycle.

Fortunately, practically all steps of the breeder fuel cycle are fairly well simulated by their equivalent in the recycling of plutonium in LWR's. This recycling is hence an excellent test bed for the fuel cycle of the industrial breeders.

I therefore think that, independently from other considerations, the plutonium recycle deserves special attention : it should be thorougly followed and evaluated as an efficient contributor to the evaluation of the breeder cycle and to its safety, and hence as a preparation of the future.

One may notice that the significance of recycling in view of the penetration of the fast reactor is explicitely recognised in the Japanese nuclear programme published in mid 1987.

A remark on burnup which is an important parameter linking the fuel cycle to the power station : the increase in burnup should receive continued attention because of :

- the better fissile and fertile material utilisation,
- the reduction of the risks associated with the handling of fuel and the reduction of material losses to be disposed of. This reduction results from the reduced number of iterations of the fissile and fertile material through the cycle.

An increased burnup adds to the safety of the fuel cycle.
However, actual industrial experience on increased burnup requires a long lead time and an extensive effort.

CLOSING PANEL

Chairmen

H.J.C. KOUTS
United States of America

M. ROSEN
International Atomic Energy Agency

STATUS AND TRENDS IN NUCLEAR POWER DEVELOPMENT IN ITALY

G. PETRANGELI
Directorate for Nuclear Safety and Health Protection (ENEA/DISP),
Rome, Italy

1. PRIMARY REFERENCE POINTS IN ITALY

Following the intense debate on the use of nuclear energy in Italy in the years '86 and '87 and a national referendum on the abrogation of some specific points of the italian nuclear legislation, a resolution was passed in the Parliament in December '87 which, among other instructions, pledged the Government not to plan for new nuclear plants over the subsequent five years and to start concrete initiatives in the fields of research and applications of passive safety reactors.

Subsequently, in August 1988, a scheme of new National Energy Plan (PEN), prepared by a Technical Committee for Energy under the Chairmanship of the Minister of Industry, was approved by the Governement.

This Plan is now before the Parliament for discussion and approval. It obviously complies with the Parliament resolution of December '87 and includes some specific implementation provisions. The following ones are considered as particularly meaningful points:

- the most qualifying and relevant part of the future research program on nuclear fission is declared to concern the exploration and the development of new plant design solutions based on an extensive use of inherent and passive safety features, which are considered accepted by the public opinion;
- the need is stressed to acquire, through a nationwide program which should benefit of a number of international cooperations, the necessary information concerning design and technology of the types of innovative plants which, through a cooperation among a number of Countries, might firmly establish themselves in the international field and, in perspective, also in Italy;
- in order to define the lines of action to be followed an Advisory Committee has been set up which includes representatives of ENEA (the Nuclear and Alternative Energies Research and Development Organization), ENEL (the Electric Energy Generating Organization), Industry and DISP (the ENEA Directorate for Licensing and regulation of nuclear activities).

The scheme of new PEN tentatively earmarks nearly 200 billion lire (roughly equivalent to 140 million dollars) for research and development on enhanced inherent or passive safety fission reactors.

It is here noted with satisfaction that international cooperation in the development of new reactors for Italy is viewed as an "essential" factor not only in the technical circles but also at the highest political level, as it is evident from the above listed excerpts of official documents.

This fact well matches the belief and intentions of italian technical bodies according to which, also in the interest of safety, design activities concerning new reactors should preferably build over the experience of proven ones as the outcome of a natural process of innovative evolution, rational "re-thinking" and optimization in the light of the experience gained so far.

This belief by no means implies that also completely new solutions be considered if they rest over proven/tested technology.

2. ACTIVITIES AND TRENDS

In view of the definition of a program of research and applications over the future years, a whole series of preliminary works, performed by all the interested organizations and institutions, has started in Italy in addition to previous initiatives of study and research.

However, it is still premature to talk about an Italian position or structured program on the matter /1/.

Published papers (/2/, /3/, /4/ are some examples) at the present stage can only offer a limited outlook. Paper /2/, as an example, summarizes, some general considerations as well as the results of the survey, performed by ENEA/DISP, on the current industrial proposals, as requested by the Ministry of Industry in November '87 in view of future research activities and applications in our Country. In addition, its appendixes give a brief description of studies already performed in Italy on specific reactors or systems.

Paper /3/ and /4/ deal with some recent developments under consideration at ANSALDO S.p.A. or ENEL, presently the subject of evaluation by other bodies too.

Some features of future reactors for Italy are, however, actively aired and discussed in technical and planning circles and in the media.

Give time, some of these features will, perhaps, emerge as consensus guidelines.

Here is a sample list of desirable features currently under dicussion:
- maximum use of inherent and passive safety features;
- maximum transparency of safety characteristics (simplicity, strenght of protective provisions, non reactive combinations of materials, deterministic safety criteria, which are thougth to be more easily understood by the public, and so on);
- no need for planned evacuation of population even without plant personnel intervention for a significant time lenght (grace period) and limited land use restrictions also in case of severe accidents; it is, in this regard, frequently expressed the belief that if an emergency evacuation plan were required for a reactor type abroad, this reactor would not be accepted in Italy;
- consideration in design of all of the accident scenarios so far conceived and important (e.g. current PRA scenarios; e.g. NUREG 1150 risk dominant scenarios plus external events and sabotage);
- reliable plant operation (availability factor).

It has also to be noted, in this connection, that the competitive cost of the produced energy is not unanimously considered as an essential feature of future plants. In order to justify in some way this belief seemingly shared by many in Italy, it has to be considered that diversification of energy sources has to be highly prized in the italian energy situation.

3. A FINAL REMARK

A certain amount of activity seems to be going on in several countries, perhaps not yet completely surfaced, aimed at the study of future reactors capable to cope, by design, with severe accident conditions. This effort is deemed as an highly commendable one as it is intended to overcome the obstacle of public acceptance for nuclear plants.

Yet, there are indications that the same effort might risk to fall short of its goal in the long term. It seems, indeed, that in many cases, particularly for small LWRs, protections against severe accidents are proposed which are based on active systems without a previous thorough search and study of passive ways to obtain the same effect.

Now, nobody in the technical field believes that "more inherently and more passively safe" necessarily means "safer", yet passive, simple and inherent safety features are generally credited with a "potential" for being preferable.

Will the attitude of being content with active protections against severe accidents not result, in the long range, in public opposition again?

Objections against this trend are, indeed, already heard like: "which is the point of getting rid of such active components as diesel generators and pumps and of retaining, at the same time, a large number of active valves"?

Another concept to be carefully meditated is the potential benefit of bringing into being in the shorter time scale reactor plants made of a proven power generating reactor system and of passive containment systems able to cope with severe accident situations. This is said without anything detracting from the merits of more conceptually innovative plants for the longer time range.

Moreover, the search for passive, simple technical solutions might help to get rid of cumbersome and costly requirements concerning redundancy, testing, maintenance and quality assurance.

Examples of areas where a more intense effort towards design simplicity seems appropriate are, for small LWRs:

- protection against destructive steam explosions and reactor vessel perforations which is obtainable either through primary system active depressurization or by passive means (passive depressurization or missile protection envelope around the pressure vessel);
- protection against excessive leaks through mechanical containment penetrations or against "V type" sequences obtainable by active means or by passive features (leak dilution and delay volumes in auxiliary buildings and in the lower part of turbine buildings, minimization of mechanical containment penetrations, use of discontinuous buffer - type fluid transfer means through the containment, filtered venting systems for auxiliary and lower turbine building and so on).

Not all, of these new passive technical provisions may at the end of a complete screening process result as advisable or even practicable, although first scoping evaluations tend to confirm their feasibility (ENEA/DISP is, by the way, ready to share with anybody interested the content and the result of some evaluation of this kind).

The point is, however, here stressed that a more intense and wider effort is warranted in order to look for passive, simple protections against a larger set of severe accident phenomena. It is strongly felt, indeed, that means of this kind could help to more durably solve problems in the containment early failure and containment isolation areas. Consideration of passive means seems, on the contrary, to have been limited so far to core and containment cooling for extended times and, in some proposed design, to reactor shutdown.

In summary, if the natural evolution of the fission reactor technology calls today for a "re-thinking" and optimization exercise in connection with future reactors, this exercise should take advantage of all the experience previously accumulated, both in the technical ground and in the public acceptance field. It is, therefore, more advisable to take into account probable future public criticism while new reactors are still on the drafting boards than having possibly to modify them later.

This line of action could even result less costly than others at the very end.

I apologize for the rather detailed nature of some of the last remarks.

I however decided not to lose the opportunity to bring them to the attention of this exceptional audience in view of their possible long term implications.

REFERENCES

/1/ NASCHI G., "The italian experience on the development of safety criteria for Nuclear Power Plants", Regulatory Practices and Safety Standards for Nuclear Power Plants (Proc. IEAE/FRG/NEA Int.l Colloquium, Münich FRG, 1988) IAEA - SM - 307/20.

/2/ NASCHI G, PETRANGELI G., "Italian Approach on more inherently and passively safe reactors", U.S. - ITALY Bilateral Study - Energy Security - Alternatives to Oil (Proc. Symposium, Argonne, III. 1988).

/3/ ADINOLFI R., OLIVIERI M., SIMONOT H. (ANSALDO S.p.A.), NOVIELLO L. (ENEL), Functional and structural requirement for the containment of a new advanced passive PWR Nuclear Power Plant" Small and Medium - Sized Nuclear Reactors: you and your environment (Post SMIRT Int.l Seminar, San Diego Ca. 1989).

/4/ GENCO M., CINOTTI L., ADINOLFI R. "Passive Features and Components for the next generation Nuclear Power Plants" Small and Medium-Sized Nuclear Reactors: you and your environment (Post SMIRT Int.l Seminar, San Diego Ca., 1989)

WHERE DO WE GO FROM HERE?

A. ALONSO
Polytechnical University of Madrid,
Madrid, Spain

The most probable answer to the question in the title of the session: "Where do we go from here?", will be the desired one: "We are going towards a large deployment of nuclear power plants, along the 21st century, in most countries of the world". Of course, there is a residual risk that such deployment would not take place, but that could only be motivated by extraordinary events, affecting the whole world.

Nevertheless, such foreseen large deployment of nuclear energy will not take place without complications and distresses, which will emerge from the very nature and intrinsic characteristics of nuclear science and tecnology. Four of such peculiarities are of particular relevance to this workshop.

First of all, Nuclear Science and Technology is intellect intensive; its implementation demands highly qualified individuals and institutions, so that only countries with a certain scientific and technical infrastructure would be able to use nuclear energy in a substantial way. This has been recognized by Dr. Ahearne and discussed at length.

Secondly, Nuclear Science and Technology is capital intensive. Very significant amount of capital is needed to build the power plants and the related fuel cycle installations. This problem has not been discussed in our workshop, as it mainly concerned with safety; nevertheless, it is to be recognized that finantial problems, and not public opinion, are now hindering the implementation of nuclear energy in many countries.

Thirdly, it must beacknowledged that in the process of liberating nuclear energy strategic materials are also produced, with deep international implications regarding safeguards and non-proliferation. This workshop has not considered this aspect, which should be regarded as crucial in any large deployment of nuclear technology. The fuel cycles to be chosen will have to be non-proliferation resistant and strategic materials will have to be consumed and be under tight control.

Fourth and last, it is also to be recognized that nuclear reactions produce undesired toxic materials and so creating a safety and a waste disposal problem, with profound public opinion implications, that have been discussed at lenghth.

While these four factors, and others, would control, and possibly limit, any large deployment of nuclear technology, it is also true that mankind can put into play resources to counterac and surpass such difficulties and obstructions. One of such resources is education; being and educator myself, I have found proper to stress the benefits and advantages of deploying education on Nuclear Science and Technology at all possible levels and in all countries.

Education would be the factor needed to overcome the high demand for intellect which Nuclear Science and Technology requires; moreover, education could, at the same time, help to solve other problems and it is a key element in the public opinion issue. In Spain, an education programme has been implemented by the Spanish Atomic Industrial Forum aimed at educating high school teachers. This programme, which has been going on for the last ten years, is being considered very successful due to its multiplicative effect.

In industrialized countries, nuclear industry is not longer attracting the most brilliant students, who prefer other technologies and activities. From my vantage position as Professor of Nuclear Engineering at the Polytechnical University of Madrid, I am observing this decline with a certain apprehension and I undestand this is certainly the case in other countries.

On the other side, from my experience, I conclude that only very few developing countries have established educational programms of importance. It is true that the different training courses sponsored by the International Atomic Energy Agency represent a very positive response to such requirement, but the number of trainees is necessarily limited, and not always the former students remain active in the field due to the lack of challenging activities in the country of origin.

In case of a substantial resumption of nuclear power, industrialized countries could react within a short (a few years) dalay time and recuperate the lost talent. But the needed education in developing countries can only be implemented at a given rate, which is country dependent, and the question arises whether the achievable rate would be compatible with the need to solve the long range climatic problems and the need for energy of such countries.

One may be tented to say that the industrialized countries have already written the "Book of Kowledge" on Nuclear Science and Technology and that such book is there for every body to read and learn fron it, but it is well known that "Any Book of Knowledge can only be properly read, and I stress the word properly, by those who participate on its writing".

In Spain, an importing country with a large, for its size, nuclear power programme, we know a lot about the difficulties one may find when trying to read the Book of Knowledge on Nuclear Science and Technology. We started to understand the problems when we decided to participate deeply in the design and construction of our nuclear power plants. We accumulated knowledge in paralell with the operation of our nuclear stations, and so we can more easily understand the experience in other countries. A big leap is taken place through our participation in international research and development programmes on safety and in the performance of PRA'S LEVEL I for our nuclear installations. On the other side, we are yet unable to perform, for example, a complete risk study, up to LEVEL III, or perform an individual plant examination.

INSAG-3 very clearly states two basic safety principles: (1) the responsibility of the plant owner-operator and (2) the independence of the licensing authority. There is no way to satisfy such principles without an understanding of the scientific and technical basis and details of nuclear technology.

As it has been said by Dr. Chancey Starr, we should not understimate devoloping countries, but we should not over-rate them also. For all these reasons, I believe that, as a responsible group, we should recognize the importance of education in the large foreseen deployment of nuclear power in the next century. Moreover, we should call the attention of appropiate international organization and prospective nations upon the need for education on nuclear science and technology.

STATUS AND TRENDS IN NUCLEAR POWER DEVELOPMENT IN THE UNION OF SOVIET SOCIALIST REPUBLICS

A.A. ABAGYAN
All-Union Research Institute for
Nuclear Power Plant Operations,
Moscow, Union of Soviet Socialist Republics

Progress of civilization inevitably results in the increase of power consumption in the society. Introduction of energy-saving technologies may slow down power demand growth rates causing even its temporary freeze but only for a limited period of time.

As shown by the research, it is impossible to make up for the required growth in power consumption without commissioning of additional nuclear power plant (NPP) capacities. Otherwise irretrievable ecological damage will result. Therefore, for the near future up to the year of 2000 and beyond we plan to increase NPP capacities

Before the Chernobyl NPP accident soviet public acceptance of nuclear power in the USSR was positive. Different regions in the country were eager to obtain nuclear power sources to cover the lack of electricity and thermal power.

After the Chernobyl tragedy the situation has dramatically changed. And now nuclear power development in the USSR will depend on our ability to convinqe the public that the measures taken ensure NPP safe operation and future designs will further improve plant characteristics.

To give a dialectical answer to the questions concerning the near and distant future of nuclear power development in the USSR, let me give you a brief outline of its history and present status.

The soviet nuclear power is 35 years old. In this period several generations of different reactor types have been designed and built, as shown in Fig. 1.

After commissioning of the world's first NPP in the USSR, pressurized water uranium-graphite type reactors have been the main option.

As of beginning of 1989, 16 NPPs with 46 nuclear reactors with the total installed capacity of 35 400 MW gross were in operation in the USSR. These include 15 units with RBMK reactors of 1000 MW and 1500 MW capacity and 25 units with VVER reactors of 440 MW and 1000 MW capacity.

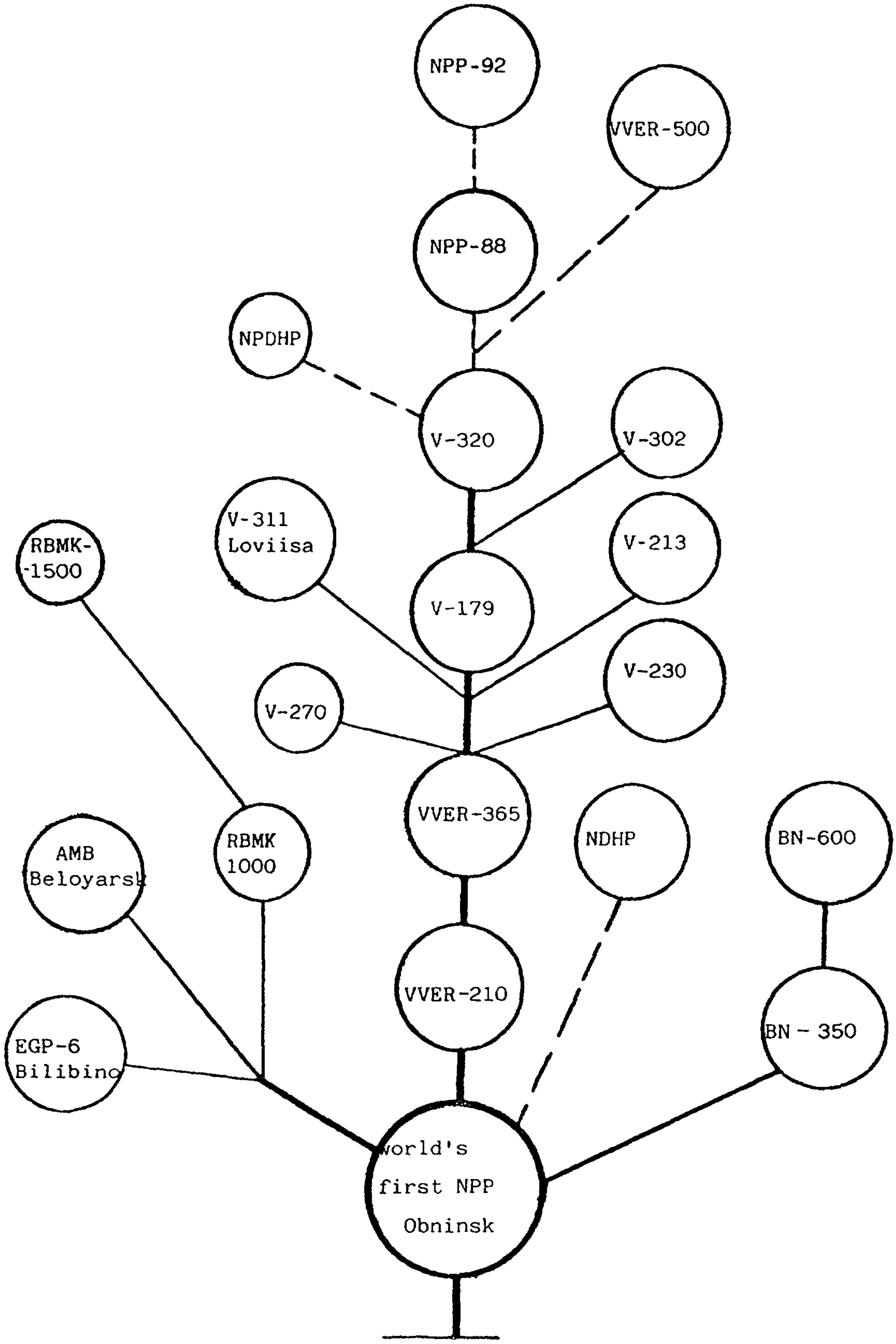


Fig. 1. Family tree of soviet nuclear power

______________ operating units; _ _ _ _ _ _ _ _ _ Units in the design stage

NPDHP - nuclear power and district heating plant
NDHP - nuclear district heating plant

A number of corrective measures have been taken at RBMK plants after the Chernobyl accident. These measures cover both technical matters and personnel activities and enable to significantly improve plant safety and prevent severe accidents even in case of personnel errors like those committed in Chernobyl. Nevertheless, since these measures do not meet the present safety requirements the decision has been taken to cancel the programme of building new RBMK plants. This means that on expiration of their design lifetime the plants will be shut down and decommissioned and new RBMKs will not be built.

The major increase in NPP capacities will come from VVER plants.

The possibilities of introducing nuclear district heating plants (NDHPs) are at present being restricted by the negative response of the public. But despite this there is some progress in this area, especially after probabilistic safety assessment (PSA) was performed and IAEA team of experts gave a positive conclusion of the Gorky NDHP design. Of course, much attention will be given also to other reactor types. This first of all applies to fast breeder plants and high temperature gas cooled reactors. Their development will primarily depend on economic considerations.

Now a few details concerning VVER plants. At operating VVER plants measures have been taken to further improve their operational safety level. Much attention is given to personnel training in the training centres and stations. The simulators are being improved and modified. A number of VVER units of earlier generations were decommissioned because of economic inefficiency of their modifications or under the influence of public opinion as was the case with Armenia NPP.

To explain the trends in nuclear power development and in particular of VVER plants, the following considerations can be given.

1. At present the safety is not determined from the quantitative viewpoint and probably will not be in the near future. This is due to the fact that safety is a qualitative category and a social one. One can speak about the relative level of safety of a certain reactor type implying the value inversely proportional to risk.

The value of risk, i.e. the product of an accident probability multiplied by its economic consequences is not the absolute value, since it includes significant uncertainty due to inaccuracy of equipment reliability data and human factor, for example, promptness and effectiveness of operating personnel actions to manage the severe accident.

2. Fig. 2 is a qualitative illustration of enhancement of requirements to the level of safety.

Stepwise enhancement of the required safety level is determined both by the accumulated design experience, new R&D and plant incidents which have occurred.

Actual safety levels of several generations of VVER plants are schematically shown by horizontal lines. Steps in the levels correspond to the implemented unit modifications.

Another three considerations can further be given which are of importance.

3. Safety requirements are changing more rapidly than the specified NPP lifetime.

4. Possibility of modifications, maximum substitution capability and modular design principle are to be taken into account in new NPP designs.

5. Trends in the enhancement of safety level requirements make it necessary to include in the design the safety margin existing at the time of the design process.

Determination of the value of the appropriate margin is a very difficult task because the history of nuclear power development is not sufficient for reliable prediction for the decades to come bearing in mind that the specified lifetime of new units will be 50-60 years.

In other words, extrapolation interval is longer than prehistory interval which inevitably leads to error.

Today there are three distinct ways of safety level improvement (Fig.3):

-elimination of the potential causes of accidents;

-prevention of event progressing into severe accident, i.e. core melt with decay products release into environment;

-effective management of severe accident with the aim to mitigate its consequences and return reactor facility to stable and safe condition.

Figures 4 and 5 present the basic new scientific-technical solutions used in the designs of NPP-88 and NPP-92 according to the above three ways.

Fig. 6 shows VVER safety systems promotion and improvement from generation to generation.

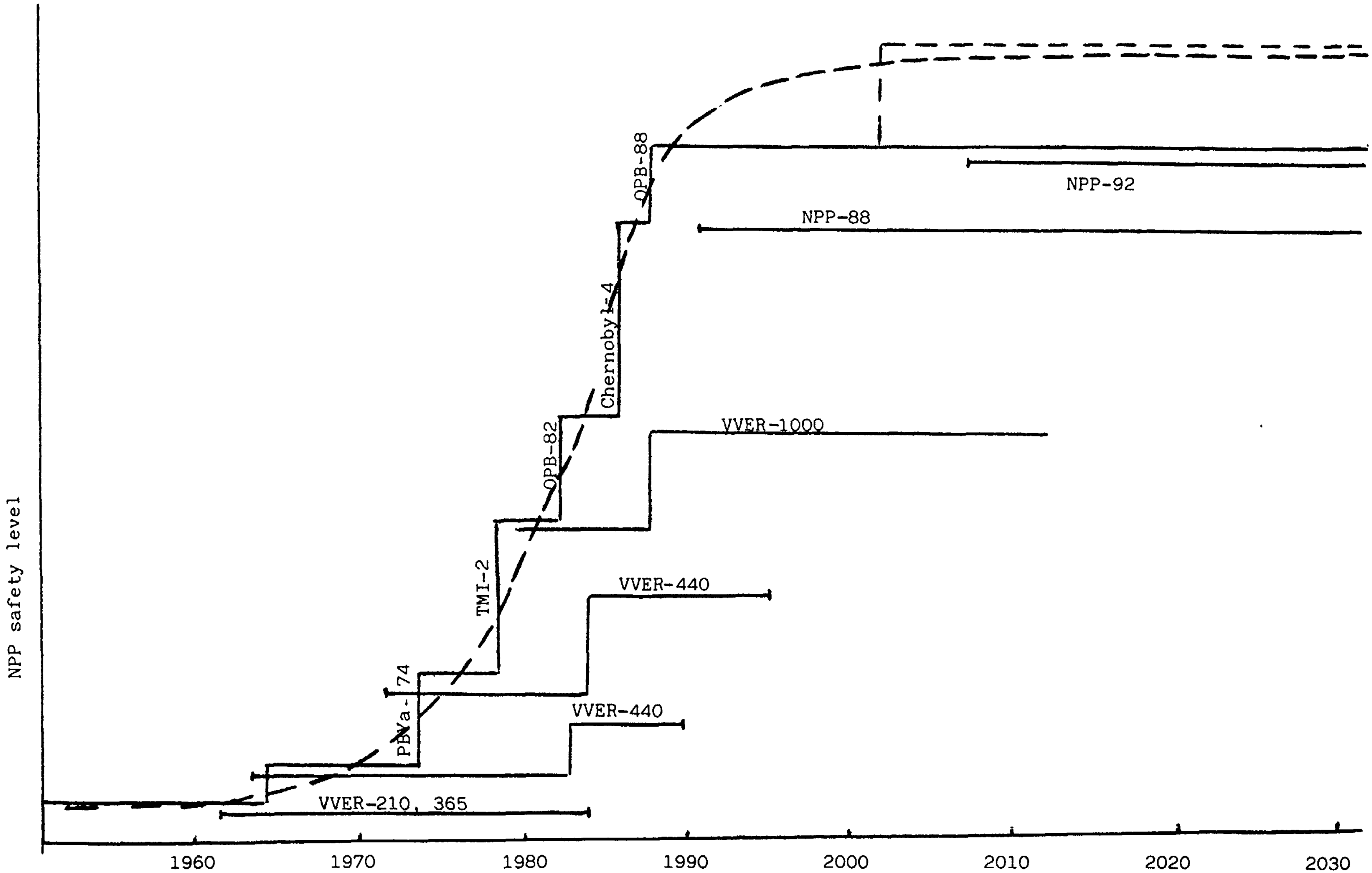


Fig. 2. Relationship between the required and actual safety levels of VVER plants

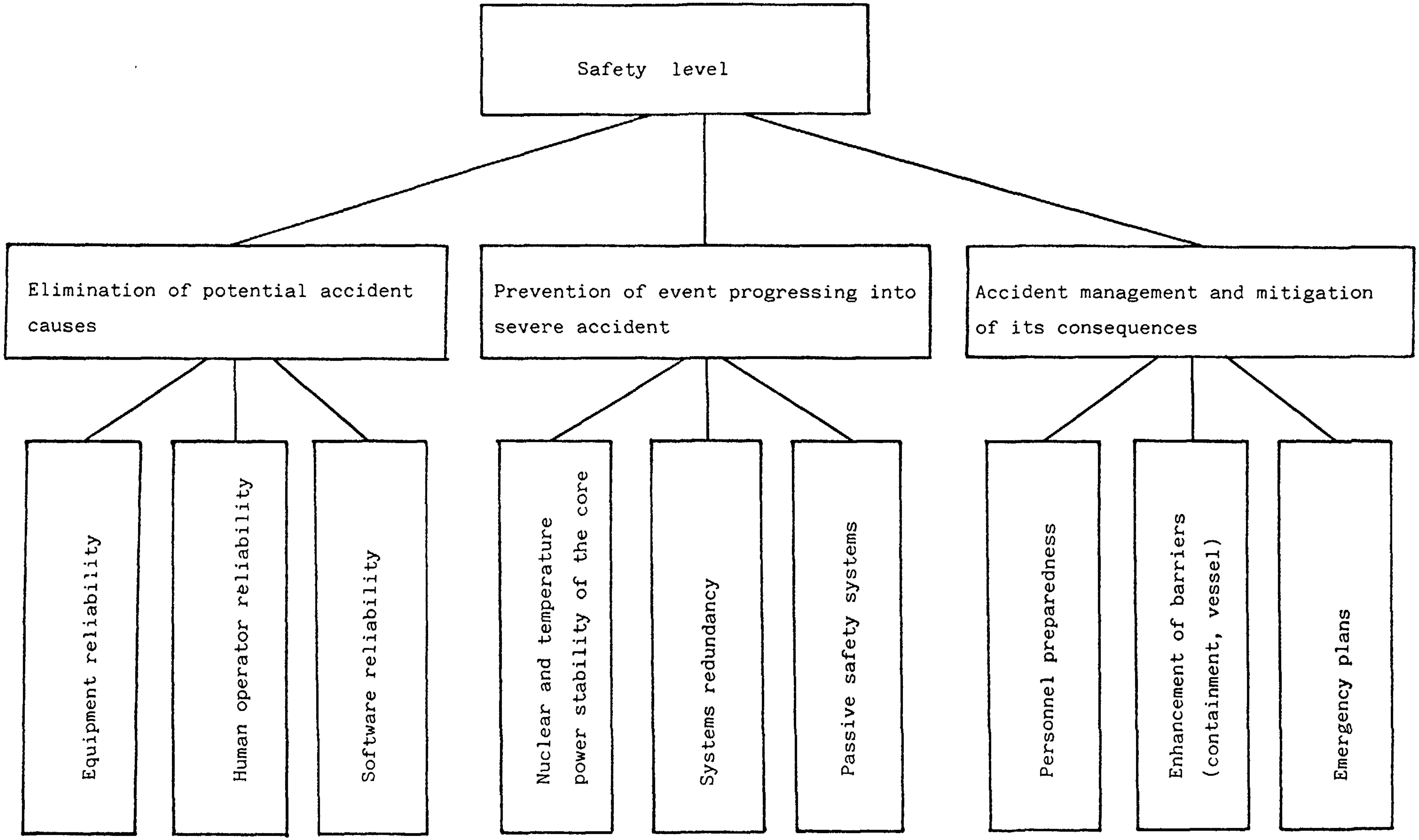


Fig. 3. Sources and ways of improvement of NPP safety level

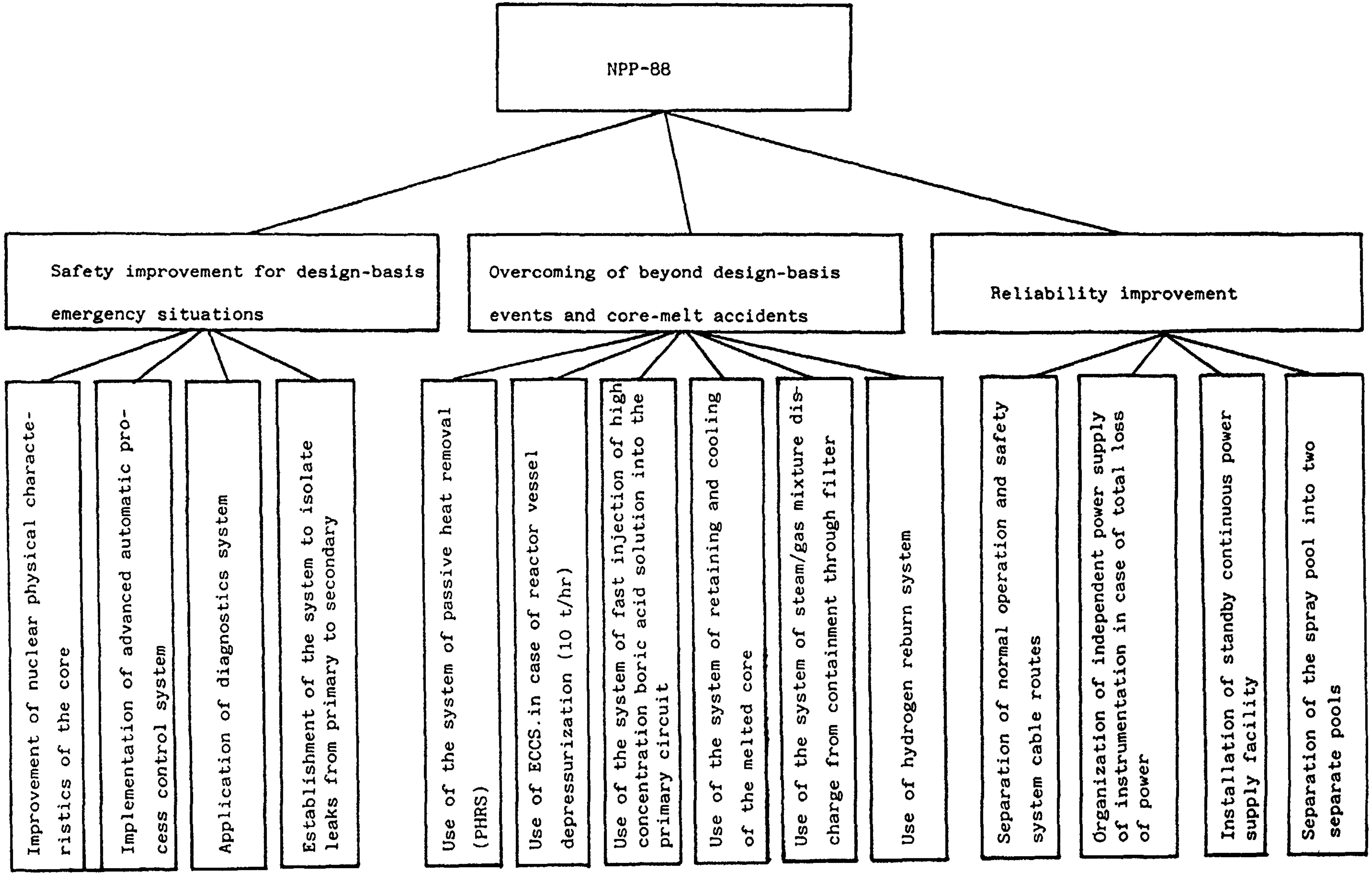

NPP-88
Safety improvement for design-basis emergency situations
Overcoming of beyond design-basis events and core-melt accidents
Reliability improvement
Improvement of nuclear physical characteristics of the core
Implementation of advanced automatic process control system
Application of diagnostics system
Establishment of the system to isolate leaks from primary to secondary
Use of the system of passive heat removal (PHRS)
Use of ECCS.in case of reactor vessel depressurization (10 t/hr)
Use of the system of fast injection of high concentration boric acid solution into the primary circuit
Use of the system of retaining and cooling of the melted core
Use of the system of steam/gas mixture discharge from containment through filter
Use of hydrogen reburn system
Separation of normal operation and safety system cable routes
Organization of independent power supply of instrumentation in case of total loss of power
Installation of standby continuous power supply facility
Separation of the spray pool into two separate pools

Fig. 4

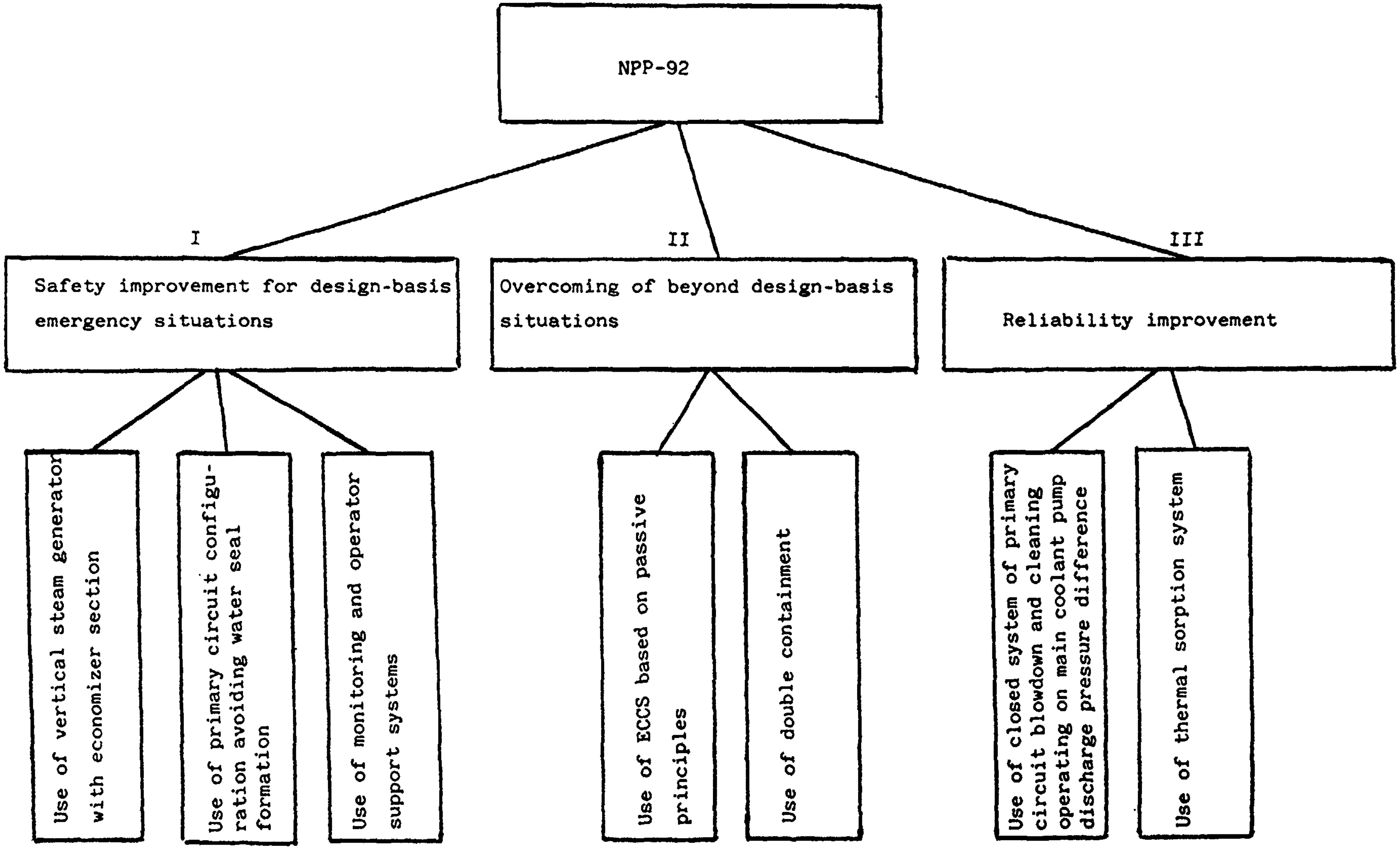

NPP-92
I
II
III
Safety improvement for design-basis emergency situations
Overcoming of beyond design-basis situations
Reliability improvement
Use of vertical steam generator with economizer section
Use of primary circuit configu-ration avoiding water seal formation
Use of monitoring and operator support systems
Use of ECCS based on passive principles
Use of double containment
Use of closed system of primary circuit blowdown and cleaning operating on main coolant pump discharge pressure difference
Use of thermal sorption system

Fig. 5

Type of design	Thermal power MW	Specified lifetime, years	ECCS		System of fast reactivity control	Level maximum DBA, mm (leaks)	Melt retaining and cooling system	Sealed containment	Passive heat removal system
			Active systems	Passive systems					
V-1	760	20	none	none	mechanical	none	none	none	none
V-179 V-230 V-270	1375	30	none	none	mechanical	$\emptyset_{nom}$ 32	none	none	none
V-213(U)	1375	40	3x100	4x50	mechanical	Full rupture of main circ. pipe ($\emptyset_{nom}$ 500)	none	available (single)	none
V-320(U)	3000	50	3x100	4x50	mechanical	Full rupture of main circ. pipe ($\emptyset_{nom}$ 850)	none	available (single)	none
NPP-88(I)	3000	50-60	3x100	4x50	mechanical + system of fast boron injection	Full rupture of main circ. pipe ($\emptyset_{nom}$ 850)	none	available (single)	available
NPP-88(2)	3000	50-60	3x100	4x50	mechanical + system of fast boron injection	Full rupture of main circ. pipe ($\emptyset_{nom}$ 850)	available	available (single)	available
NPP-92	3900	50-60	none	4x50 4x100	mechanical + system of fast boron injection	Full rupture of main circ. pipe ($\emptyset$nom 850)	available	available (double)	available

Fig. 6. Comparative analysis of VVER plant designs

In future a situation may arise when the use of other reactor types than VVERs will prove more acceptable on economic grounds as well as from the viewpoint of meeting the enhanced safety requirements. In this case the leading role in the nuclear power may be taken by the above mentioned fast breeders and high temperature gas cooled reactors as well as pressurized water reactors.

And finally, a somewhat controversial statement may be possible. Since today we realize that the most dangerous situation is related with the core melt, then one day such reactor types are likely to appear in which nuclear fuel will be in the melted condition, that is, the present severe accident becomes the normal operational state of the facility.

POSTER PRESENTATIONS

THE PIUS NUCLEAR POWER REACTOR:
A POSSIBLE ANSWER TO THE GREENHOUSE EFFECT

K. HANNERZ, C. PIND
ABB Atom AB,
Västerås, Sweden

ABSTRACT

The new awareness of the environmental effects of fossil fuel burning on the earths climate through the greenhouse effect, should make the nuclear option more attractive in a world hungry for energy. In the last few years new designs have emerged of nuclear reactors with improved safety that should make them more acceptable to the public, thereby diverging the energy option from a question of choosing between plague (coalburning) and cholera (nuclear power perceived as hazardous). ABB Atom has in the last decade developed the PIUS reactor with outstanding, clearly understandable safety features imbedded in the hydraulic principle. By simple laws of nature the reactor core is protected against overpower, loss of coolant, human mistake and mischief and other plausible events. In any such events the core is brought to a shutdown state and cooled without use of active components or actions from plant personnel. The paper briefly describes the design of the PIUS reactor and shows its unique safety aspects, compared to other LWRs. Economic studies have shown that the revolutionary safety performance can be obtained without economic sacrifice. The ultimate target is to start operation of a 600 MWe lead plant before the end of the century.

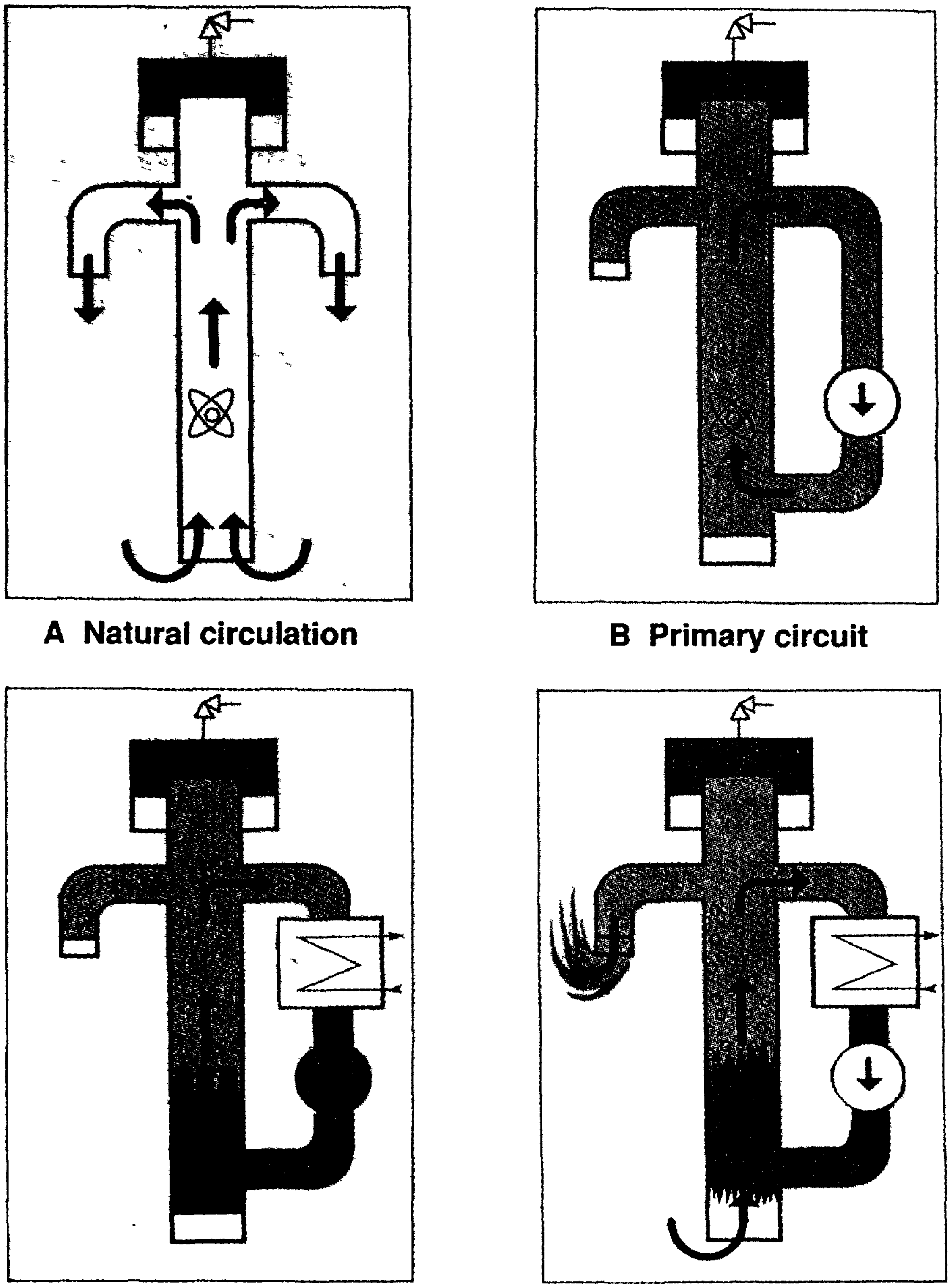
1. OPERATING PRINCIPLE

The PIUS hydraulic principle is shown in Figure 1 together with a short explanation of the natural circulation path that is always open and ready to take over the cooling of the core in case of overpower or failure of the cooling capacity of the circulating water. A detailed discussion of the hydraulic principle in PIUS can be found in Reference 1 and 2.

The main hydraulic paths in PIUS are shown on Figure 2 and the design with main components can be seen on Figure 3.

As can be seen on Figure 3 the steam generators are placed vertically outside the concrete pressure vessel which contains most of the primary system. The concrete pressure vessel has a volume of about 3000 cubic metres of which 2500 m^3 are cold borated water surrounding the primary system (mainly core and riser on Figure 3). In the primary system the main coolant pumps (4 on Figure 3) pump the primary coolant to the upper part of the pressure vessel, down through the downcomer to a plenum under the core (9 on Figure 3), through the core and up through the riser and thereafter through external pipes to the steam generators (2 on Figure 3).

PIUS
Hydraulic principle



A Natural circulation

B Primary circuit

C Power operation

D If high riser temp

Figure 1

A. A (nuclear) heat source causes natural circulation when placed in a vertical pipe in a water pool due to decrease of the density of water with increase in temperature.

B. A pump returns the natural circulation flow to the inlet of the core. There is no flow to the pool.

C. Hot water is layered above cold in bundles of open small diameter pipes ("density locks") at upper and lower ends of the pipe. The system is pressurized by a steam bubble.

D. The cooling of the circulating water is lost. Boiling of the water in the pipe commences. Increased difference in density between the circulating water with steam bubbles and the cold pool water causes increased natural circulation flow. The pump is no longer capable of returning it to the core inlet. The deficit enters the core from the pool through the lower density lock. Boric acid in the pool water shuts the reactor down.

PIUS 600

Basic arrangement principle

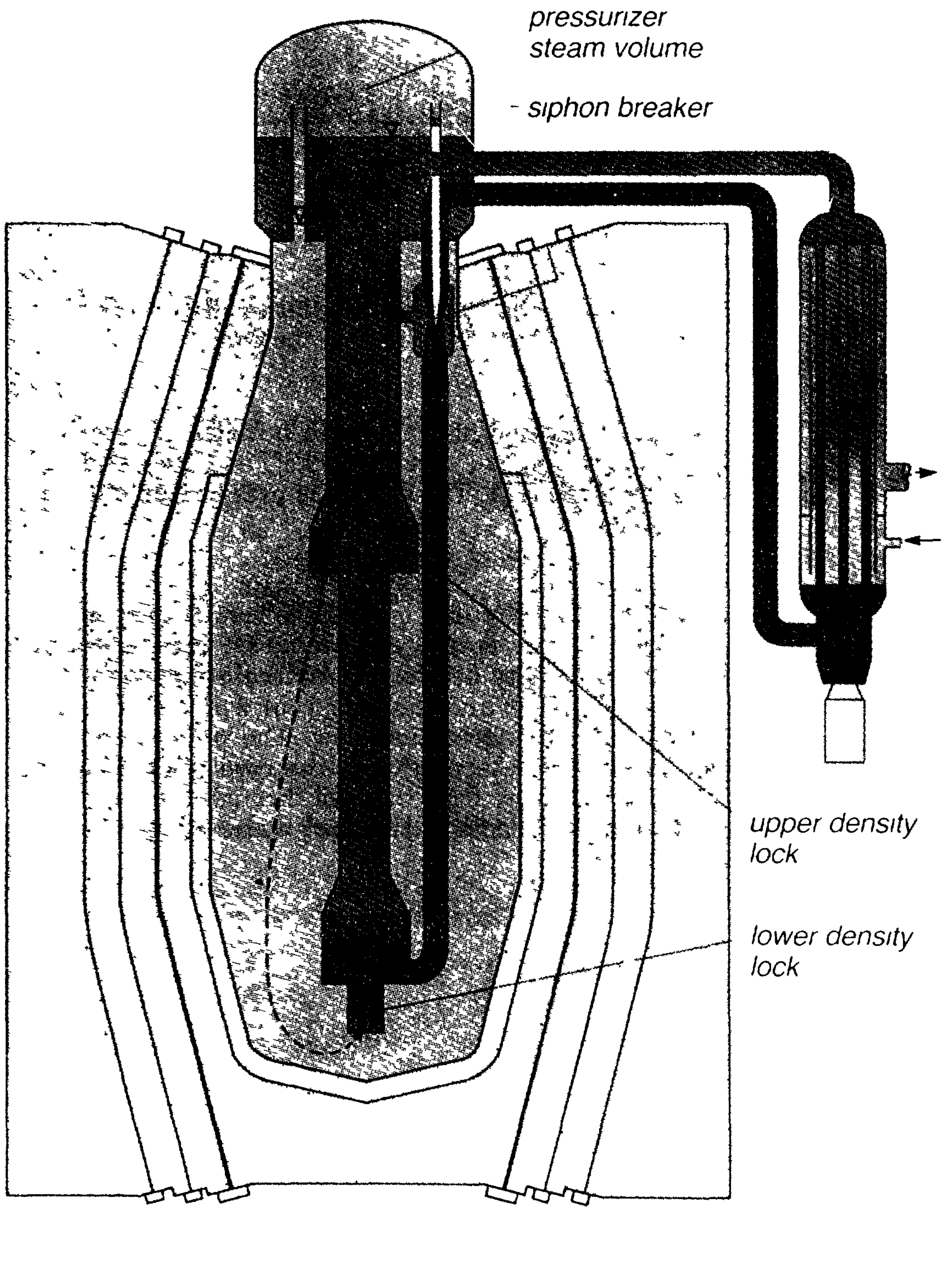


Figure 2

PIUS

1. Pressurizer steam volume
2. Steam generator (4)
3. Upper density lock
4. Main coolant pump (4)
5. Riser
6. Core instrumentation
7. Embedded steel membrane
8. Pool liner
9. Core
10. Lower density lock
11. Pool coolers for passive dissipation of core decay heat to ambient air (air coolers not shown)

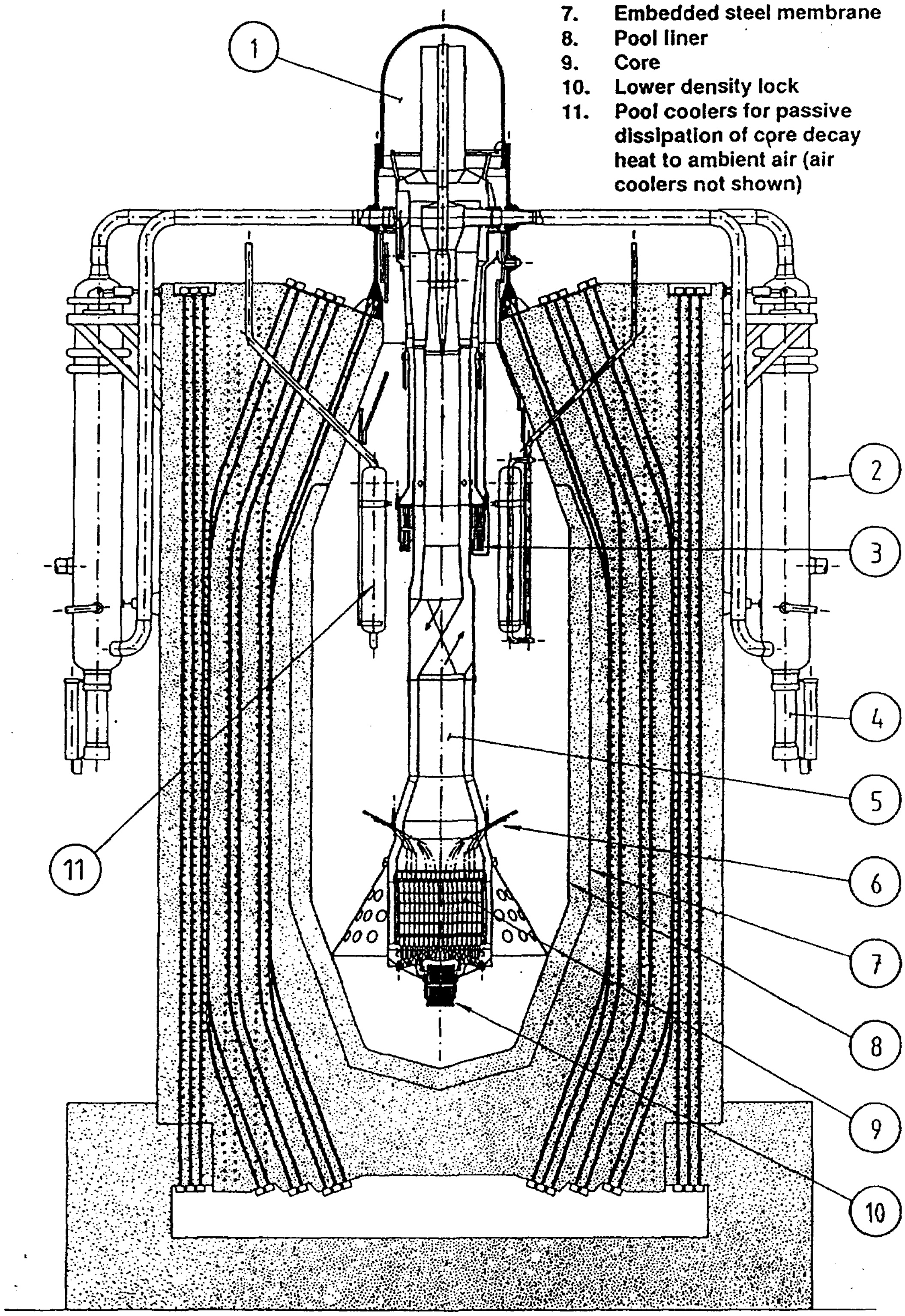


Figure 3

2. CORE PROTECTION

The primary system is connected to the cold pool water through the always open density locks (the upper density lock 3 on Figure 3 and the lower density lock 10 on Figure 3). In this way the cold poolwater is always ready to take over the flow path and to cool the core in case of operating disturbances as overpower, too high primary risertemperature or failure of one or more of the primary pumps.

In case of too high power in the core the primary temperature in the riser increases. The density of the water in the riser is thereby decreased. This will give a larger driving pressure through the density locks acting on the primary circulation flow. If the primary circulation pumps can not compensate for this added pressure by increasing the flow, then there will be some inflow of cold borated water from the pool through the lower density lock. The borated water will mix with the primary system water thereby decreasing the core power by adding neutron absorber.

Ingress of highly borated water also occurs when the primary pressure is lowered, giving void formation in the riser. The mean density of the riser content is thereby lowered giving rise to the same pressure disturbance as overpower and eventually ingress of highly borated water through the lower density lock.

In case of loss of cooling to the steam generators, the primary water temperature is increased, thereby upsetting the pressure balance and leading to ingress of borated water from the pool.

If one or more of the main circulation pumps stop (pump failure or loss of power) then the risertemperature increases giving ingress of borated water from the pool through the lower density lock and shutting the reactor power off.

The specific power of the core is rather low compared with modern PWRs. The data of the PIUS core compared with a modern PWR (Doel 4 in Belgium) concerning thermal rating are very favourable to PIUS as can be seen from the following.

Table I

PIUS FUEL OPERATING DATA

Compared with modern PWR

		PIUS	Doel 4
Operating pressure	bars	90	150
Fuel rod diameter	mm	9.5	9.5
Pellet diameter	mm	8.2	8.2
Average coolant temperature	°C	275	313
Core active height	m	2.5	4.2
Power density	kW/l	72	96
Average rod linear heat rate	kW/m	11.9	16.5
Average cladding heat flux	kW/m^2	400	560
Core coolant flow velocity	m/s	2.8	4.6
Core pressure drop	kPa	36	165

The low fuel rating means that the fuel can cope better with transients, and calculations with the RIGEL model (Reference 3) have shown that Departure from Nucleate Boiling (DNB) is not limiting as for a conventional PWR.

The core is extremely well protected against overheating in a LOCA situation. The core is placed near the bottom of a big pool (~3000 m^3) of cold borated water. The concrete vessel surrounding the pool is prestressed with individual tendons that can be tested during refuelling. Even if half of the tendons fail, the other half of them can keep the vessel intact during normal operating pressure. No pipe break can drain the vessel below a safe level and the concrete vessel has a liner as a seal against pool water leakage. The liner is backed up by a steel membrane embedded in the concrete about half a meter from the inner liner. By these measures it is not credible that a leakage can occur in the concrete vessel. The worst credible LOCA situation will leave the vessel with so much water above the core level that this water is sufficient to cool the core for more than a week by evaporation if all cooling systems are incapacitated.

The mentioned evaporation cooling of the core is to be seen as a (never used) back-up of the passive decay heat removal system.

3. DECAY HEAT REMOVAL

In the pool water there are 8 pool coolers for passive dissipation of core decay heat, see Figure 3, number 11. The coolers are tubed heat exchangers with the pool water in open connection to the shell side. The vertical tubes are with pipes connected to air coolers situated on top of the building. The connection between the pool coolers and the air coolers is always open so that natural circulation transports heat from the poolwater to the ambient air when the poolwater temperature is higher than the air temperature. Even on the air side natural circulation is used. The system is in this way totally passive, starting and working without the use of electric power and driven only by the temperature difference between the poolwater and the ambient air. With seven of the eight coolers in operation the system can take care of the residual heat from the core with the pool water temperature not exceeding 95°C and with the air temperature at 32°C.

In case of LOCA the water level in the pool will always be above the level of the 8 pool coolers. The core will be cooled by natural circulation of pool water through the lower density lock, through the core, the riser and through the upper density lock back to the pool. In the pool the heated water from the upper density lock will enter the upper part of the shell side of the coolers and by natural circulation come out of the bottom part of the coolers shellside.

The whole coupled natural circulation system from core to ambient air lends itself to standard thermalhydraulic calculations and there can be no doubt of the capability of the system.

4. CONTAINMENT

PIUS has a pressurized pipe system outside the concrete pressure vessel and a pipebreak can therefore be postulated. The core is well cooled by totally passive means in all LOCA situations so only a relatively small amount of active matter is released in a pipe break situation. To keep the release to the environment to a minimum, PIUS is provided with a containment enclosing the concrete reactor vessel, the primary loops with steam generators and reactor coolant pumps as well as other high pressure high temperature reactor systems and components.

The containment is of the pressure suppression type used in all ABB Atom BWR plants. The pools for quenching steam and hot water release following a pipe break are located at the bottom of the reactor building.

Because of the passive long term residual heat removal system, no further release of radioactive matter to the containment will occur after the initial depressurization of the reactor system. A containment spray system driven by diesel generators and a system to inject water to the pressure vessel is not required.

In this way only really passive means are used to protect the environment in the long term LOCA situation.

5. SIMPLICITY IN SAFETY

Compared to other LWRs the PIUS safety system is very much simpler and easy to understand for the public. The comparison is most easily understood by reference to Figure 4.

In present generation LWRs core integrity depends on the integrity and function of the equipment in the "outer boxes" in the figure, i.e. instruments such as neutron detectors and level indicators, electronic logic circuits, cable connections, valves, control rod drives etc.

Any such equipment can fail, be inactivated by faulty maintenance, or mistakenly or maliciously tampered with by plant personnel. Recource to redundancy, diversity and spatial separation complicates the design greatly and increases cost but is if anything counterproductive in achieving understanding and confidence.

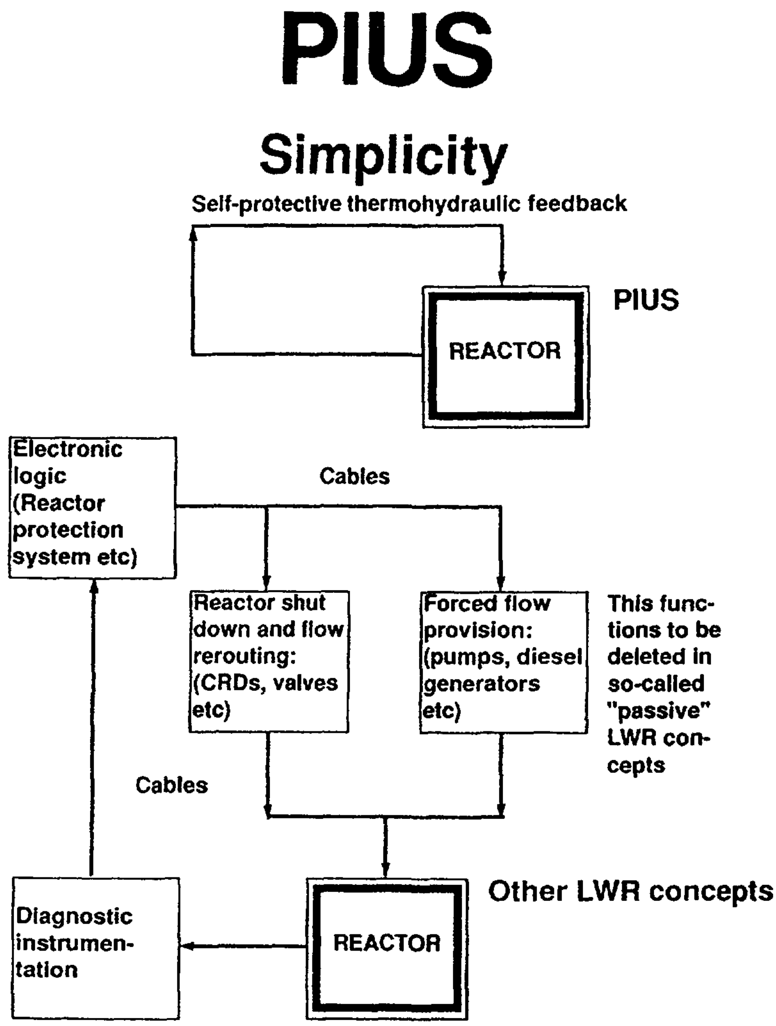
In some recently proposed so called passive LWR concepts the equipment in the right box ("Forced flow provisions etc") is eliminated. Although this represents a significant simplification the dependence on potentially failure prone equipment that can be interfered with remains.

In contrast, in PIUS prevention of large accidents, i.e. preservation of core integrity, is completely independent of such systems and equipment and of any credible structural failure. It is a built-in property of the reactor configuration and the self-protective thermohydraulic feed-back mechanism that it confers on the core cooling system. A lead plant can indeed be tested under conditions normally leading to severe consequences without suffering damage to either fuel or equipment.

6. PLANT OPERATION

PIUS is not just uniquely safe, it will also be a practical and user-friendly power plant.

Power operation is very simple. The combination of once-through steam generation and a strongly negative moderator temperature reactivity coefficient, achieved by means of extensive use of gadolinia burnable absorber,



A comparison of functions needed for core integrity protection in PIUS and other LWR:s

Figure 4

brings in its train automatic load following properties to the reactor. The plant output can be controlled by means of the feedwater pumps and the turbine throttle. Control rods are neither used nor provided and changing the boron content in the coolant can be very infrequent. By allowing the core average water temperature to vary, the reactor power is self-adjusting to the cooling capacity of the feedwater when it evaporates in the once-through steam generator.

The power can be controlled between 100% and 60% with 20%/min and between 100% and 0% with 1 to 2% per minute. Daily load following down to 50% power can be achieved without adjusting the boron content in the primary coolant.

Reactor scram is achieved by tripping one of the four reactor coolant pumps. The remaining three pumps cannot maintain the hydraulic pressure balance in the lower density lock and the result is a temporary ingress of borated water from the reactor pool to the core. The ingress ceases when the coolant temperature in the riser and thereby the buoyance, has decreased to a value corresponding to the core pressure drop maintained by the three reactor coolant pumps in operation. The coolant temperature goes down from 290°C to about 230°C.

7. COSTS

Economic studies have shown that turnkey cost estimate based on Swedish conditions gave a distinct cost advantage for PIUS over the ABB Atom BWR of the same size (which is known to be a very competitive plant).

The results of an independent cost evaluation for US circumstances agree with these conclusions. The US cost evaluation was made in cooperation with United Engineers & Constructors and was based on unit costs and rates from the Energy Economic Data Base (EEDB) and on ABB Atom quantities.

8. VERIFICATION

The principal new feature in the PIUS design is the hydraulic principle with the always open density locks.

At ABB Atom an extensive development program has been devoted to the study of the hydraulic behaviour of the PIUS system and to the density locks.

The hydraulic principle has been studied at the ABB Atom laboratories in a high pressure loop containing all the essential details of the PIUS system. The behaviour of the loop was compared with calculations on a dynamics model. Very good agreements were obtained between experiments and computations. The work is found in Reference 3.

The density lock design is based on an extensive development program covering the last 4 years. Large scale tests have been made at ambient temperature and pressure as well as on a full scale density lock pipe at full pressure and temperature under representative conditions.

Theoretical two-dimensional flow calculation models have been developed and correlated with measurements.

The program has fully shown the functionality of the density locks. The transport of boric acid via diffusion and turbulence through the density locks has been shown to be very low. Spurious boron ingress due to operational transients will not be a problem.

9. CONCLUSION

The PIUS reactor introduces a new dimension in reactor safety. The basic hydraulic design is made so that the core in all plausible events is protected against overpower, DNB, LOCA, malicious treatment and other incidents that are a threat to present LWRs.

The safety merit of PIUS is easily understandable and make many of present LWRs engineered safety systems superfluous. Therefore PIUS shows a simplified plant design and can compete economically in smaller plant size with other forms of power plants.

In the PIUS design there is a technological basis for a change in public perception so that serious accidents (core melt) can be seen as no longer being a threat.

REFERENCES

(1) U. Bredolt et.al:
PIUS, the next generation water reactor.
ANS Topical Meeting on the Safety of Next Generation Power Reactors, Seattle, May 1-5, 1988.

(2) D. Babala, K. Hannerz:
Pressurized Water Reactor Inherent core Protection by Primary System Thermohydraulics.
Nucl Sci & Eng Vol. 90 no 4, 400-410, 1985.

(3) U. Bredolt, J. Fredell:
PIUS self protective Thermohydralics. Transients without safety system intervention.
Contribution to ANS Winter meeting, nov 1989.

CONTAINMENT DESIGN FOR SEVERE ACCIDENTS: DEFENSE OF CONTAINMENT BASEMAT INTEGRITY AGAINST CORIUM ATTACKS

A. TURRICHIA
Direzione delle Costruzioni,
Ente Nazionale per l'Energia Elettrica,
Rome, Italy

Abstract

A device intended to prevent the attack of the molten corium on the containment basemat, in case of a severe accident, is described.
It consists of a flooded stack of staggered stainless steel beams located in an enlarged cavity below the reactor pressure vessel.

---

1. INTRODUCTION

The main purpose of this document is to illustrate a reactor cavity design which, in case of a severe accident with pressure vessel melt-through, is capable of preventing molten core-concrete interaction (MCCI), thereby preserving the integrity of the containment basemat and minimizing the radioactivity release to the environment.
MCCI is bound to take place if the molten corium falls into a dry cavity /1/. There is concern that MCCI may take place also with a flooded cavity if its cross section is small and the fall is massive and sudden. Therefore, after an assessment of what is necessary to avoid MCCI, a solution to the problem has been developped.

2. THE BACKGROUND

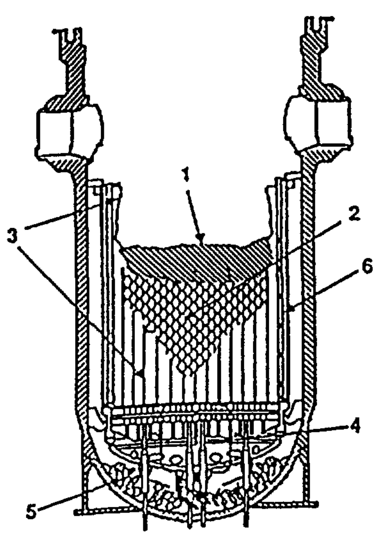
The TMI accident has shown /2/ that the following conditions are sufficient (though, maybe, not strictly necessary) to reduce the molten core core to a coolable configuration (Fig.1):

i) the molten core drops into water;

ii) the fall of the corium into the water is distributed in time (in the TMI accident it took from 20 to 60 seconds for 20% of the molten core to fall down on the bottom of the vessel) and in space (i.e. the falling corium mass is subdivided in several streams of limited cross section);

iii) the surface power density of the debris, referred to the area of deposition, is lower than 0.4 MW/m^2.

The conditions i) and ii) allow the transfer of most of the sensible heat of the corium mass to the water; the condition iii) permits a safe dissipation of the decay power.



ZONE	DESCRIPTION	ESTIMATED QUANTITY (kg)
1	Upper Debris Bed	26,400
2	Resolidified Mass	32,700
3	Intact Assemblies (Partially or Fully Intact)	44,500
4	Lower CSA	5,800
5	Lower Head	19,200
6	Upper CSA	4,200
7	Ex-Vessel	<400
	TOTAL	133,200

FIG. 1. Post-accident estimated core material distribution in TMI-2 /2/.

3. THE FLOODED STACK-OF-BEAMS (SOB) CONCEPT

Basically, the proposed cavity design aims at recreating and enhancing, in the reactor cavity, the corium quenching mechanisms which took place inside the pressure vessel in the TMI-2 accident.

In order to fragment the corium and spread it over a large surface area, thereby obtaining, for the debris, a surface-to-volume ratio which leaves no doubts about their coolability, a cavity design with the following features is proposed for a 1000 MWe plant (Fig. 2):

a) a cavity diameter of 10-12 m;
b) a cavity depth of about 7m below the level normally required, under the vessel head, for instrumentation tubing (in PWRs) or for control rod drive housing and removal (in BWRs); the cavity should be filled with water (borated in PWRs) ready to receive, quench and cool the falling corium for several hours;
c) a structure inside the cavity (called SOB i.e. stack-of-beams) with the task of:
   - breaking up the falling corium;
   - presenting a large horizontal surface, subdivided among various layers, for the deposition of core debris;
   - preventing the arrival of a large amount of debris on the containment basemat.
d) a set of openings in the upper part of the cavity to permit the exit of the steam into the containment atmosphere and the drainage of condensed water back to the cavity;
e) provisions for long term corium cooling.

The part of the cavity immersed in water has a stainless steel liner.

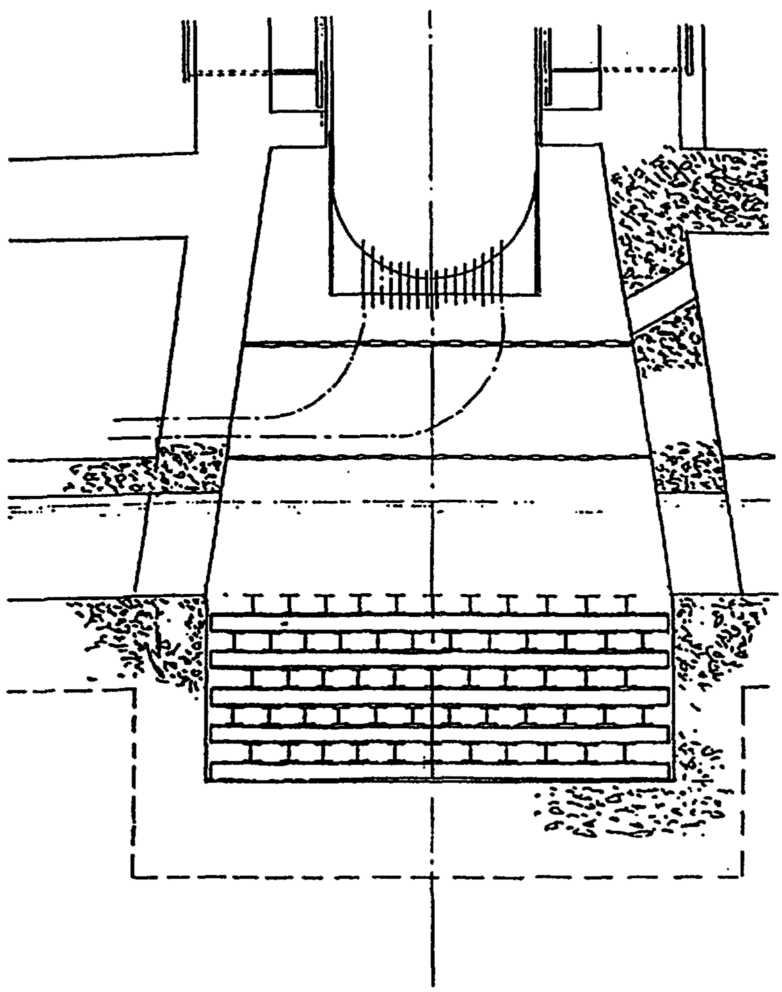


FIG. 2. Cavity design based on the stack-of-beams concept.

3.1 The SOB structure and its interaction with the corium

The proposed SOB structure, shown in Fig. 2, fits inside the lower part of the cavity, has a height of 4 m, and is made up of various layers of SS beams of I cross section with a height and a width of 25-50 cm.

Each layer of beams is rotated 90° with respect to the adjacent one and is shifted sideways a distance equal to the width of beams (25-50 cm) in order to induce a large number of hits, turns, drops and bounces in the falling corium stream (Fig. 3 and 4).

In other words the corium is forced to follow a tortuous path through the water and, in so doing, it is cooled and ends up solidifying and stratifying itself before reaching the bottom of the cavity.

The wings of upper beams are smooth, to limit the amount of molten corium which stops over them; the wings of the lower beams have the shape of a trough, in order to better retain the fraction of the corium deposited on them.

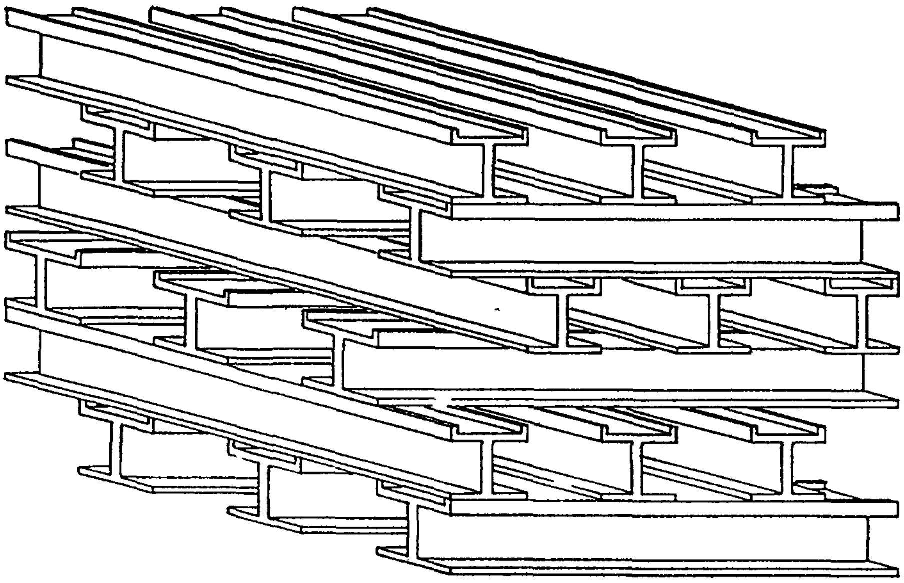


FIG. 3. Pattern of layers of staggered beams.

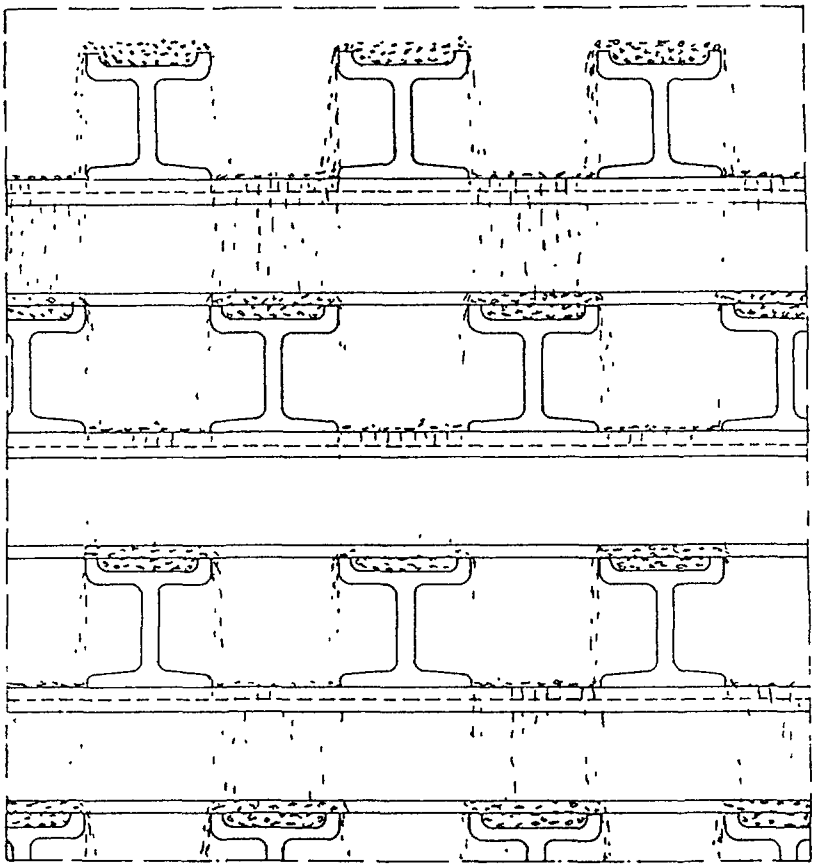


FIG. 4. 'Trevi Fountain' effect of corium dropping on SOB structure.

At their intersection, the SS beams can be bolted or welded in such a way as to realize a strong and monolytic structure capable of maintaining the initial geometry and layout also in the presence of localized pressure forces produced by the violent interaction of the corium with the cavity water.

The uniformity of the spreading of the debris on the SOB is difficult to be assessed theoretically but, apart from the configuration of the SOB structure, the violent interaction of the molten corium with the cavity water is expected to greatly contribute in achieving an adequate spreading of the corium debris.
As observed in the TMI accident it is expected that the corium falling onto the flooded SOB fragment itself into a kind of gravel with a grain size distribution from a few mm to a few cm. But it should be noted that even if the corium does not fragment and maintains, instead, a continuous ingot-like structure, the corium surface-to-volume ratio is increased more than an order of magnitude with respect to that obtainable in most present day cavities (and in effect it rises to about 10% of the value available in an intact core - 4500 m^2 in a 1000 MWe PWR).

3.2 Venting and drainage ducts

In the upper part of the cavity some holes are made for venting the steam or gases emerging from the cavity and for draining condensed steam back into the cavity.

3.3 Long Term Cooling

After the molten core has redistributed itself in the SOB and has been cooled down, it is of course necessary to keep it covered with water or, in other words, to compensate for the water which vaporizes and leaves the cavity after the saturation temperature is reached. If a containment heat removal system (active or passive) is available and if the condensed water can drain into the cavity, the SOB remains covered thereby affording corium cooling for an indefinite period of time. But if the containment heat removal system depends on the operation of active components, in some severe accidents the assumption is made that the CHR system is unavailable. To face that situation it is necessary to have, inside the containment, a large SS-lined, water reservoir (say, a few thousand m^3) which can supply, by gravity feed, coolant to the cavity or which is in continuous communication with the cavity.
The passive PWR and BWR reactors now under study are characterized by the passive dissipation of decay heat to the external environment through the containment dome. If the condensed steam is allowed to flow back to the cavity, continuous corium coverage would be maintained without the need of an additional water reservoir (which however exists, at a high level, to provide core flooding by gravity in case of LOCA).

4. THE APPLICATIONS

The cavity design based on the flooded stack of beams can be applied to all kind of future LWRs.
In addition to the cavity redesign, an internal water reservoir must by accomodated in the large dry containments of PWRs, as sketched in Fig. 5.

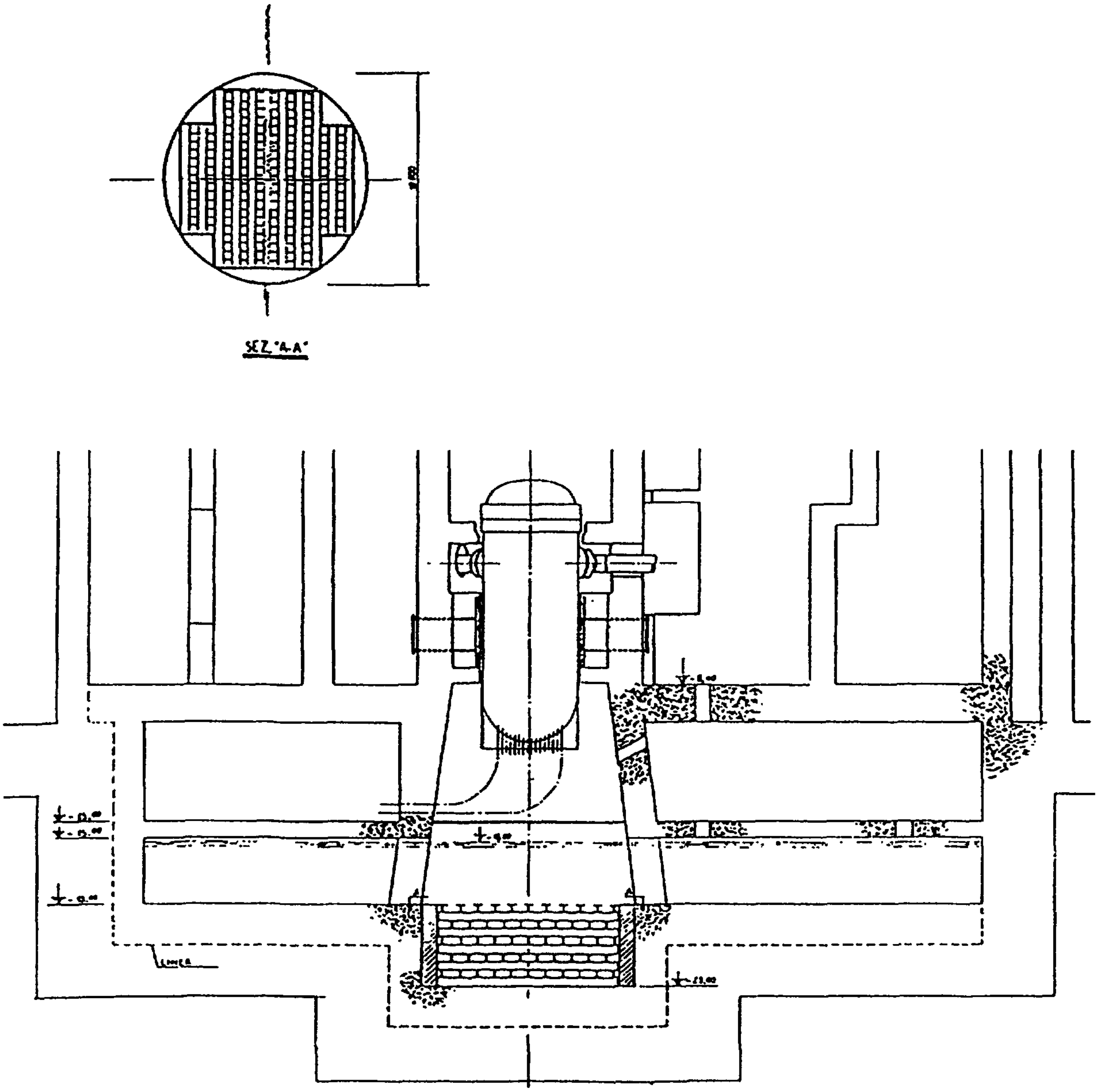


FIG. 5. Large dry containment modified to allocate the SOB structure and the long-term cooling reservoir.

For BWRs it would be necessary to redesign the drywell of the Mark III but no feasibility problems are anticipated. The outer suppression pool is already present in current designs and, with suitable connections, this large water supply can contribute to keep the corium flooded for a long time.

Finally the proposed cavity design is particularly well suited also for the reactors with "passive" safety features such as those now under study (AP-600, SBWR). In fact, with the passive dissipation of decay heat to the environment, it is possible to dispense with the additional water reservoir. Also the filtered venting system might not be necessary. Furthermore, the cavity can be made smaller than the one described in the previous paragraphs because of the smaller reactor size.

5. THE STEAM EXPLOSION ISSUE

The fall of the molten core into water raises the fear of steam explosions. The problem deserves careful attention but should not prevent from taking into consideration design provisions which are potentially beneficial from many other points of view.

First, one should remember that, in most current cavity designs, the possibility of having water in the cavity at the time of pressure vessel melt-through cannot be ruled out and so the problem must be, in any case, addressed.[1]

Second, it must be verified whether the conditions for a steam explosion exist. According to the present trend in severe accident management, when the lower vessel head fails, the primary circuit should already be depressurized; furthermore, the vessel head itself generally presents many preferential places of local failure (instrumentation tubing in PWRs; control rod drive housing in BWRs). In these conditions the fall of the molten corium into the cavity is expected to take place not suddenly but distributed in time, thereby reducing the corium mass involved in a steam explosion.

Third, if the possibility of steam explosion cannot be ruled out, the dynamic loads on the cavity walls and on the containment must be quantitatively evaluated. It may well be that even it a steam explosion takes place it does not damage the containment structure.

Finally, if fears of a damaging steam explosion still persist, a "temporary", dry, refractory core receiver placed under the vessel and above the water, could help in allaying these fears. In fact, by placing a suitable number of melting plugs in the bottom of the corium receiver, it would be possible to "regulate" (slow down) the rate of corium fall in to the water at a value considered safe. The

---

1 This problem has actually been addressed for some operating reactors and the conclusion has been that the presence of water in the cavity of large containments (e.g. Zion, Sequoyah) is a desirable feature because, at least for some severe accidents, it provides a mechanism for quenching the molten core without causing excessive loads on the containment /5/. With the solution proposed in this paper the quenching of the molten core is extended and guaranteed to all severe accidents with pressure vessel melt-through .

only drawback would be a temporary increase in the release of radioactivity to the containment atmosphere and, of course, the structural complications associated with the added structure.

6. TRANSIENT ANALYSES

(The author is indebted to Mr. G. Mariotti of the ENEL Center for Nuclear and Thermal Research at Pisa, who performed the transient analyses).

6.1 Pressure and Temperature transients in the containment

Preliminary pressure and temperature transients in the large dry containment of a 1000 MWe PWR have been computed for for the following sequences:

- Large LOCA with no safety system operating (AB);
- Large LOCA as above but with containment spray system operating (AD);
- Small LOCA with no safety system operating (SE);
- Total Station Blackout (TE or TMLB).

The pressure transients, obtained with the MARCH-3 Code, for the TE and AB seqeuences are shown in Fig. 6. With reference to these curves, it should be pointed out that a total of 4000 m^3 of water has been assumed to exist inside the cavity and the auxiliary reservoir. Furthermore, a primary circuit depressurization has been introduced at the time of core uncovery. However, for the time being,

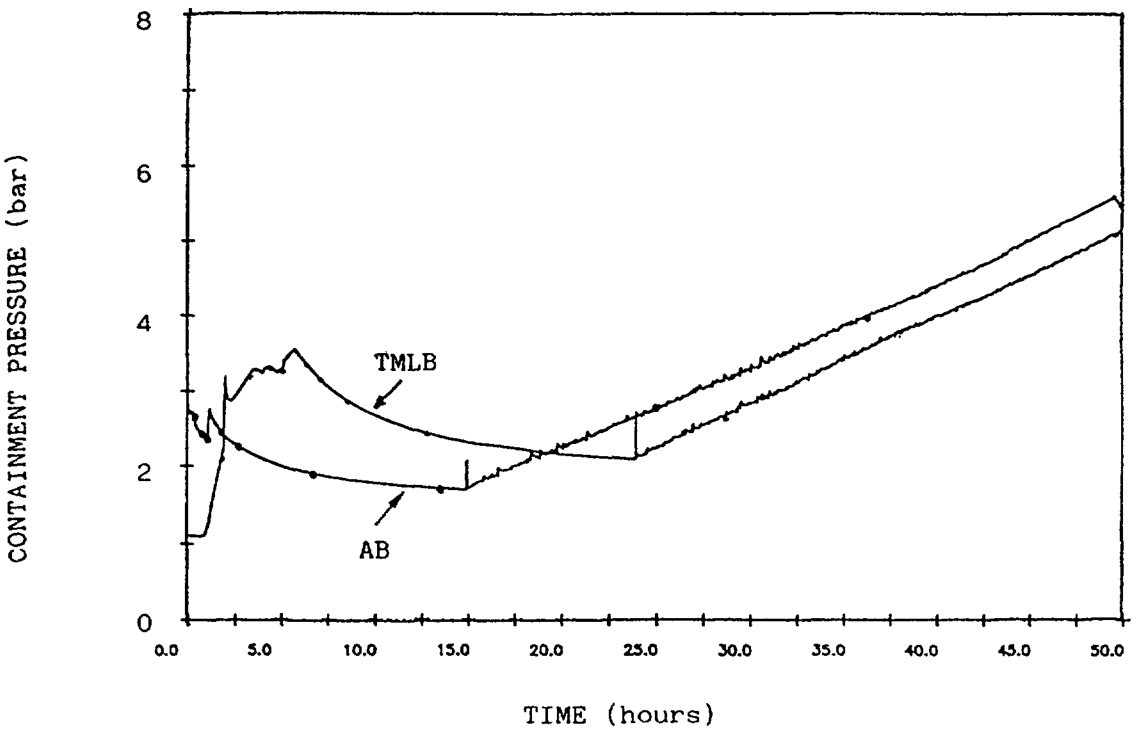


FIG. 6. Pressure transients in a large dry containment for two typical severe accident sequences.

because of code limitations, it has not been possible to simulate the quenching of the primary coolant into the auxiliary reservoir during the depressurization phase.

It is interesting to note that the containment pressure remains below the expected venting setpoint (0.55 MPa) for more than two days, leaving ample time for recovery of a containment (air or water) heat removal system. This recovery would prevent the containment venting, which remains, in any case, the last overpressure protection feature.

6.2 Temperature transients in the SS beams

Some preliminary calculations have been performed to determine the foreseable temperature transients in the wings of the beams receiving directly the impact of the molten corium.

In Fig. 7 the temperature profiles in the wing of a beam are shown at various times after the corium arrival, for a typical case.

As shown in the grafic, by making the conservative assumption of a continuous, uniform and initially molten corium layer (3.2 cm thick) over the SS wing (4.8 cm thick), the interface temperature reaches immediately a value of about 1000°C, raises somewhat above this value for about 15 min and decreases slowly thereafter. However it should be pointed out that if the corium has not a continuous ingot-like structure but has instead a gravel-like structure, its equivalent thermal conductivity is much lower and the corium-SS interface temperature is also much less than the value calculated above. Of course if the corium thickness is lower, the time at high temperature is reduced.

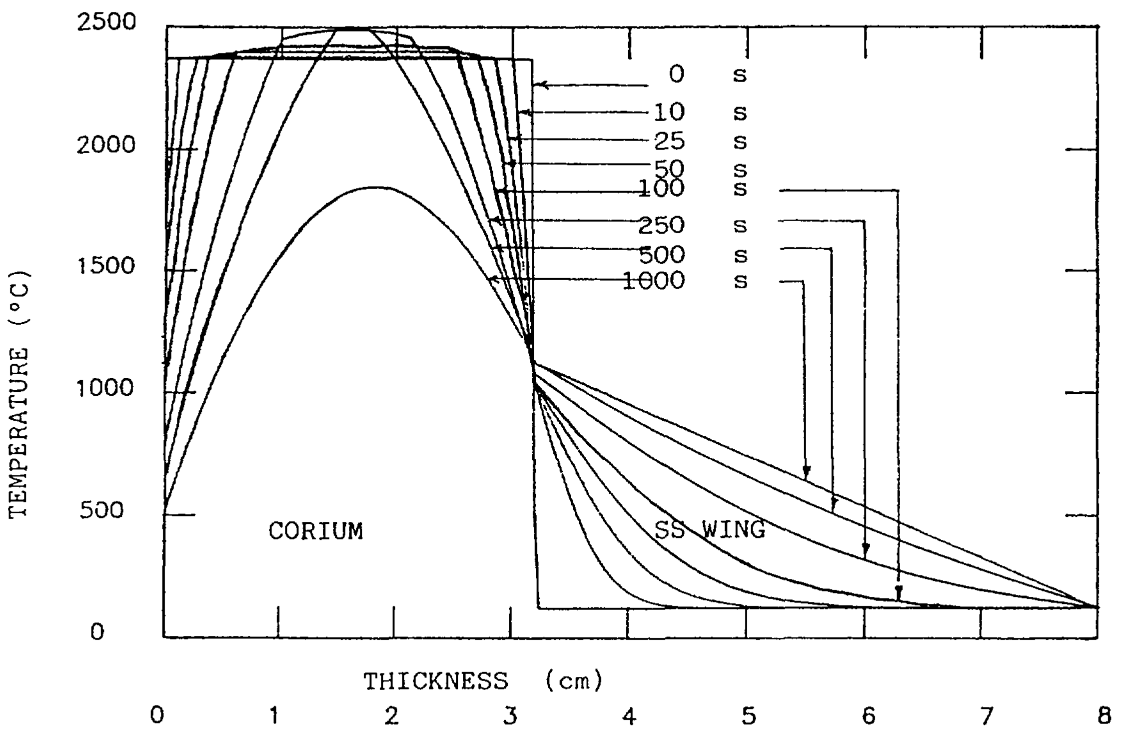


FIG. 7. Temperature profiles in the corium and in the SS wing after the fall of the corium on the SOB.

7. CONCLUSIONS

The cavity design based on the flooded stack of beams concept (SOB) has been derived from a careful examination of the core meltdown phenomena which have taken place in the TMI-2 accident. This cavity design, simple and fully passive, allows the coolability of the corium in case of pressure vessel melt-through, even if the entire core were to come out of the vessel, and prevents the molten-core-concrete interaction thereby preserving the integrity and leaktighkness of the containment basemat. This is basically due to the tortuous path that the molten corium is compelled to follow during its fall and to the three-dimentional redistribution of the corium debris on a multi-layered surface area which is an order of magnitude larger than that of present reactor cavities. The large surface to volume ratio of the debris leaves no doubts about their rapid quenching and continued coolability.
The SOB concept can be applied to all kind of reactors and is well suited also for the so-called "passive" types now under development. More details on the proposed solution are described in Ref. 4.

REFERENCES

/1/ Alsmayer, H., "Recent results from BETA/WECHSL melt-concrete interaction analysis", Paper presented at the International ENS/ANS Conference on Thermal Reactor Safety, Avignon 2-7 October 1988.

/2/ Eidam,G.R. et al., "TMI-2 defuelling conditions and summary of research findings", IAEA-SM-296/74, Paper presented at the Symposium on Severe Accidents in Nuclear Power Plants-Sorrento 21-25 March, 1988.

/3/ IDCOR Technical Report 20.1-Core Retention Devices - July 1983.

/4/ Turricchia,A., Containment Design for Severe Accidents: Defense of Containment Basemat Integrity against Corium Attack, ENEL Report 9NO 2110 TNIU 0001, Roma, Feb. 16, 1989.

/5/ U.S. NRC., Severe Accident Risks: An Assessment of Five U.S. Nuclear Power Plants, Summary Report, Second Draft for Peer Review, Rep. NUREG-1150 , VOL. 1, Pages 5-12, 7-9, 9-9 and 9-10. (June 1989).

TERMINOLOGY FOR FUTURE NUCLEAR POWER PLANTS

E. LO PRATO, G. PETRANGELI,
R. TONONI, C. ZAFFIRO
Directorate for Nuclear Safety and
Health Protection (ENEA/DISP),
Rome, Italy

Abstract

The growing interest of the Technical Community and of the Public in advanced nuclear plants designed according to specific safety principles (such as passive safety) require the adequacy and consistency - still not well established - of the pertinent terminology. A Working Paper Draft on this subject was prepared recently under the auspices of IAEA: an additional contribution is given by the present paper, which discusses interpretation and use of terms already defined in the Draft, and suggests the introduction of new terms, useful to better characterize the safety features of advanced future plants.

Concerning previously defined terms, the present paper suggests:

- caution in the use of terms such as "inherent safety" and "inherently safe", which require in any case specification of the hazards avoided or eliminated by means of inherent safety features;
- an enlarged scope of the "passive safety" term, to include systems which perform passively safety functions, but rely for their activation on suitable internal "self-acting" devices (to these systems could be assigned a further category of passivity, in addition to the three ones proposed in the W.P. Draft);
- a revised definition of the "grace period" concept, which should point out the correlation between grace period duration and limits of the accident consequences and and also take into account the advisability of plant monitoring during the same period; as a consequence, the use of "walkaway safe" should be discouraged.

Moreover, the present paper proposes the introduction of the following terms:

- "inherent and passive safety plant", to define an advanced plant in which the essential safety functions (reactor shutdown, emergency

core cooling and F.P. containment) are achieved by means of inherent characteristics - to the extent possible - and by passive systems; the requirements for these plants should include an adequate "grace period" and very low accident consequences even for low probability events ("reference bounding events");

- "reference bounding event", to indicate an event (of a class of very unlikely events defined for plant safety assessment purposes), which bounds any uncertainty in event frequency analysis and equipment performance evaluation and can be identified by engineering judgement supported by probabilistic considerations;
- "not by-passable", to highlight the contribution to the availability of a passive safety system given by passive means preventing human error.

---

1. INTRODUCTION

In view of the importance of communicating with the Public and within the Technical Community, it is necessary to assure adequacy and consistency of the terminology adopted for describing the safety characteristics of some future nuclear power plants - in particular of those often defined "inherent" and/or "passive safety" - in order to reach an international consensus on what the used terms mean and imply. Actually, it is very important to avoid confusion and misuse of terms, also to enhance the confidence of the Public in technical discussions.

A remarkable attempt in the above direction was made recently under the auspices of IAEA: a "Working Paper on Safety Related Terms", drafted by the pertinent Technical Committee and by a Consultants Meeting held in Vienna in 1988, was subsequently distributed through official channels as an eclosure to the IAEA letter of invitation at the "Technical Committee on Passive Safety Features in Current and Future Water Cooled Reactors", held in Moscow, on March 21-24, 1989.

The present paper makes reference to the quoted Working Paper (called W.P. Draft in the following) and discusses some safety related terms therein defined, as well as additional terms. Among the already defined terms, the paper focuses attention mainly on those of general scope, such as "inherent safety" and "passive safety", but also considers other terms, like "grace period" and "walkaway safe", related to specific safety features of future nuclear power plants. Definitions of additional terms suggested by the present paper are: "inherent and passive safety plant", "reference bounding event" and "not by-passable", useful for a better understanding of future plant designs and of the issues such designs imply.

Other safety related terms, which are already used for regulatory or assessment purposes, are not covered by the present paper, (even if they are discussed in the reference Draft) since it has the only aim to provide a further contribution for the definition of an adequate terminology applicable to plant concepts now in development.

2. DISCUSSION OF TERMS DEFINED IN THE W.P. DRAFT

2.1 Inherent safety

The term "inherent safety" generally means the achievement of safety through elimination or avoidance of plant inherent hazards. In a nuclear power plant these hazards are related to design and operating plant features, and possibly to site characteristics, which determine physical situations with potential threat to the safety, including human injury, damage to the environment or some combination of them. Usually, the dangerous potentials of these hazards are released by events or chains of events, due to hardware faults or human errors, which impair the plant defences.

The primary hazard, related to an operating characteristic of the plant, is the building-up of fission products in the reactor fuel, and the associate decay heat, which require - in lack of control - the emergency shut-down of the reactor and its cooling, in order to avoid degradation of fuel claddings and massive release of radioactive contaminants inside the pressure boundary and beyond it.

Examples of inherent hazards related to the reactor design are: the core reactivity excess and its associated potential for nuclear power excursions; the chemical incompatibility between core materials in certain physical conditions, which can produce significant energy release by chemical reactions, if these conditions are reached (e.g. H_2 production by metal-water reactions in LWRs). Another hazard related to the plant design is fire, that is the existence of combustible materials inside the plant areas.

The site may contribute to the plant hazards by means of its seismicity, or its capacity to produce flood; other site hazards may be related to man-induced external events.

It has to be pointed out, in plant safety assessment, that an event or a chain of events may release in the same time the dangerous potentials of several hazards. For example, hardware faults or operation errors may produce a reactivity accident; an earthquake may damage plant structures and equipment. Any of these accidents may result in degradation of fuel-claddings and/or in pressure boundary ruptures, hence in fission products release, that is in the fearful effects of the primary hazard release. The importance of such hazard is largely predominant, so that, in a nuclear power plant, the other hazards are evaluated primarily looking to their capability of releasing it.

By definition, the inherent capability of eliminating a hazard exists only if no "ad hoc" safety action (manual or automatic, active or passive) is required to counteract the hazard. Therefore, the above capability must be tied - in principle -to basic features of the plant systems, such as the characteristics of the utilized materials, which make the hazard of no safety concern anyway. For instance, a plant in which no combustible materials are employed is inherently safe with respect to fire. A negative temperature coefficient makes a reactor inherently safe against reactivity and overpower hazards (reactivity accidents) provided that the same coefficient cannot be vehicle of process perturbations able to generate dangerous reactivity transients: the compliance with this condition depends on the plant concept. More generally, as shown by the previous examples, a plant safety feature may be effective only against one hazard, or a limited number of hazards; therefore the eliminated hazards must be specified when discussing the plant inherent safety characteristics, to avoid ambiguities and misunderstandings.

Unfortunately some hazards, by their very nature, are strictly related to the basic conception of a nuclear reactor and cannot be eliminated (i.e. by inherent defences) even if they can be successfully controlled and the consequences of their release be lowered to acceptable limits through the intervention of reliable safety systems. On the other hand, engineering and technological problems often limit the feasibility of inherent defences against other hazards: a typical example is fire. As a further example, the use of an inert gas as primary coolant makes the plant inherently safe against chemical hazards due to fuel-coolant interactions, until the primary circuit tightness is maintained and entry of air or water-vapour in the primary circuit is avoided (in such case, the effectiveness of an inherent safety feature is conditioned by the integrity of a "passive" defence: the primary pressure boundary). Therefore, to conceive and build a nuclear power plant based only on the principle of inherent safety does not appear a realistic aim. That has to be accounted for when discussing, mainly with non-technical people, about future advanced plants.

In particular, a plant provided with a safety feature, which is able to eliminate an inherent hazard, may be defined "inherently safe" only with respect to the eliminated hazard (such feature, as elsewhere stated, should not be subject to failures of any kind). But the use of the term "inherent safety" or "inherently safe" without specification of the intended hazard is misleading and should be avoided.

2.2 Passive safety

With respect to the hazards for which a nuclear power plant is not inherently safe, "ad-hoc" safety functions must be provided to counteract these hazards, in practice to prevent any event able to release the dangerous potential of them or to mitigate the consequences of such release.

The term "passive safety" is currently used to qualify the operating safety features of structures and devices (systems and components) designed to counteract specific events without reliance on mechanical and/or electrical power, forces or "intelligence" signals external to the same structures or devices. These features should rely only on natural laws and properties of materials, as well as on lack of human action, so that they are, in principle, very effective in the prevention of equipment failures and of human error. In practice, the applications of the passive safety principle depend on the functions to be performed and on the technology required by specific plant concepts; therefore they are represented by very different design solutions at system level, characterized by different "degrees" of passivity: that will be the main subject of the following considerations. Moreover, accounting that the passive safety features of a plant are effective only against one or a limited number of hazards,the counteracted hazards should be specified when discussing passive safety features of the plant. In addition, the endurance of any passive system performing a safety function and the consequence limit compatible with the success of the function itself should be specified (see also the comments on the "grace period" definition).

Passive safety devices are currently used in the nuclear power plant technology: the pressure boundary of a reactor is a typical passive protection barrier against the release of radioactive contaminants dispersed in the primary fluid; a similar function is performed by a reactor containment structure, mainly in accidents with degradation of the pressure boundary, even if the containment function as a whole, performed by a number of structures and interacting systems, is not completely passive in most nuclear plants. Passive protection of the plant against the seismic hazard is assured by the design of plant buildings to the pertinent seismic class rule and by the coherent seismic design/qualification of the essential plant equipment. Moreover, the class of passive components includes: fire proof doors and penetrations separating adjacent fire areas, rupture disks, accumulators and so on.

A variety of passive safety system has been designed for future nuclear power plants, expecially for the small-sized innovative ones: examples of such systems are: the emergency shutdown/cooling system of the PIUS plant; the water-wall heat removal system designed for the SBWR plant; the containment emergency cooling systems of the AP-600 and MHTGR plants. Several systems of this class largely use proven passive components; however, new components were conceived for specific applications (i.e. the "density locks" of the PIUS plant). In the mentioned plant designs a more extensive application of the passive safety principle - with respect to other, even if advanced, designs - is allowed by their sizing and system simplification, and is adopted as a suitable way to improve the availability on demand of their safety systems, eliminating "by the roots", to the possible extent, any problem related to hardware faults, energy loss and human error.

It has to be pointed out that the implementation of the "passive safety principle" may or may not exclude the physical movement of fluid masses and/or mechanical parts, which might be subject to certain kinds of failures or human interference. Therefore, different categories of passive safety devices should be considered, depending on how the passive safety concept is implemented. The W.P. Draft considers a classification in three categories, each related to the operating features of the systems performing safety functions: only in a static mode (e.g. by thermal radiation between opposed surfaces), or by some movement of fluid (e.g. by natural fluid circulation), finally by movement of fluids and mechanical parts (e.g. by natural fluid circulation activated by rupture disks or check-valves). Clearly, going towards categories of higher order, the passivity degree of the systems decreases. However, such decrease must not be related to a progressive reduction in the reliability or availability figures of the systems, which are conditioned by a series of other factors, including design, construction, installation and maintenance.

The mentioned Draft does not include in the class of passive safety systems those performing the intended functions in a passive way, but dependent on internal non-passive devices or subsystems for alignment/initiation purposes. Examples of already designed systems of this kind are the emergency cooling or injection systems of some new LWR designs, which perform passively their cooling functions by gravity-driven or N_2-pressure driven circulation of water, provided that their activation is made by opening of electrically-operated or electropneumatic valves. Really, the initiation logics of these systems, at the present stage of their design, seem to be still dependent on external power sources and activation signals: this feature should not assign to the mentioned systems the independence characteristics claimed for the passive systems. However, systems of the same kind, but exempt from the same drawback, appear feasible; in particular, suitable activation subsystems, relying only on internal power sources and signals, could be conceived and designed.

Any system (or subsystem) not made by passive components only, but independent on external "intelligence" inputs and power sources or forces for its actuation, is defined "self-acting" or "autonomous" in the already quoted W.P. Draft; on the other hand, the same document considers still passive any component relying only on internal inputs and forces for its actuation (see par. 2.2-1 of the Draft). That appears somewhat inconsistent and may be cause of ambiguities, since it is not always simple to distinguish between systems and components, or the distinction is based on questionable conventions. However it is more important to observe that a self-acting system or subsystem could not differ from a passive one performing the same function, as far as the availability on demand is concerned (which is the ultimate aim of a passivity requirement) if it is designed with adequate characteristics of reliability, fail-to-safety and immunity from human error.

According to the above considerations, a fourth category of passive systems may be added to the three defined in the W.P. Draft. Such category, corresponding to the lowest level of passivity, should include any system which relies on natural forces or energy sources to perform the intended function, but on self-acting devices of acceptable design for the initiation of the same function. The acceptance criteria of the initiation subsystem should regard essentially: reliability, independency from external events and common mode faults, fail-to-safety and freedom from human error.

In order to highlight the difference between a passive safety system of the fourth category and a self-acting safety system, it may be pointed out that the latter may require internal power sources both for initiation purposes and, later on, to perform the initiated function, without human action and throughout the time requested by safety requirements.

A proposal for categorization of passive systems according to the above criteria is presented in the Appendix to the present paper, together with examples of application.

2.3 Grace period/walkaway safe

A "grace period" is a new general requirement for future plants, which enlarge, in a sense, a similar requirement applied in some countries to current plants, in order to assure their safety in front of special events (man induced external events). It implies that the passive safety systems provided to mitigate the effects of unfavourable events are able to perform their functions without human intervention and for a sufficiently long time to assure that any accident is terminated and the plant control fully recovered. The events to be considered are those to which reference is made in the plant design and for plant safety assessment purposes, including the class of "bounding events" (see par. 3.2). The latter are of outstanding importance to evaluate the adequacy of the grace period duration and of the relative plant conditions.

During the grace period the external release of radionuclide harmful to human health and for land contamination should be adequately limited by means of the physical containment barriers of the plant. Obviously, the acceptable limit of the external consequences must be defined with reference to the most severe (bounding) events considered in the plant design. For several new plant concepts, the conformance to the last requirement could be assured through passive control of the containment temperature and pressure, and possibly using passively actuated filtered venting systems.

The W.P. Draft defines "grace period" a period of time following an incident/accident, during which the safety of the plant is assured without the need for personnel action or attendance. Such definition apparently does not correlate the duration of the grace period to a limit of external radiation dose which cannot be exceeded during the same period. Moreover, it does not take into account the advisability of the plant monitoring during the grace period. Therefore, the mentioned definition should be revised, as a minimum suppressing the word "attendance" (or even specifying better its significance) and making explicit reference to the acceptable level of the external accident consequences. A tentative revised definition of "grace period" will be given in par. 4.

Similar considerations could be applied to comment the definition of "walkaway safety" given in the mentioned W.P. Draft (a plant safety condition ensured for a protracted period of time, after an accident, without personal action or attendance). Such definition does not express correctly the safety philosophy on which the requirement of a "grace period" is based; moreover, a specific term should not be needed to qualify the plant safety condition during the grace period. Accounting for that, the use of the term "walkaway safety" should be discouraged.

3. DEFINITIONS OF NEW TERMS

3.1 Inherent and passive safety plants

The common term "advanced plants" is related, at present, to a variety of plant designs, which range from large LWR plant designs (such as ABWR and APWR) to the designs of smaller-size units based on the same proven technology (such as SBWR and AP-600) and to other more innovative plant designs, which require less known technologies (examples are: the PIUS plant and some HTGR designs). It is difficult, especially for non-skilled people, to distinguish among so different plant concepts and reach an adequate understanding of the safety approaches followed by their designers, if explained by use of somewhat inconsistent terminologies. In particular, it is difficult to identify, on these bases, differences in the application extent of some safety principles, such as those of inherent and passive safety.

Therefore, mainly to avoid confusion and misunderstanding when communicating with the Public, it may be useful to adopt the term "inherent and passive safety plant" to indicate any advanced plant in which the essential safety functions (emergency reactor shutdown/cooling and fission products containment) are achieved by means of inherent characteristics - to the extent possible - and of passive systems. In such plants the passive safety systems should integrate effectively the inherent plant defences, counterbalancing their weaknesses due to conception or engineeering limitations, and should ensure an adequate level of freedom from hardware faults and human error. Moreover, the passive safety systems of these plants should be demonstrated capable to perform the intended functions in front of an extended set of internal and external events and for a period of time sufficient to terminate the accident (without exceeding acceptable consequence limits) and to allow recovery action. A discussion of what the requirement of passive safety can imply, as far as constitutions and specifications of the safety systems are concerned, is included in the Appendix to the present paper.

A number of plant concepts now under development has the potential of satisfying the above definition: it should include some "simplified" and small-size LWRs, such as the SBWR and AP-600 plants already mentioned, and primarily more innovative plant concepts such as the PIUS one. However it is too early for estimating to what extent such previsions will be confirmed in the near future. Indeed, engineering designs and safety analyses of the quoted plants are still incomplete; very likely, some of them could require only improvements and/or development of suitable "safety options", but others may require significant research and development effort, to confirm the expected performances of systems and components.

Design developments and relative analysis/experimentation programs will also highlight possible differences in performance and safety characteristics among the plants included in the class defined above. For instance, expected differences regard: the exploitation level of the inherent safety principle, the passivity degrees of the safety systems and the implementation of the "defence in depth" principle, with particular reference to the strength of single barriers and to the capability of one of them to support another or compensate for accidental reduced effectiveness of it.

3.2 Reference bounding events

The safety assessment of "inherent and passive safety plants" may require an integrated safety approach, based essentially on deterministic criteria and requirements supported by probabilistic evaluations, as well as on the consideration of an extended set of "reference events", in front of which the adequacy of the plant defences should be demonstrated.

In particular, for the quoted plants, the term "reference event" should be intended as having an enlarged scope: it should include events ranging from the present AOT (abnormal operating transients) and DBA (design base events) to the class of "severe" and "boundary" events now considered in evaluating plant design margins and problems related to emergency planning and management. However, allowance must be given to the differences existing between the quoted events in expectation frequencies, possible consequences and means of defence required. Accordingly, it is appropriate to distinguish different classes of reference events: an example is the event classification made by N.R.C. for advanced future reactors developed in U.S. (see NUREG 1226), which may be considered a sound and rational approach to the problem of coupling events, defence requirements and safety assessment.

A special consideration must be given, in this context, to the very unlikely events included in the third class of the above example, which are characterized by very difficult assessment and existing uncertainties in expectation frequencies. The individuation of one of the above events, which can be termed "reference bounding events", should be based on a deterministic assessment of a set of plant states and failure modes (which bound the existing uncertainties in the event frequency analysis and plant performance evaluation) making use of engineering judgements supported, in case, by probabilistic considerations. However, the application level of this approach is strictly dependent on the available experience on the concerned plant concept, and could require, in some cases, a substantial program of analysis and research, including experiments on prototypes or lead plants.

3.3 Not by-passable

A nuclear power plant should have the capability - inherent in the design - to prevent any human error affecting the availability on demand of the essential safety systems. Attention must be focused on mistakes, omissions or off-rule manouvres, made by the operator when performing his functions in plant operation control, maintenance, in-service inspection and testing. Such prevention should be achieved by means of hardware provisions: obviously, for a passive safety system, passive prevention means should be utilized.

To indicate that a passive safety system is equipped with prevention means of this kind, the system may be defined "not by-passable". The concept expressed by this term integrates usefully the concepts expressed by other terms defined in the W.P. Draft ("fool proofness" and "error tolerance") in highlighting the soundness and the effectiveness of a passive safety function in front of possible undetected degradations induced by human error.

4. REVISION AND NEW DEFINITIONS OF TERMS

On the basis of the previous considerations, a proposal for the definitions of the terms already discussed follows. It is limited only to the terms included in the mentioned W.P. Draft, which could be subjects of revised definition, and to the new terms proposed in the present paper.

- Passive component

  A component which performes its function without need for any external force, power source or actuating signal. The function is performed by static or dormant unpowered or self-acting means.

- Active component

  Any component which is not passive.

- Passive safety system

  A system composed only of structural parts and of passive components, possibly integrated by self-acting devices of suitable design, which performs a specific safety function.

- Passive safety function

  A safety function to be achieved primarily by exploitation of natural laws and anyway without need for human intervention and for power sources, forces or "intelligence" signals external to the system which performs it.

- Not by-passable

  A passive safety system whose availability on demand is assured by provisions including passive means to prevent human error.

- Self-acting system

  A safety system which may contain active components, but relies only on internal power sources or forces and internal "intelligence" inputs for carrying out the intended function.

- Inherent hazard

  A plant physical situation (related to a design or operating feature, or a site characteristic) with a potential threat to safety.

- Inherent safety characteristic

  A plant characteristic which avoids or eliminates a specified inherent hazard, relying only on choice of materials, design features and spontaneous exploitation of natural laws.

- Grace period

  A period of time, following and accident, during which the plant safety and an acceptable limit of external accident consequences are ensured without necessity of personnel action.

- Inherent and passive safety plant

  A nuclear power plant in which the fundamental safety functions (emergency reactor shutdown/cooling, and F.P. containment) are achieved by means of inherent characteristics - to the extent possible- and by passive systems capable of ensuring acceptable accident consequences in front of an adequate set of events and for a period of time sufficient to terminate the accident and allow recovery action.

- <u>Reference event</u>

  Any event challenging the plant safety, which must be considered in the plant design.

- <u>Reference bounding event</u>

  A reference event which bounds any existing uncertainty in event frequency analysis and equipment performance evaluation.

APPENDIX

PROPOSAL FOR CATEGORIZATION OF PASSIVE FUNCTIONS AND OF SYSTEMS OR COMPONENTS

The contents of this Appendix - to be compared with those of the Appendix A to the W.P. Draft - were developed with the aim of integrating and clarifying, also by application examples, the considerations previously reported in the present paper.

A.1 Passive systems

- <u>Category 1</u>

  The systems of this category require:

  . no signal inputs of "intelligence", no external power sources or forces,

  . no moving working fluid,

  . no moving mechanical parts.

  The no-motion requirement does not regard the effects of possible changes in geometry due to inherent properties of materials (such as thermal expansion).

  Examples of safety systems included in this category are:

  . physical barriers against the release of fission products, such as: nuclear fuel claddings, pressure boundary systems and containment buildings;

. hardened building structures for the protection of a plant against seismic and or other external events;

. core/containment cooling systems relying on heat radiation from nuclear fuel to outer structural parts, with the reactor in hot shutdown (as it is foreseen for the MHTGR plant).

- Category 2

The systems of this category require:

. no signal inputs of "intelligence", no external power sources or forces,

. moving working fluids and/or

. no moving mechanical parts.

The fluid movement is only due to thermoidraulic conditions occuring when the safety function is activated. No distinction is made among fluids of different nature (i.e. borated water and air) although the nature of the moving fluid may be significant for the availability of the function performed by a system of this category.

Examples of safety systems included in this category are:

. reactor shutdown/emergency cooling systems based on injection of poisoned fluid produced by the rupture of some hydrostatic equilibrium between the pressure boundary and an external water pool (a concept developed for the PIUS plant);

. reactor emergency cooling systems based on air or water natural circulation in heat exchangers immersed in water pools (internal to the containments) to which the core decay heat is directly transfered by passive design provisions (again, PIUS plant);

. containment cooling systems based on natural circulation of air flowing beside the containment walls, with intake and exaust through a stack (solution foreseen for the AP-600 plant) or in tubes covering the inner walls of the "silos" (for underground reactors, such as PRISM and MHTGR).

- <u>Category 3</u>

The systems of this category require:

. no signal inputs of "intelligence", no external power sources or forces;

. moving working fluid and/or

. moving mechanical parts.

The fluid motion is characterized as in cat.2; mechanical movements are due to unbalance between forces already incorporated in the system (e.g. static power in check - and relief valves, hydrostatic pressure in accumulators) and forces directly exerted by the process.

Examples of safety systems included in this category are:

. emergency injection systems made by accumulators or storage tanks and discharge lines equipped with check valves (AP-600 plant);

. overpressure protection and/or emergency cooling devices of pressure boundary systems based on fluid release through relief valves (boiling and pressurized water reactors);

. filtered venting systems of containments activated by rupture disks (containment overpressure protections presently adopted in some BWRs and PWRs).

<u>Category 4</u>

The systems of this category (not included in the passive safety systems classification of the W.P. Draft) require:

. no external signal inputs of "intelligence", power sources or forces,

. moving working fluid and

. moving mechanical parts.

In a system of this category, a self-acting sub-system, including logics (activated by dedicated process input signals) and actuation devices, enables the operation of a passive sub-system devoted to perform the intended function. Mechanical movements may be ascribed both to some components of the self-acting sub-system and to components of the other sub-system; indeed, the initiated passive function is performed as in a system of Cat. 3. As previously stated, fundamental features of the self-acting sub-system are: fail-to-safety, reliability and freedom from human error (due importance should be given, in this context, to the "not by-passability" characteristics). The result should be the best fitting between the two sub-systems, concerning the availability on demand of the system as a whole.

Example of safety systems included in this category could be:

- emergency core cooling/injection systems, based on gravity-driven or N_2 pressure-driven fluid circulation, initiated by fail-safe logics actuating electric or electro-pneumatic valves;
- emergency core cooling systems, based on gravity-driven flow of water, activated by explosive valves which break open on demand (if a suitable qualification process of the actuators can be identified);
- emergency reactor shutdown systems based on gravity-driven, or static pressure - driven control rods, activated by fail-safe, trip logics.

Safety systems of this category are included in - or may be developed for - the most important designs of advanced future nuclear power plants.

A.2 Passive components

The above categorization may be applied also to passive components of any system which performs passively a safety function. That is pointed out in the Appendix A of the W.P. Draft, which gives some application examples, of course limited to the three categories of passivity it considers.

Here following a further set of examples is given, which also regards the fourth category of passivity proposed in the present paper.

- Category 1

  This category includes static components of safety related passive systems (e.g. tubes, pressurizers, accumulators, surge tanks), as well as structural parts (e.g. supports, shields) and some kinds of instrumentation (e.g. thermocouples).

- Category 2

  This category includes mainly fluidic gates between process systems, such as "surge lines" of PWRs and, more generally, free connections between pressure boundary systems and process instruments.

- Category 3

  This category includes mechanical actuators, such as check valves and spring- loaded relief valves, as well as some trip instruments (e.g. thermostatic devices, pressure and level switches).

- Category 4

  This category includes typical components of fail-safe and self-powered trip devices performing the activation of safety functions (fail-safe electric or pneumatic valves, some control rod actuators, etc.).

It has to be pointed out that the attribution of some components to one or another of these categories may not be always an easy task. As an example of such difficulties - and a subject for desirable more in depth thinkings - the case of a rupture disk could be suggested. Is the action of such protective feature, when it is activated, more similar to the mechanical movement of a check valve, or to the movement produced by thermal expansion? Then, should a rupture disk be classified in Cat. 2 or in Cat. 3? And to what extent its assigment to a category should be conditional upon a careful set of design, installation, test, inspection and replacement conditions? This subject seems to deserve a treatment by itself, and is here mentioned for memory only.

Finally, some considerations may be useful to highlight the significance of the passive safety principle in the general context of the nuclear safety principles and requirements, also to clarify what the passivity category of a device (system or component) means for the safety evaluation of such device. As previously stated, passivity is not a synonymous of reliability or availability, even less of assured adequacy of the safety device, though several factors potentially adverse to its performance can be more easily counteracted if it is designed according to the passive safety principle. Moreover, a safety device assigned to a passivity category of high figure is not necessarily worse than a passive system of lower figure designed to perform the same function; indeed, the difference in categorization implies only a difference in the application extent of the passive safety principle. But the capability of the device to perform adequately the intended function depends also on a number of items (related to design, construction, operation, etc.) which must be anyway and carefully considered, in order to achieve an acceptable safety evaluation of the device.

SIMPLIFIED BWR PERFORMANCE AND SAFETY

A.S. RAO, C.D. SAWYER, R.L. HUANG,
F.M. PARADISO, H.E. TOWNSEND
Nuclear Energy Division,
General Electric Company,
San Jose, California,
United States of America

ABSTRACT

The design for the Simplified Boiling Water Reactor (SBWR) nuclear plant represents a complete conceptual design for a 600 MWe power plant. This paper provides a description of the SBWR including the passive safety design features and the thermal hydraulic analysis of their performance. The SBWR is a plant that is significantly simpler to build, operate and maintain compared to currently operating plants. The reason for this simplification is inherent in some of the key features -- elimination of the forced recirculation system, use of passive safety features and use of a direct cycle system. The use of passive safety systems has resulted in the elimination of all safety-grade pumps and diesel generators and has enabled significant simplification of the plant design. The major passive safety systems include a depressurization system/gravity driven cooling system to provide core cooling. An isolation condenser is used to remove decay heat for all transients and accidents.

1. INTRODUCTION

Recently there has been increasing utility interest in potential future nuclear units combining the characteristics of smaller size, greater simplicity and more passive safety features. This interest is driven by a worldwide slowdown in electrical growth rates which provides an incentive for smaller capacity additions, and by a recognition that smaller nuclear units offer potential simplifications with attendant economic benefits. In response to such interest, GE began development in 1982 of a 600 MWe reactor with simplified power generation and safety systems [Reference 1]. The following basic objectives for the new design were established:

- Power generation costs must be, superior to coal.
- Plant safety systems should be simpler than those employed in current designs.
- The design should be based on existing technology.
- The design should considerably shorten construction schedules.
- Plant should have an electrical rating in the 600 MWe range.

This paper provides a brief overview of the SBWR design. Additional details of the design and comparison to the basic objectives are given in Reference [2]. Results of analyses demonstrating the performance of the SBWR are also presented. The analyses cover normal operation and transient and accident responses. These analyses are based on extensive analytical and experimental development.

2. DESCRIPTION OF THE SBWR

The SBWR power production systems utilize the simplicity inherent in a direct cycle nuclear plant. The nuclear fuel directly heats the water that is converted to steam in a single pressure vessel. This direct cycle has the inherent advantage of being easy to startup, operate and shutdown during power production and following transients and accidents. The SBWR incorporates an additional major simplification -- elimination of any pumping to recirculate the water through the core by using natural circulation. The use of natural circulation results in an extremely reliable and simple system to produce the steam needed to drive the turbine and generator. The turbine island includes several simplifications. This simplification is achieved by the use of advanced GE turbine technology and the use of a turbine design with tandem compound two flow (TC2F) 52" last stage buckets. Table I summarizes the key technical parameters of the plant. Figure 1 shows the SBWR reactor vessel and shows a schematic of the SBWR plant.

The power cycle is dependent on auxiliary systems during normal operation and startup and shutdown. The SBWR has a design that has improved the reliability of these systems by the appropriate use of margin, redundancy and diversity in these auxiliary systems. For example, shutdown cooling has been considerably simplified by incorporating the ability to remove decay heat over the full reactor pressure range by modifying the reactor water cleanup system and eliminating a separate shutdown cooling system. The entire man-machine interface aspects of the design have been substantially improved using state-of-the-art technology, including use of digital controls, fiber optics and multiplexing.

Major strides have been made in the SBWR for the handling of operational transients and accidents. The basic philosophy has been to first build in inherent margin into the design to eliminate system challenges. The second line of defense is to enhance the normally operating systems to handle transients and accidents. And as a final line of defense, passive safety-grade systems (see Figure 1) have been included in the design to provide confidence in the plant's ability to handle transients and accidents.

The system simplifications discussed in the above paragraphs has resulted in a building design (Figure 2) that is easy to construct and has also permitted a significant reduction in safety-grade equipment and structures. The use of passive safety systems requires only a relatively small containment and a small area around it to house this equipment, resulting in a major plant simplification by reducing the safety envelope (i.e., building volumes) and thus simplifying construction.

3. SBWR PERFORMANCE AND SAFETY ANALYSES

The SBWR is a natural circulation reactor requiring no pumps to circulate the water through the core. The natural circulation flow is dependent upon the difference of water density between the downcomer leg and the core region. To facilitate the establishment of natural circulation during a cold startup, a proper water level must be maintained to allow the communication of water between the downcomer and the reactor core. After the reactor core starts to generate steam voids, the natural circulation flow starts to increase. The flow rate continues to increase until the core power reaches about 60% of rated condition. After that, the core flow stays at a constant level with minor fluctuations.

Table I - SBWR Technical Data Summary

<u>Plant output</u>	
Net electrical output	600 MWe
Gross thermal power	1800 MWt
Plant cycle	Direct
Vessel dome pressure	71.1 kg/cm^2
Main steam flow	3490 tons/hour
Turbine	TC2F-52 inches
Reheat stages	One
<u>Nuclear boiler</u>	
Reactor vessel	
Inner diameter	6.0/7.0 m
Height	23.6 m
Primary coolant recirculation system	Natural circulation
Recirculation flow	23,700 tons/hour
<u>Core and fuel</u>	
Active fuel length	2.44 m
Equivalent core diameter	4.73 m
Power density	42.0 kw/l
Number of assemblies	732
Fuel material	UO_2
Cladding material	Zircaloy 2
Fuel lattice type	8x8 barrier
<u>Reactivity control</u>	
Number of control rods	177
Neutron absorber	B_4C
Control rod form	Cruciform
Control rod drive	Electro-hydraulic, fine-motion
Other control	Burnable poison (Gd_2O_3)
<u>Containment</u>	
Type	Pressure suppression
Configuration	Cylindrical reinforced concrete
<u>Construction Schedule</u>	
First concrete to fuel load	30 months

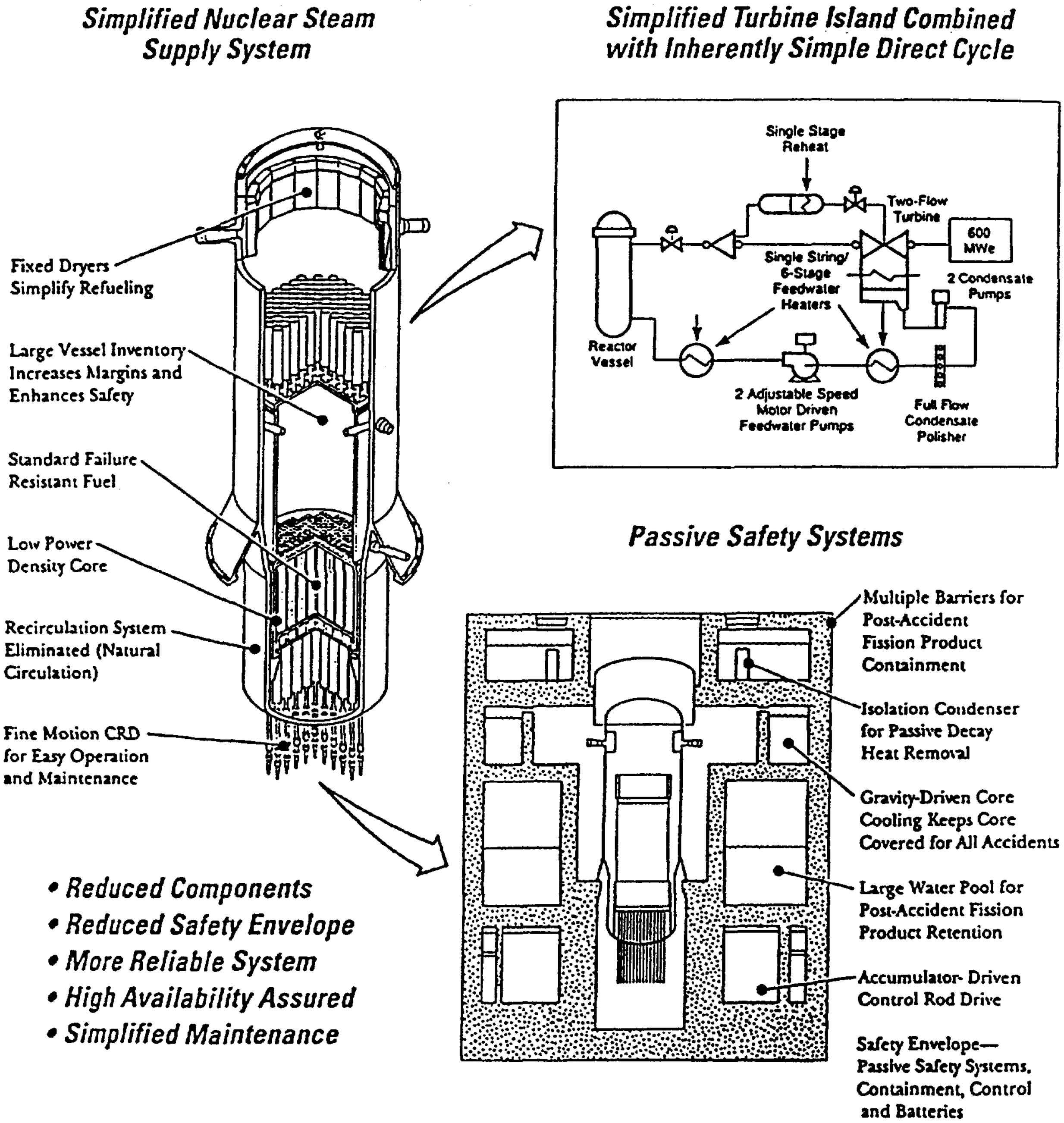
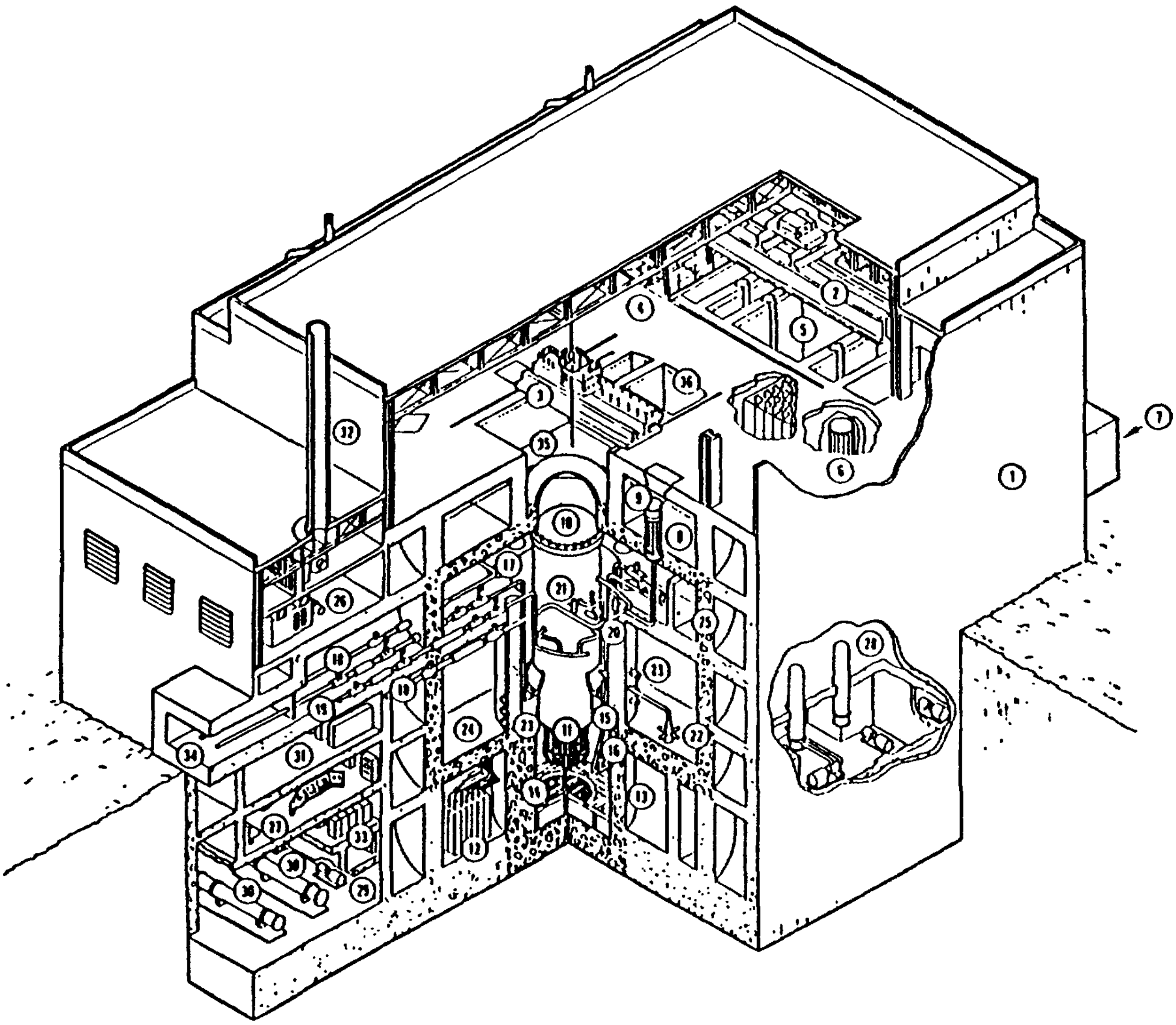


FIG. 1. The SBWR conceptual design — a 600 MWe total plant design.

The SBWR design philosophy is based on the premise that the plant would have large margins with reduced demand on equipment and operators. With the incorporation of natural circulation and passive gravity-driven core cooling in the SBWR design, a large amount of water inventory is available in the reactor vessel. This results in a very low pressure rate (about 50 psi/sec vs. 150 psi/sec for operating BWRs). Taking advantage of this design characteristic, the SBWR eliminates the need for relief valves. After a reactor isolation, the energy will be initially stored in the reactor vessel and then removed by the isolation condensers. In this way, there is no energy discharged to the suppression pool.



1 Reactor Building
2 Reactor Building Crane
3 Refueling Machine
4 Fuel Handling Machine
5 Spent Fuel Storage Pool
6 Spent Fuel Shipping Cask & Pool
7 Equipment Main Entry Hatch
8 Isolation Condenser Pool
9 Isolation Condenser
10 Reactor
11 Fine Motion Control Rod Drives
12 FMCRD Hydraulic Units
13 Reactor Pedestal
14 Under-Vessel Servicing Platform
15 Lower Drywell
16 Shutdown Cooling Line
17 Upper Drywell
18 Main Steam Lines
19 Feedwater Lines
20 Depressurization Valves
21 Safety Relief Valves
22 SRV Quenchers
23 Horizontal Vents
24 Suppression Pool
25 Gravity Driven Cooling Pool
26 Building HVAC
27 Control Room
28 Residual Heat Removal System Heat Exchangers
29 Reactor Component Cooling Water System Pump
30 Reactor Service Water System Heat Exchangers
31 DC Batteries
32 Plant Stack
33 FMCRD Electric Panel
34 Steam Tunnel
35 Drywell Head
36 Steam Separator Storage Pool

FIG. 2. SBWR reactor building.

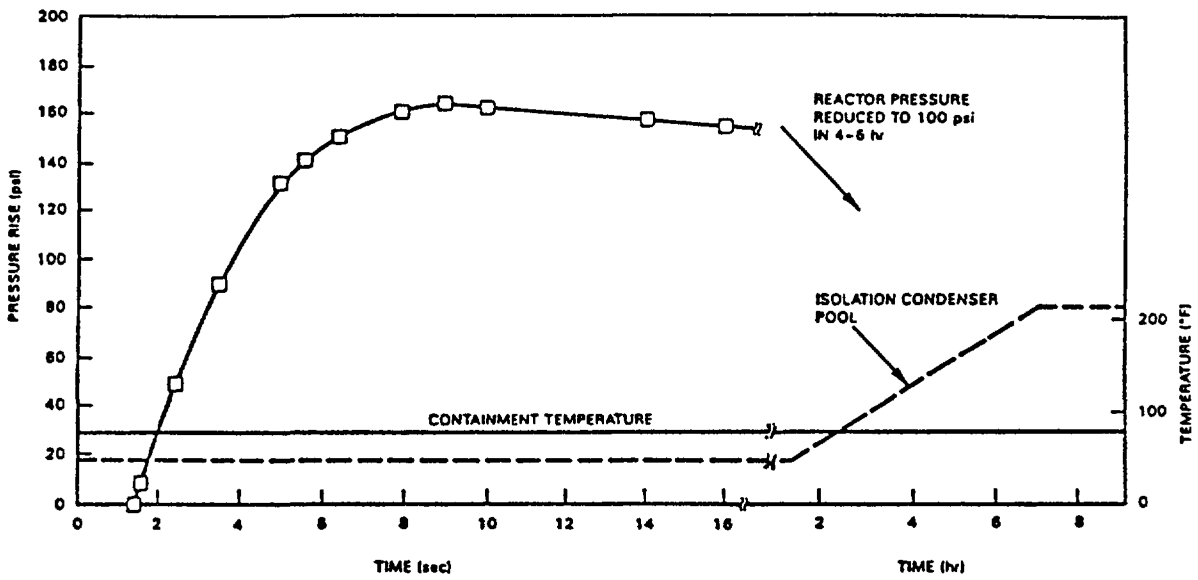


FIG. 3. Vessel pressure, containment and isolation condenser pool temperature for an isolation transient.

Also, there is no loss of reactor inventory. Consequently, no high pressure makeup system is required. Figure 3 shows the reactor pressure and containment response for a reactor isolation, using analyses methods described in Reference [3].

Major simplifications have been made in the handling of accidents -- reduced operator demands, simple operations, reduced number of components, ease of maintenance and ease of construction. The use of passive safety systems was a major contributor to several simplifications to the plant, in addition to providing enhanced confidence in the plant's ability to meet safety goals. The appropriate combination of normally operating, nonsafety and safety systems that are either motor-driven or passive, has resulted in a plant design that will build confidence in the plant's safety. The plant design has relied on utilizing concepts that in all cases have been utilized in nuclear power plants. The major innovation has been in combining the systems in a fashion that maintains the SBWR application in the parameter ranges of proven experience and technology. The systems used to handle these safety functions are summarized in Table II.

Analyses have been performed to determine the response of the SBWR following accidents. Some of these analyses have been performed using licensing basis assumptions with single failures and taking credit for safety-grade passive systems only. The calculations using models described in References [4] and [5], show that the plant design results in no uncovery of the core following any pipe break. Figure 4 shows the peak cladding temperature, vessel water level and containment response following a main steam line break--the largest pipe break. The containment pressure response shows that it does not rise for a long time (several hours) and stays well below the design pressure.

Table II - SBWR Transient/Accident Performance

Function/System	Performance/Comments
1. Reactivity Control	
- Hydraulic Accumulator	- Passive primary scram mechanism
- Electric Rod Motion	- Used for normal power variation - Backup to scram for rod insertion
- Accumulator Driven Boron Injection	- Passive and diverse shutdown system
2. Inventory Control	
- Motor Driven Feedwater	- Available for most transients/ accidents
- Control Rod Drive Pumps	- Normally operating system with increased capacity to handle all transients/accidents
- High Pressure Shutdown Cooling	- Full pressure range normally operating system to handle all transients/ accidents
- Safety-Grade Isolation Condenser	- Passive and redundant system for handling isolations
- Depressurization Plus Gravity Driven Cooling	- Passive and reliable means to handle all transients/accidents
3. Decay Heat Removal	
- Main Condenser	- Available for some situations
- High Pressure Shutdown Cooling	- Normally operating and can handle all transients/accidents
- Safety-Grade Isolation Condenser	- Passive system that handles all accidents without significant containment heatup
- Pool Cooling Combined with Vessel Blowdown	- Backup and redundant system provides diverse system
4. Fission Product Control	
- Suppression Pool	- Passive fission product retention assured
- Multiple Structural Barriers	- Passive fission product retention assured inside plant, assuring low offsite dose.

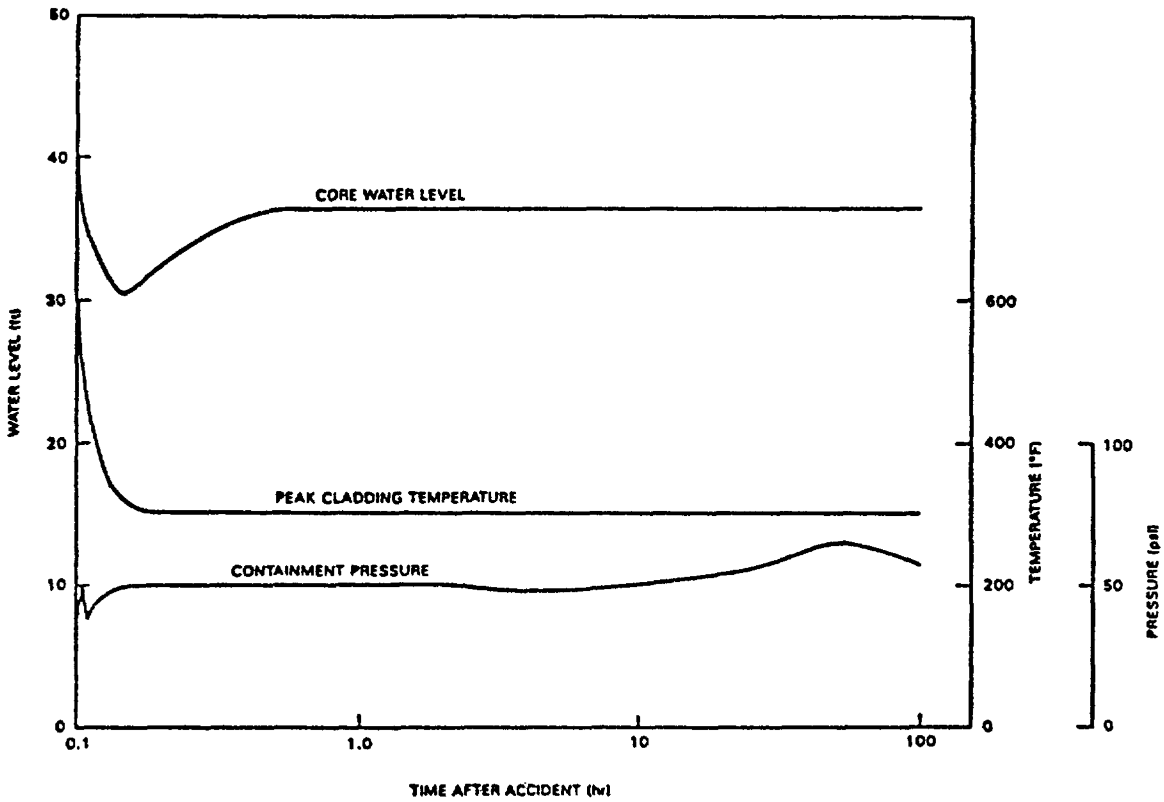


FIG. 4. Reactor and containment response to a loss of coolant accident.

4. SUMMARY AND CONCLUSIONS

GE has completed the conceptual design of the SBWR. The design shows the results of aggressive simplification in the entire plant. The conceptual design is also expected to be easy to construct, operate and maintain. Significant simplification has also resulted from the use of passive safety systems. The result of this effort is an economically competitive plant that can be constructed in a short time. The plant has several features that enhance its appeal to the public and the utilities -- primarily its resistance to accidents and reduced potential for a loss of the utilities' investment.

REFERENCES

[1.] Duncan, J. D. and McCandless, R. J., "An Advanced Simplified Boiling Water Reactor," ANS Topical Meeting, Seattle, WA, May 1-5, 1988

[2.] Wilkins, D. R. and Lowton, R. B., "World Class BWR's for the 1990s," Nuclear Plant Availability Improvement Conference, Madrid, Spain, April 10-14, 1989

[3.] Linford, R. B., Analytical Methods of Plant Transient Evaluations for the General Electric Boiling Water Reactor, February 1973, NEDO-10802

[4.] Andersen, J. G. M., Chu, K. H. and Shaug, J. C., BWR Refill-Reflood Program Task 4.7 - Model Development: Basic Models for the BWR Version of TRAC, August 1983, GEAP-22051

[5.] Cheung, Y. K., Parameswaran, V. and Shaug, J. C. , BWR Refill-Reflood Program Task 4.7 - Model Development: TRAC-BWR Component Models, April 1983, GEAP-22052

PASSIVE SAFETY FEATURES FOR NEXT GENERATION CANDU POWER PLANTS

A. NATALIZIO*, R.S. HART*, J.J. LIPSETT**,
F. SOEDIJONO*, J.E. DICK*

*CANDU Operations,
Atomic Energy of Canada Limited,
Mississauga, Ontario

**Chalk River Nuclear Laboratories,
Atomic Energy of Canada Limited,
Chalk River, Ontario

Canada

Abstract

CANDU offers an evolutionary approach to simpler and safer reactors. The CANDU 3, an advanced CANDU, currently in the detailed design stage, offers significant improvements in the areas of safety, design simplicity, constructibility, operability, maintainability, schedule and cost. These are being accomplished by retaining all of the well known CANDU benefits, and by relying on the use of proven components and technologies. A major safety benefit of CANDU is the moderator system which is separate from the coolant. The presence of a cold moderator reduces the consequences arising from a LOCA or loss of heat sink event. In existing CANDU plants even the severe accident - LOCA with failure of the emergency core cooling system - is a design basis event. Further advances toward a simpler and more passively safe reactor will be made using the same evolutionary approach. Building on the strength of the moderator system to mitigate against severe accidents, a passive moderator cooling system, depending only on the law of gravity to perform its function, will be the next step of development. AECL is currently investigating a number of other features that could be incorporated in future evolutionary CANDU designs to enhance protection against accidents, and to limit off-site consequences to an acceptable level, for even the worst event. The additional features being investigated include passive decay heat removal from the heat transport system. A simpler emergency core cooling system and a containment pressure suppression/venting capability for beyond design basis events. Central to these passive decay heat removal schemes is the availability of a short-term heat sink to provide a decay heat removal capability of at least three days, without any station services. Preliminary results from these investigations confirm the feasibility of these schemes.

1. INTRODUCTION

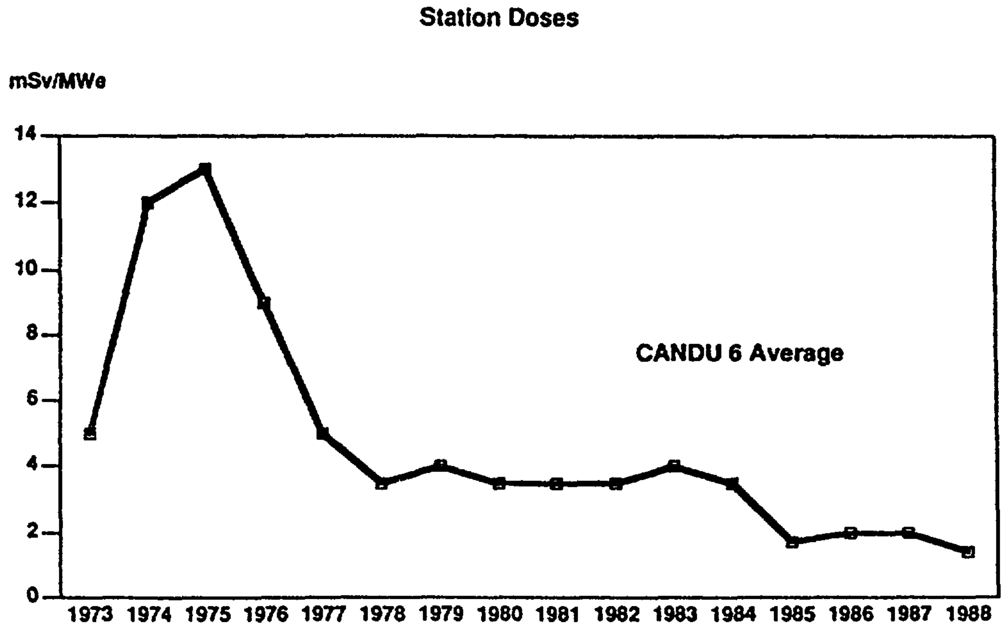
The trend for the next generation of nuclear power plants is clearly towards installations that are safer, more reliable, simpler to construct and operate and less costly. The rationale for these objectives are elaborated in a companion paper presented at this meeting[1].

Given the need for change, how do reactor designers respond to that need? The response to date has been mixed and generally falls in one of two camps: the camp that promotes an evolutionary approach, and the camp that promotes a revolutionary approach by the introduction of radical, new designs. Atomic Energy of Canada Limited (AECL) has been following the evolutionary approach.

This paper outlines the evolutionary approach to safer and better reactors that is being pursued by AECL and also discusses some of the passive design features currently under investigation that would be implemented in future CANDU designs.

2. CANDU EVOLUTION

The CANDU design has evolved continuously and consistently since its inception in the mid 1950s. A constant theme of this evolution has been simplification, with resulting improvements in station performance and safety. Figure 1 illustrates the steady reduction obtained in station doses while maintaining a steady growth in the current high levels of performance.



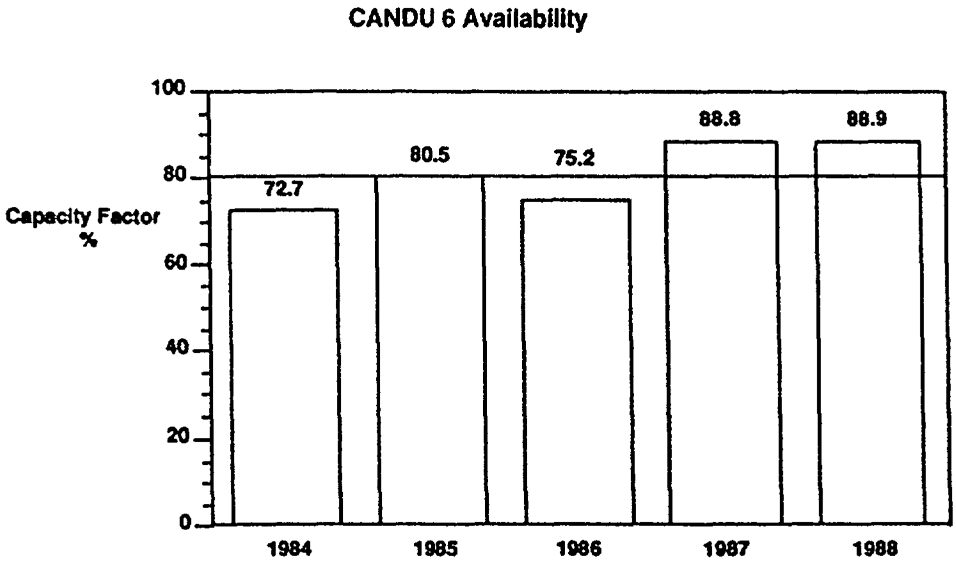


Figure 1 CANDU Performance

2.1 Simplification

CANDU reactors feature a number of fundamental simplifications relative to other types of pressurized water reactors[2]. These include:

- Carbon steel heat transport system piping instead of stainless steel. It is more easily fabricated and inspected; it is ductile and immune to stress corrosion cracking.
- Pressure tubes instead of a massive pressure vessel.
- Easily replaceable pressure tubes, the only CANDU component subjected to a combination of high stress and high radiation.
- Short, simple fuel bundle design that is easily fabricated. The same bundle design is used for the entire core.
- Natural uranium, requiring no enrichment or burnable poison.
- No control devices in the high pressure reactor coolant circuit for reactivity control. They are located in the low temperature, low pressure moderator.
- Flexible irradiated and new fuel storage (no concerns over criticality regardless of storage configuration due to low reactivity of CANDU fuel).

Reduction in the number of components used has been a focus of CANDU evolution over the past 25 years. Tables 1, 2 and 3 illustrate the number of key components. The reduction in the number of these components is, of course, accompanied by a reduction in auxiliary components, including piping, cabling, instrumentation and support structures. These are not accounted for in the tables.

Table 1: Steam Generator Evolution

Station	Net Reactor Output (MWe)	MW(th) per SG	Area (m^2) per SG	No. of SG
Pickering	515	138	1850	12
Bruce	825	265	2415	8
CANDU 6	640	500	3200	4
Darlington	885	665	4760	4
CANDU 3	450	690	4200	2

Table 2: Reactor Coolant Pump Evolution

Station	Net Reactor Output (MWe)	Total No. of Pumps	No. of Pumps Operating	Motor Rating (kW)
Pickering	515	16	12	1420
Bruce	825	4	4	8200
CANDU 6	640	4	4	6700
Darlington	885	4	4	9400
CANDU 3	450	2	2	9400

Table 3: Valve Evolution

Station	Net Reactor Output (MWe)	No. of Valves Packed	No. of Valves Bellows Sealed
NPD	22	1500	0
Douglas Point	220	2000	0
Pickering	515	175	570
Bruce	825	75	500
CANDU 6	640	90	300
Darlington	885	90	300
CANDU 3	450	50	200

Further simplifications and reductions in the number of components can only be achieved by changes in approach, as with the introduction of passive cooling methods.

2.2 Safety

The CANDU reactor uses natural uranium fuel and heavy water moderator and coolant. The fuel is contained in individual fuel channels that separate the coolant from the moderator. This reactor configuration, therefore, provides fundamental and inherent features that have a direct contribution to plant safety.

The combination of D_2O moderation and natural (or slightly enriched uranium fuel) gives:

- A CANDU fuel channel lattice that is optimized for maximum reactivity. Hence, any event that relocates the fuel reduces reactivity and shuts down the reactor. Criticality is impossible with light water or dilute heavy water in the channels, e.g., after emergency coolant injection.

- Power transients due to reactivity excursions are slow due to long neutron lifetime (about a millisecond).

- Ease of handling of new and irradiated fuel. No possibility for criticality regardless of storage configuration.

On-power refuelling results in:

- Very small and constant excess reactivity in the reactor at all times during station life.

- Low total worth of all reactivity regulation devices.

- Constant worth of reactor regulating system over the life of the plant.

- Short fuel bundles limit the fission product source term per fuel element.

- Low radiation fields in the reactor coolant, due partly to on-line failed fuel detection and removal of fission products, and the absence of chemicals for reactivity control.

The cool low-pressure moderator, separate from the high pressure heat transport systems provides:

- a heat sink that can remove decay heat under severe conditions such as a loss of coolant coincident with a loss of emergency core cooling,

- a cool low pressure environment for all reactivity control devices, and

- a means to obtain comprehensive neutronic data for reactor control, facilitated by simple low cost detectors.

In building upon these fundamental and inherent safety features, CANDU also incorporated engineered safety and safety support systems to provide a high standard of safety for both plant personnel and the general public.

These engineered features include:

- two independent, fully capable, actively triggered, passively driven, shutdown systems that are diverse and functionally independent of the reactor regulating system,

- a shutdown cooling system that can be brought into service at full heat transport system temperature and pressure for decay heat removal, and

- discharge of coolant from valves connected to the heat transport system, such as pressure relief valves, is routed to a high pressure tank, which has relief devices set above the heat transport system operating pressure; hence the valve activation or failure of such valves to reclose after activation will not lead to a large inventory loss from the heat transport system.

Licensing requirements in Canada have also encompassed a relatively wide range of design basis events; these include the failure of any special safety system (including containment or emergency core cooling) coincident with major process failures (including a loss-of-coolant accident), and the failure of the reactor pressure vessel (the fuel channel).

It should be noted that fuel channel failure is not accompanied by disastrous consequences. In fact, the two fuel channel ruptures experienced in CANDU plants were catered to by normal process systems, without the initiation of any of the safety systems.

3. ADVANCED CANDU

The focus of the advanced CANDU design has also been on plant simplification and safety. This is evident from the design objectives established for the CANDU 3.

3.1 Design Objectives

Development of the CANDU 3 started in 1982 by identifying key design objectives[3,4]. These design objectives are listed below:

a. To improve traditional CANDU advantages, including safety, low radiation exposure, high capacity factor, ease of maintenance and low operating cost.

b. To reduce specific capital cost, construction schedule and unit energy cost.

c. To standardize the plant design such that it is suitable for any reasonable site, worldwide, without significant changes to the design.

d. To accommodate division among the plant structures and systems to facilitate a variety of shared financing, contractual arrangements, or partners with one or more organizations, without significant design or documentation changes.

e. To employ state-of-the-art technologies, including design, construction, operation and project management technologies, consistent with construction in the 1990s.

f. From a component design viewpoint, to:

(1) maximize component life,
(2) provide easy replacement at end of component life ("easy" replacement means quick and simple - without complex tooling or an extended outage, thereby minimizing radiation exposure),
(3) minimize component cost, and
(4) minimize component installation time and cost.

g. From a maintenance/in-service inspection viewpoint, to:

(1) achieve a minimum of two years of station operation between scheduled maintenance/in-service inspection outages, which will not exceed 21 days, and
(2) accommodate major equipment replacement (fuel channels, steam generators, etc.), major systems modification or modernization (control, computers, etc.), or major equipment refurbishing (reblading turbine, etc.) in a major maintenance outage not exceeding 90 days. Such a major main-tenance outage is expected to be required no more frequently than every 15 years.

h. From an operations performance viewpoint, to

(1) achieve a lifetime capacity factor of 94% with less than one unplanned shutdown per year, and
(2) provide the operator with modern information processing tools and methods to enhance human performance and to minimize the potential for plant upset due to error.

With the engineering of the CANDU 3 standard plant over 30% complete, we are confident that all of the above objectives will be achieved.

3.2 Safety

After reactor shutdown, decay heat removal from the fuel is the key to reactor safety. As with previous CANDU plants, the CANDU 3 follows an in-depth approach to heat removal.

Normal heat removal paths include the steam generators, which are supplied by two independent feedwater trains, and the fully capable shutdown cooling system, which is supplied with station services from two separate sources.

Should all normal heat removal paths be lost, the residual heat is rejected to the moderator system. Unlike other pressurized water reactor types, CANDU operates with the pressure vessel (fuel channels) surrounded by the cool low pressure moderator. Moderator volume is about 15 times the in-core coolant volume.

These multiple lines of defense result in a very low frequency of severe core damage for the CANDU 3.

In current CANDU designs, these heat removal systems are powered by pumps and controlled using valves. However, as discussed below, all of the decay heat removal systems can be made passive with built-in heat removal capability of at least three days.

4. NEXT GENERATION CANDU

Even as the engineering for the CANDU 3 is being completed, AECL is looking towards further improvements and evolution of this product. Some very challenging objectives and targets are being established for the next generation CANDU design. These include an expansion of the design basis set and stringent limits for off-site radiation doses and land contamination.

These, of course, are in addition to the objectives for further design simplification, improved constructibility, operability and maintainability, and lower plant cost.

To meet the above challenges, three principal design goals have been established:

a. to improve the overall capability of the plant so that it will have a higher level of resiliency to accident initiators.

b. to improve the capability of containment in coping with large releases of energy resulting from severe accidents, and

c. to improve the reactor design so that large reactivity transients can be eliminated,

A number of design studies have been identified and initiated to address the above goals.

The passive safety features currently under investigation, to address the above, are discussed below.

5. PASSIVE SAFETY FEATURES

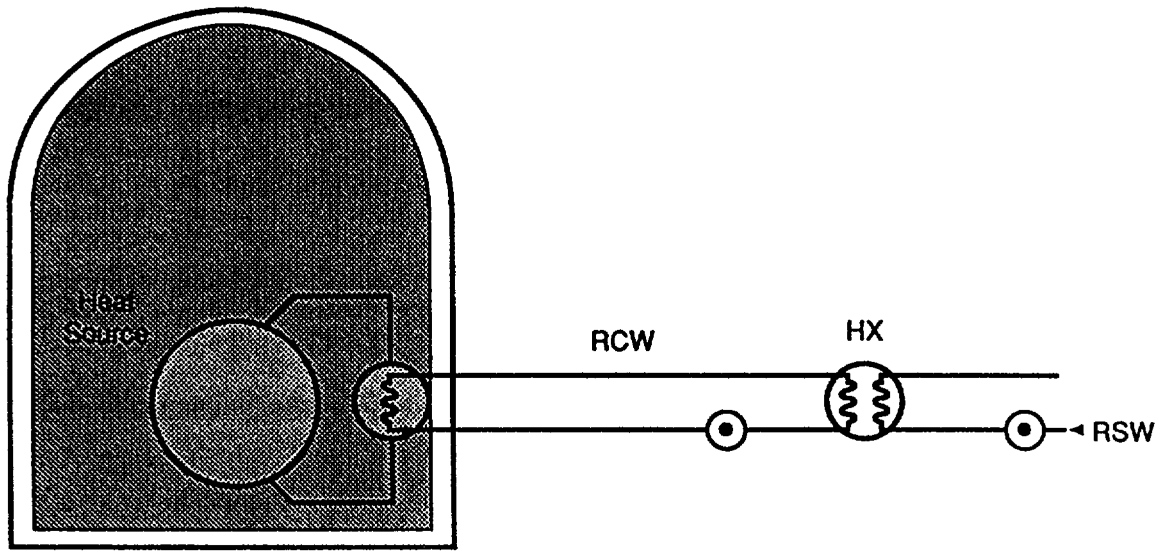
The key feature of the passive cooling systems described below is the presence of a water source, close to the heat source, with sufficient capability to provide decay heat removal for at least three days, following a plant transient or accident. As shown in Figure 2, this concept effectively decouples the heat source from the normal heat sink by the introduction of a large thermal inertia between the two. This thermal inertia makes the plant more resilient and tolerant to disruptions or failures in the cooling water supply circuit.

5.1 Passive Safeguards for LOCA Events

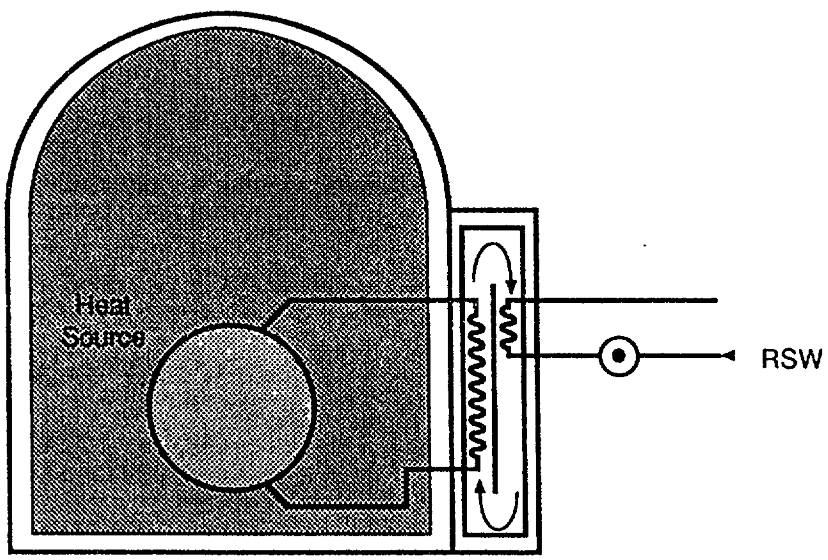
The first line of defense against LOCA is the emergency core cooling system. The second line of defense is the moderator system. Design studies have been undertaken to simplify and improve the reliability of both systems.

Emergency Core Cooling System - This system is being considerably simplified so that the number of active components and automatic actions that have to take place after a LOCA are the absolute minimum. Core refill is achieved with two high pressure water tanks injecting into the reactor headers. Once the core is flooded, it is kept filled by recirculating water from the reactor building sump. The passive core refill system and the recirculating system are shown in Figure 3.

Moderator System - The moderator system is in operation during normal plant operation; therefore, its availability during a LOCA is assured. When the emergency core cooling system is available, the moderator provides cooling of the calandria tubes for those high power channels whose pressure tubes may expand into contact with the calandria tube. In that instance the moderator does not have a long-term function. However, in the case where the emergency core cooling system is unavailable, the function of the



Conventional Approach



Passive Approach

FIGURE 2 Conventional and Passive Cooling Water Approaches

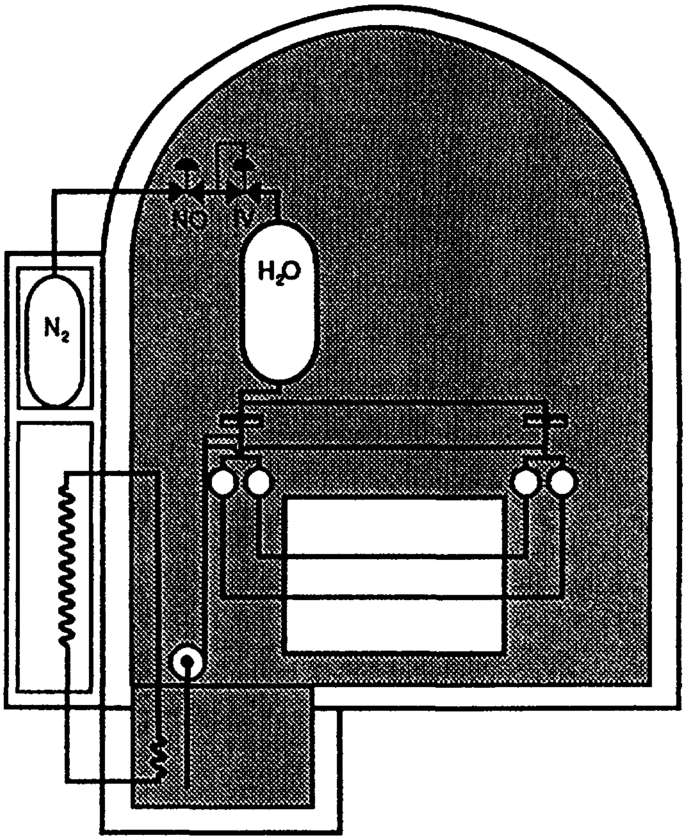


FIGURE 3 Simplified ECC System with Passive Refill Capability

moderator is to remove decay heat for an indefinite period. In this instance it is desirable to rely on passive means for decay heat removal to ensure its long-term function.

Figure 4 illustrates one of several schemes being investigated for removing decay heat from the moderator using natural circulation. The operation of the system and the sequence of events is described with reference to Figure 5.

a) LOCA occurs at time zero. (AC power and the emergency core cooling system are assumed unavailable).

b) In ten seconds the power to the moderator is reduced to 10% of its nominal value.

c) At one minute, pressure tubes start to balloon or sag and contact the calandria tubes and at ten minutes all pressure tubes have contacted.

d) After contact is complete, the power transferred to the moderator rises to 65% of its nominal value and then follows the decay power curve.

e) Initially the moderator cooling system does not have adequate cooling capability and the moderator temperature rises until the heat transfer rate increases (due to boiling heat transfer in the heat exchanger) at about half-hour, as shown in Figures 5 and 6.

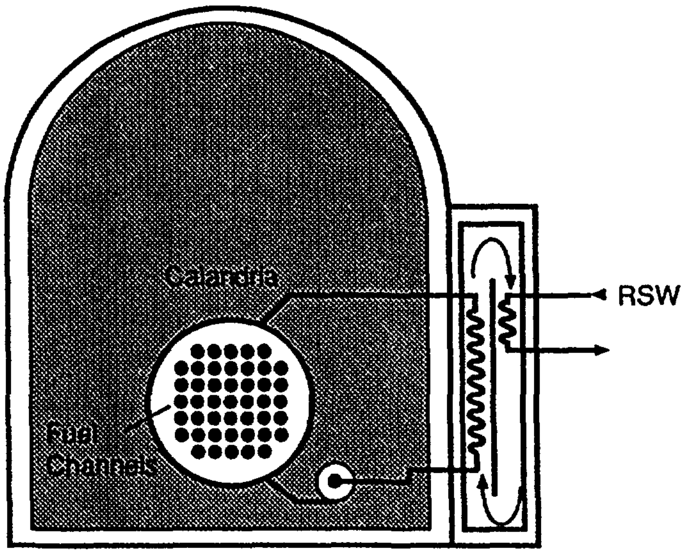


FIGURE 4 Passive Moderator Cooling System

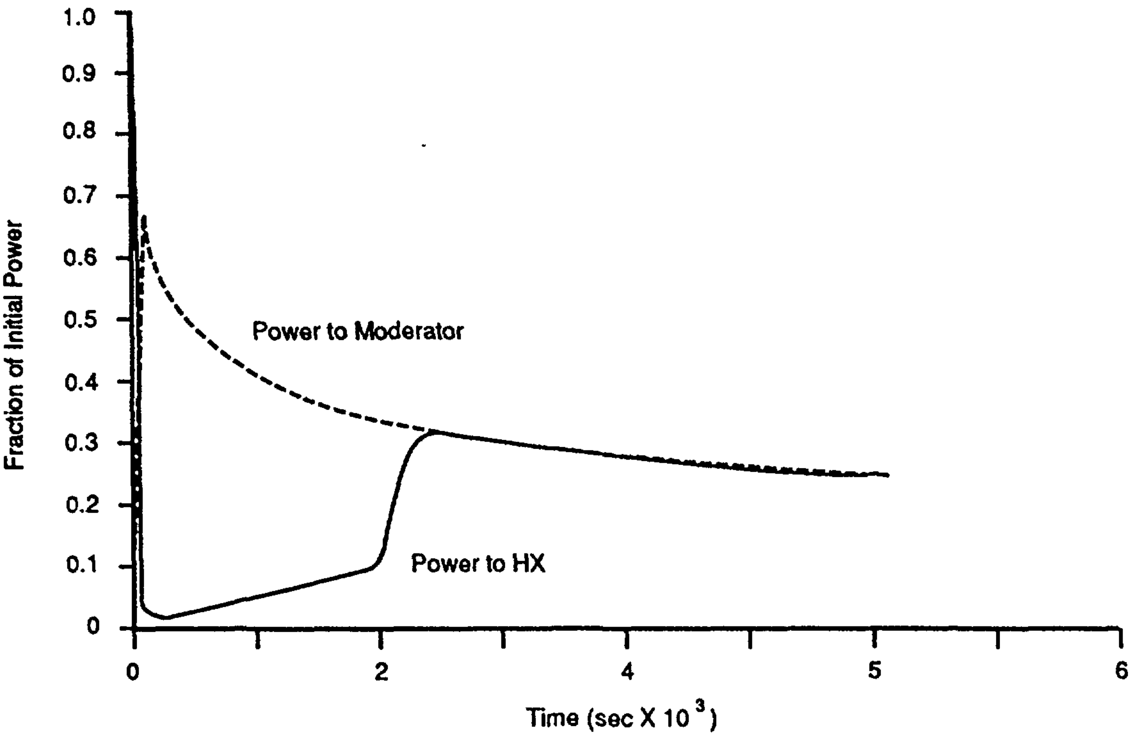


Figure 5 LOCA/LOECC Transient

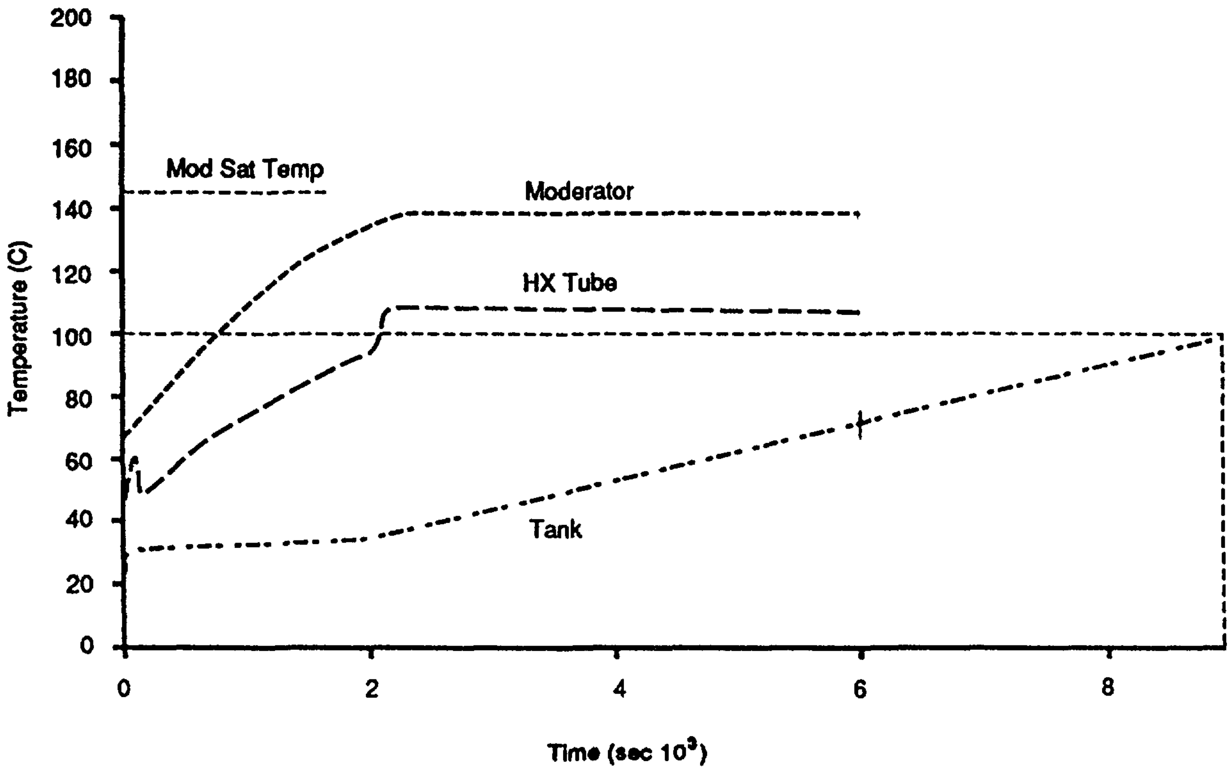


Figure 6 Moderator Cooling System Temperatures for LOCA/LOECC

f) From then on, the moderator temperature increases slowly as the water in the tank heats up. The tank will be sized to provide adequate cooling, without operator intervention, for at least three days.

The studies performed to date have confirmed concept feasibility. The ongoing work is aimed at system optimization with respect to a number of design parameters, for example, inventory of heavy water in the moderator system, calandria design pressure and heat exchanger design.

5.2 Passive Safeguards for Non-LOCA Events

The first line of defense for non-LOCA events is the auxiliary feedwater system, which is automatically initiated. The second line of defense is the shutdown cooling system, and the third is the moderator.

Auxiliary Feedwater System - Further improvements to this system will not be required due to its short mission time and as a result of the enhancements to the shutdown cooling system described below.

Shutdown Cooling System - One of the options being considered for this system is shown in Figure 7. This scheme utilizes the same cooling water tank concept developed for the moderator system (Figure 4).

The shutdown cooling circuit has a check valve to prevent flow circulation as long as the heat transport pumps are running; hence no reactor power is lost to the water tank during normal operation. If electrical power is lost to the pumps then flow will be established in the circuit by natural circulation.

For the loss of AC power event the heat transport pumps will trip

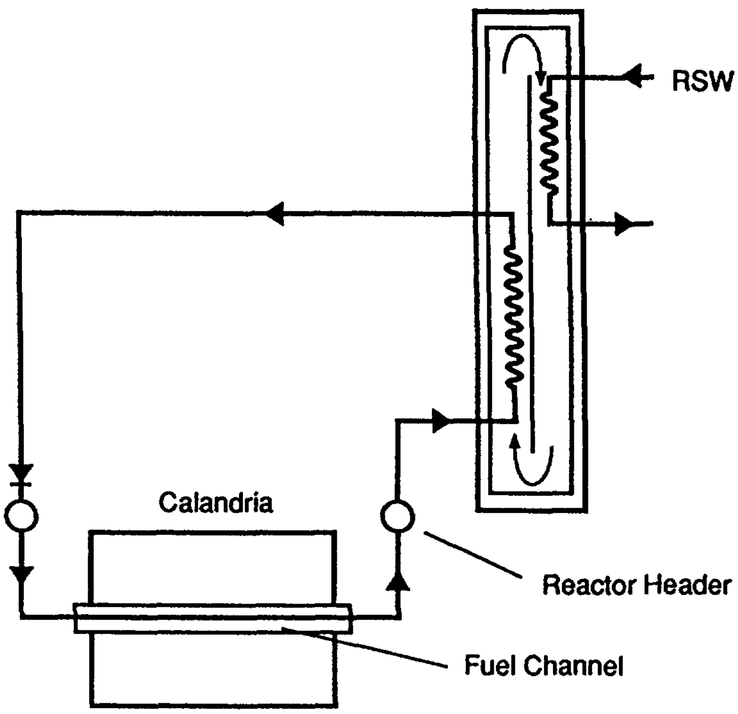


FIGURE 7 Passive Shutdown Cooling Loop

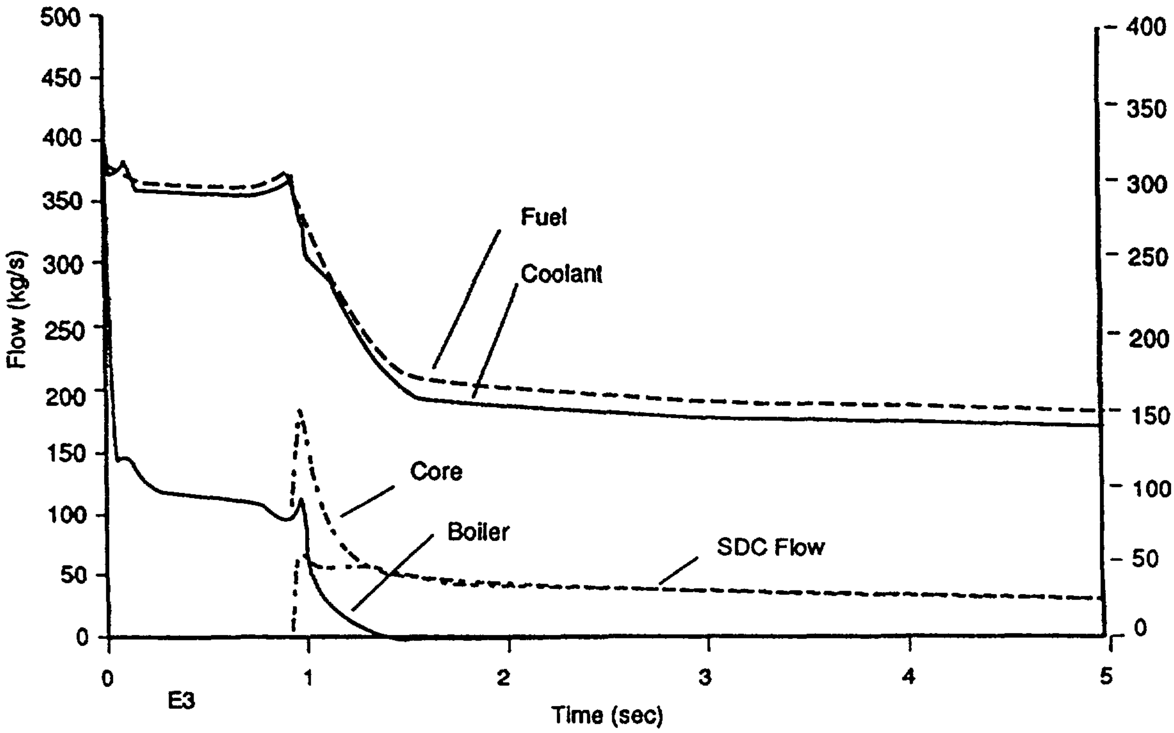


FIGURE 8 Results for Loss of AC Power

automatically. For other events, such as loss of feedwater or loss of service water, the heat transport pumps will be tripped on a steam generator "crash-cooldown" signal. As the pumps run down and the pump head decreases, the thermosyphoning head starts to build up and eventually natural circulation is established in the shutdown cooling circuit. Figure 8 illustrates the heat removal capability of this passive cooling circuit.

Moderator System - With a passive shutdown cooling system, a third line of defense is not really needed. Nevertheless, the moderator cooling circuit (discussed above) is available and is capable of removing decay heat for non-LOCA events as well.

5.3 Passive Safeguards for Containment

Although the other passive features discussed in this section reduce both the frequency and consequences of a severe accident, containment plays a special role in the safety of nuclear power plants. Because of this, it is important to ensure that containment integrity is maintained, regardless of the condition of the reactor core. This means that the isolation function must be performed with a high degree of reliability, and that the strength of the building must not be exceeded by internally generated pressure resulting from core damage.

Passive Isolation Devices - Figure 9 shows one of the passive isolation devices being evaluated for the reactor building ventilation system. The device is passively actuated by the internally generated pressure. As the cap is closed, a mechanical jaw (Not shown in Figure 9) is actuated to hold the cap closed even after the internal pressure is removed.

Pressure Suppression/Venting - The pressure suppression scheme shown in Figure 10 is being evaluated as a means for protecting containment integrity for events with severe core damage. The principle is simple. For events not leading to severe core damage, the pressure generated inside containment will be lower than the column of water in the standpipes. These events establish the design pressure of containment and do not require a relief capability. If, however, the design pressure is exceeded, the air/steam mixture inside containment is relieved through the standpipes. The steam in the mixture is condensed in the water pool, and the air is compressed in the air space above the water pool. Besides condensing steam, the water pool also cools the air escaping from containment, which also reduces the back pressure on the water pool and washes out fission products, which makes venting of the air space above the pool a possibility.

The event used to evaluate the feasibility of this concept is the early core disassembly scenario. In CANDU, this event has a very low frequency of occurrence ($<10^{-8}$ events/year). Nevertheless, it is selected because it is the absolute worst event and, if the concept works for this event, it will cover off all other severe accidents.

Early results from a preliminary investigation look promising and are shown in Figure 11. The results indicate that for a suppression volume of 5% of the containment volume, the peak pressure can be reduced by at least 15%, relative to the same containment without the pressure suppression capability.

This result is encouraging because it demonstrates that the pressure suppression scheme is at least three times more effective than increasing containment by the same volume; and, furthermore, it also

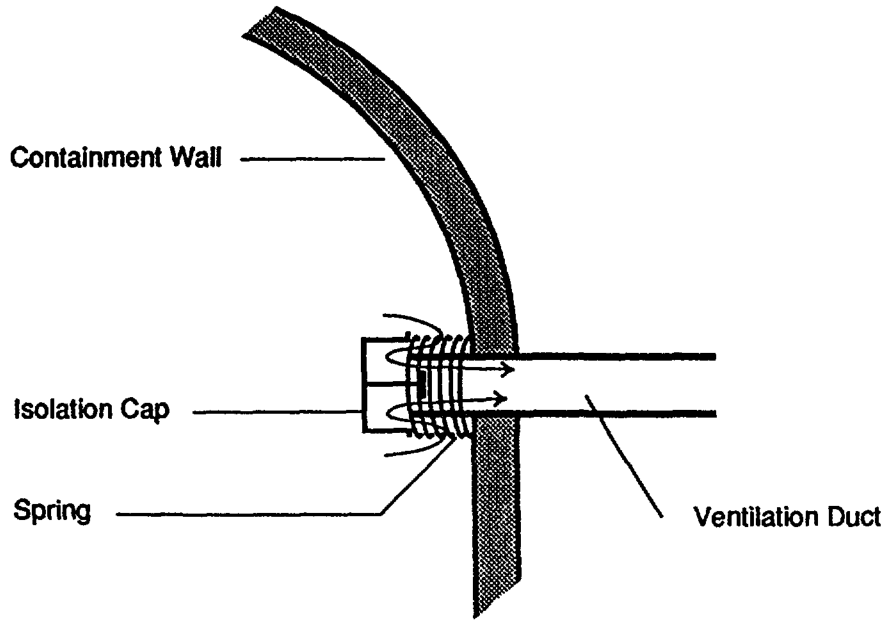


FIGURE 9 Passive Containment Isolation Device

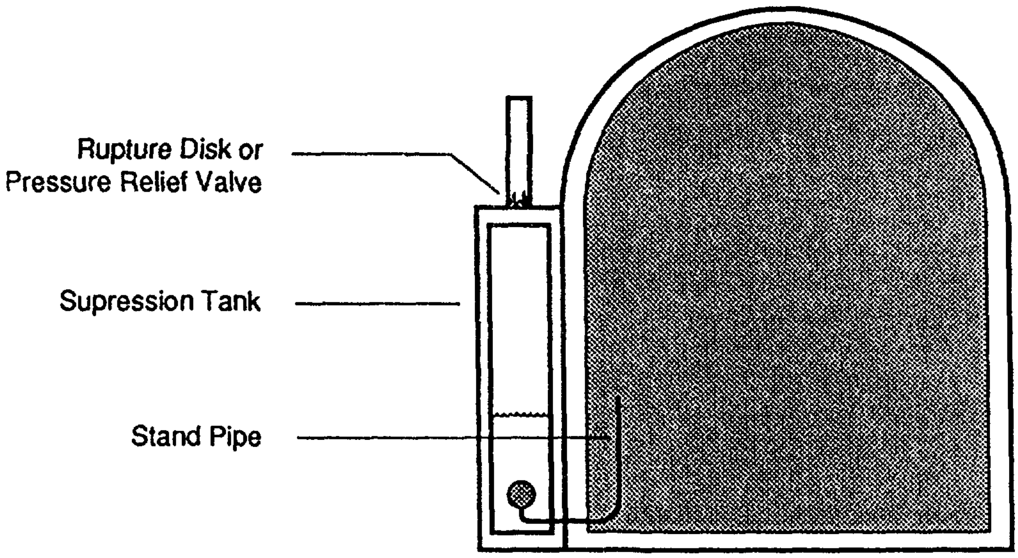


FIGURE 10 Passive Containmemt Pressure Supression/Venting Scheme

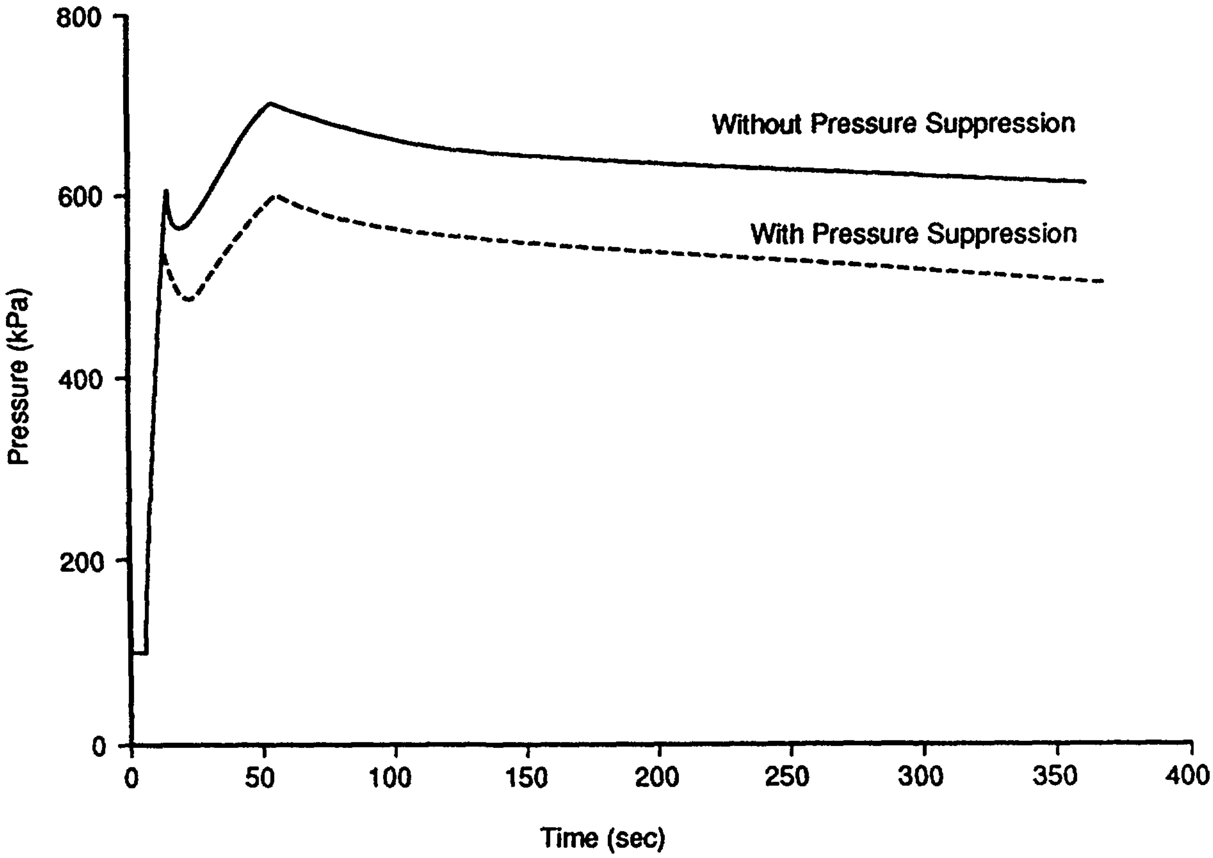


FIGURE 11 Containment Pressure Transient for a Beyond Design Basis Event

provides the possibility of venting from the air space above the suppression pool to get further reductions in containment peak pressure, with only a fractional release to the environment.

6.0 CONCLUSIONS

The CANDU 3 is the latest in the line of CANDU evolutionary nuclear power plants. Currently in the detailed engineering phase, the CANDU 3 meets the high level requirements established for the advanced LWR in all areas of design, construction and operation. For future designs, the passive cooling systems investigated to date for the moderator and shutdown cooling system are feasible and have the potential for significantly increasing safety and reliability, while reducing cost by eliminating redundant cooling water systems.

The containment studies are still in the early stages and further work is required to establish feasibility and costs. However, early results are encouraging.

References:

1. BROOKS, G.L.," Safety Aspects of Next Generation CANDU Reactors" paper presented at the IAEA Workshop on Safety of Nuclear Installations of the Next Generation and Beyond, Chicago, 1989 August.

2. HART, R.S., NATALIZIO, A. "CANDU - The Advanced PWR", Report AECL-9963, Atomic Energy of Canada Limited, CANDU Operations, Mississauga, Ont., (1989 August)

3. HART, R.S., "CANDU-3 - The Next Generation" AECL Report, Atomic Energy of Canada Limited, CANDU Operations, Mississauga, Ontario (1989 April).

4. HART, R.S., "Advances in Engineering and Construction", paper presented at the ANS/ENS International Conference, Washington, D.C., (1988, November).

CANDU COMPUTERIZED SAFETY SYSTEM

J.R. POPOVIC, G.J. HINTON
CANDU Operations,
Atomic Energy of Canada Limited,
Mississauga, Ontario,
Canada

Abstract

In CANDU 6 PHW reactors, automatic reactor trip has been carried out with digital computers since 1982. The introduction of computers in the CANDU shutdown systems was motivated by the excellent operating experience with digital systems used for direct digital control of the CANDU generating stations and by new licensing requirements for increased CANDU 6 trip coverage redundancy. This paper summarizes the evolution of digitally based design to meet these requirements, the system configuration of a fully computerized shutdown system and the associated design philosophy, software and hardware qualification process, and the operating experience of the existing installations. The fully computerized Shutdown System is described for the Darlington Nuclear Generating Station scheduled to be in-service in 1990. Future design developments are also discussed.

1. INTRODUCTION

Computerization has proven to be a significant benefit to the Safety Systems in CANDU nuclear plants. In order to ensure that these systems are developed to the appropriate level of quality, it has been necessary to address several of the issues of computerized system design. This paper outlines our operating and design experience with computerized safety systems and discusses the initiatives taken on several of the issues. Hardware qualification, the prototype program, the detailed design phase, and the testing phase of the software are addressed. The experience with these designs and the benefits of computerized systems is evaluated. Future trends in computerized safety shutdown systems and design methodology are examined.

2. EVOLUTION OF COMPUTER USE IN SHUTDOWN SYSTEMS

2.1 Traditional Design (Pickering)

A shutdown system consists of process sensors, reactivity devices (e.g. mechanical "gravity–drop" shut–off rods) and intervening instrumentation and logic. If the plant is sensed to be operating in a potentially unsafe state (e.g., power too high), sufficient reactivity is inserted to terminate the chain reaction very quickly.

Figure 1 summarizes the arrangement for one typical signal. On traditional designs, the trip setpoint is generally a constant, but may be a simple function of some other measured plant variable, such as reactor power. The trip contacts from some comparators have parallel conditioning contacts which inhibit the trip under special circumstances, (e.g. during very low power operation).

All trip signals, trip setpoints and trip status information are continuously displayed in the main control room. Manual controls allow the operators to test the shutdown system. Tests are typically conducted weekly and exercise the entire loop from sensor to reactivity device.

In the traditional design, amplifiers, comparators, etc. are solid state devices, the trip logic is done via relays, operator displays are small panel meters and lights, and the operator controls are conventional pushbuttons and handswitches.

2.2 Monitor Computers (Bruce)

Early operating experience at the Bruce A nuclear generating station, which started operation in 1976, suggested some improvements in the operator interface of the traditionally designed shutdown systems.

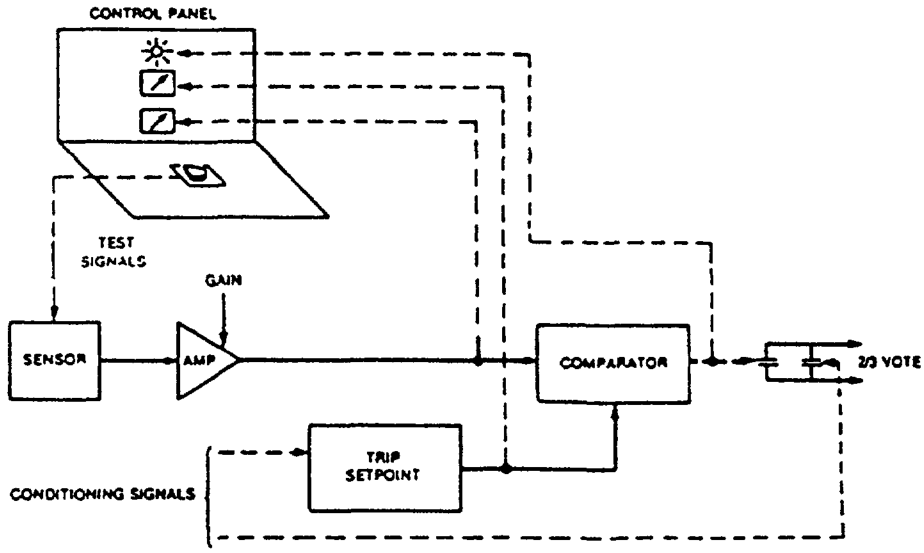


FIGURE 1 TRADITIONAL SHUTDOWN SYSTEM DESIGN

The addition of a second shutdown system (injecting a gadolinium solution into the heavy water moderator), required by new licensing rules, and an increase in the number of in–core flux detector sensors had the effect of increasing the number of trip signals threefold relative to the earlier Pickering reactors.

Aside from the sheer number of measurements for the plant operators to monitor and test, the in–core flux detectors require periodic manual calibration. The flux detectors respond to local flux variations resulting from on–power refuelling, as well as to bulk reactor power changes. These local variations increase the risk of unnecessary reactor shut-downs.

Additional manpower was employed to handle the increased testing and calibration work load, but design improvements were required to enable the operator to assimilate all the trip signal data used to give him early warning of impending reactor trips.

A simple monitor computer system was designed and installed at Bruce to upgrade the operator interface to the two triplicated, channelized shutdown systems. A remote multiplexer in each shutdown system channel scans important signals and sends them to the computer, which constructs effective bar chart displays. The computer also gives the operator warnings if it detects variables too close to their setpoints, failed signals or disagreement among similar signals measured in the three channels. A printer logs abnormal conditions, test data and can provide hard copy for any display.

Figure 2 shows how the monitor computer fits functionally into the shutdown systems.

2.3 Trip Computers (CANDU 6)

The Programmable Digital Comparators (PDC's) in the CANDU 6 plants are the first major applications of microcomputer–based trip logic in CANDU shutdown systems These units have been installed in both Shutdown System Number One (SDS1) and Two (SDS2) on three CANDU 6 plants.

Figure 3 shows a typical schematic of the CANDU 6 shutdown system. As a conservative initial approach, two PDC's are used in each channel (primary and back–up trips are in different computers) and they process seven of the ten trip parameters used in the shutdown systems. The trip parameters for SDS1 are presented in Figure 3. SDS2 trip parameters are similar. Several of these parameters require setpoints which are a function of reactor power and the number of main circulating pumps operating. Microcomputers were chosen to provide the trip logic because they were judged to provide the most flexible and reliable implementation.

The PDCs' principal inputs are the process parameter measurements and their major outputs are the trip contacts associated with each parameter. Each PDC acts as an intelligent comparator while the rest of the shutdown system remains a traditional design.

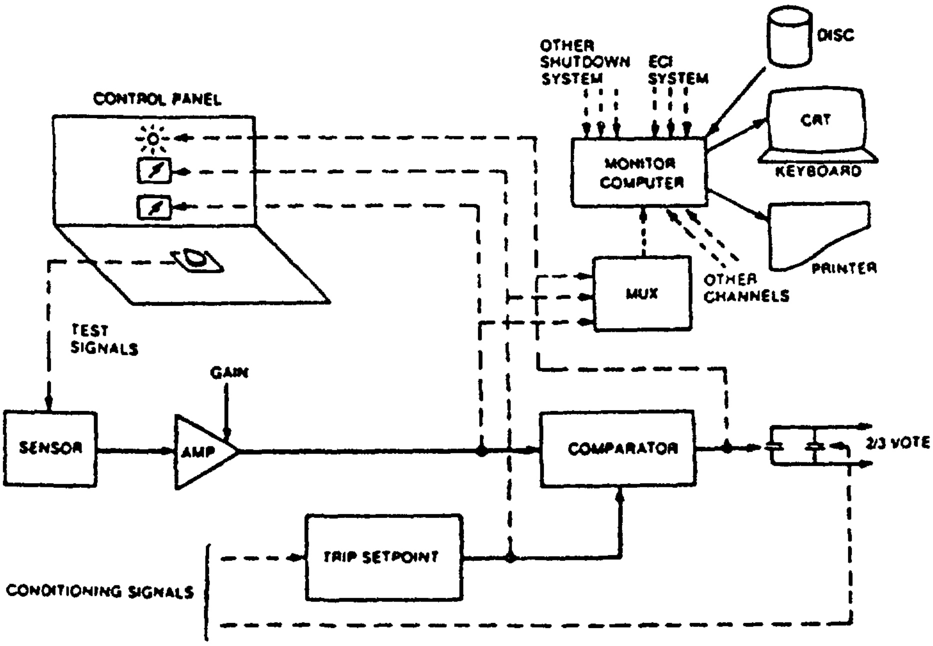


FIGURE 2 TRADITIONAL SHUTDOWN SYSTEM DESIGN PLUS MONITORING COMPUTER (BRUCE)

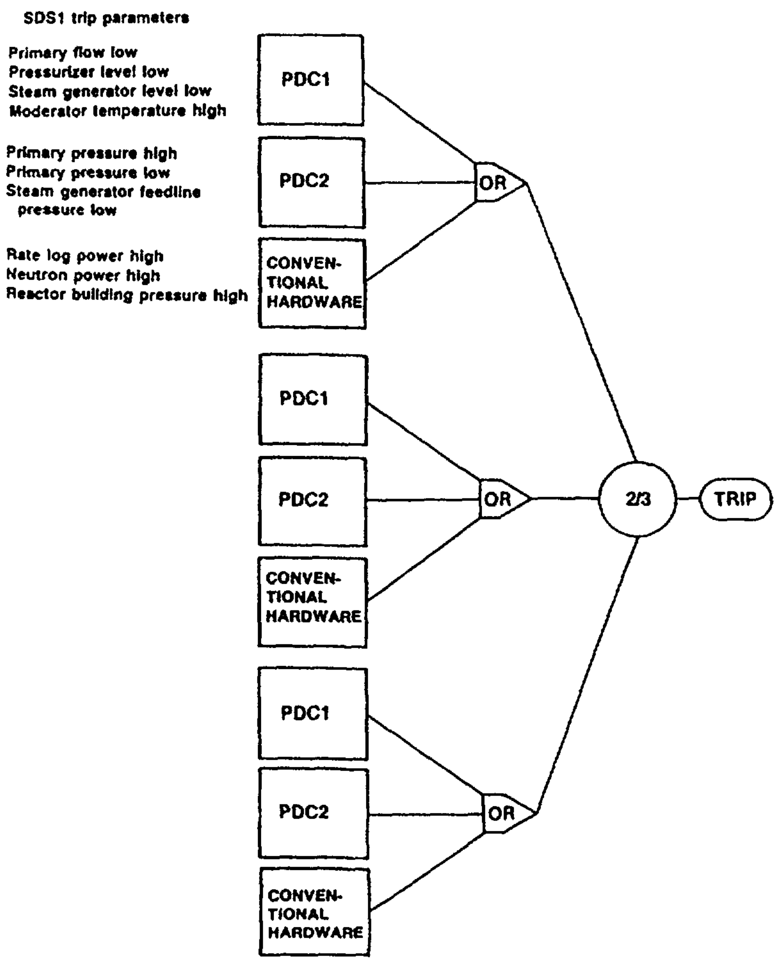


FIGURE 3 CANDU SHUTDOWN SYSTEM UTILIZING PDC'S

Each comparator in both shutdown systems consists of a Data General MP100 which has 8K of PROM memory and 4K words of RAM.

The PDC software is simple and it employs no interrupts or operating system. The software is written in assembly language.

2.4 Fully Computerized Shutdown System (Darlington)

Early in 1982, Ontario Hydro (Canadian utility with 16 operating nuclear reactors and another 4 under construction) and AECL initiated a development program to evaluate a completely computerized shutdown system. The results of this development program were discussed with Atomic Energy Control Board, the Canadian licensing authority, who agreed that the concept would be licensable. Following the successful conclusion of this program Ontario Hydro committed to fully computerized shutdown systems in its Darlington plant (4 x 881 MWe CANDUs). The first unit of the plant is scheduled to be in-service in 1990.

The major functions of this system include trip of the reactor if required, computer assisted testing of safety system components, channelized CRT display of safety system parameters (eliminating conventional panel meters completely) and on-line monitoring of system operation to immediately detect many equipment malfunctions.

Figure 4 shows the hierarchical configuration for SDS1 and SDS2. The bottom layer consists of 6 computers, three for SDS1 (channels D, E and F) and three for SDS2 (channels G, H and J). This is the trip layer and it performs the following functions:

- reads and checks safety system parameters; plant process measurements are read directly into the trip computers via a process I/O system,
- performs the trip determination algorithm and issues trip signals via outputs,
- performs self-checks,
- drives alarm windows on the main control room panels,

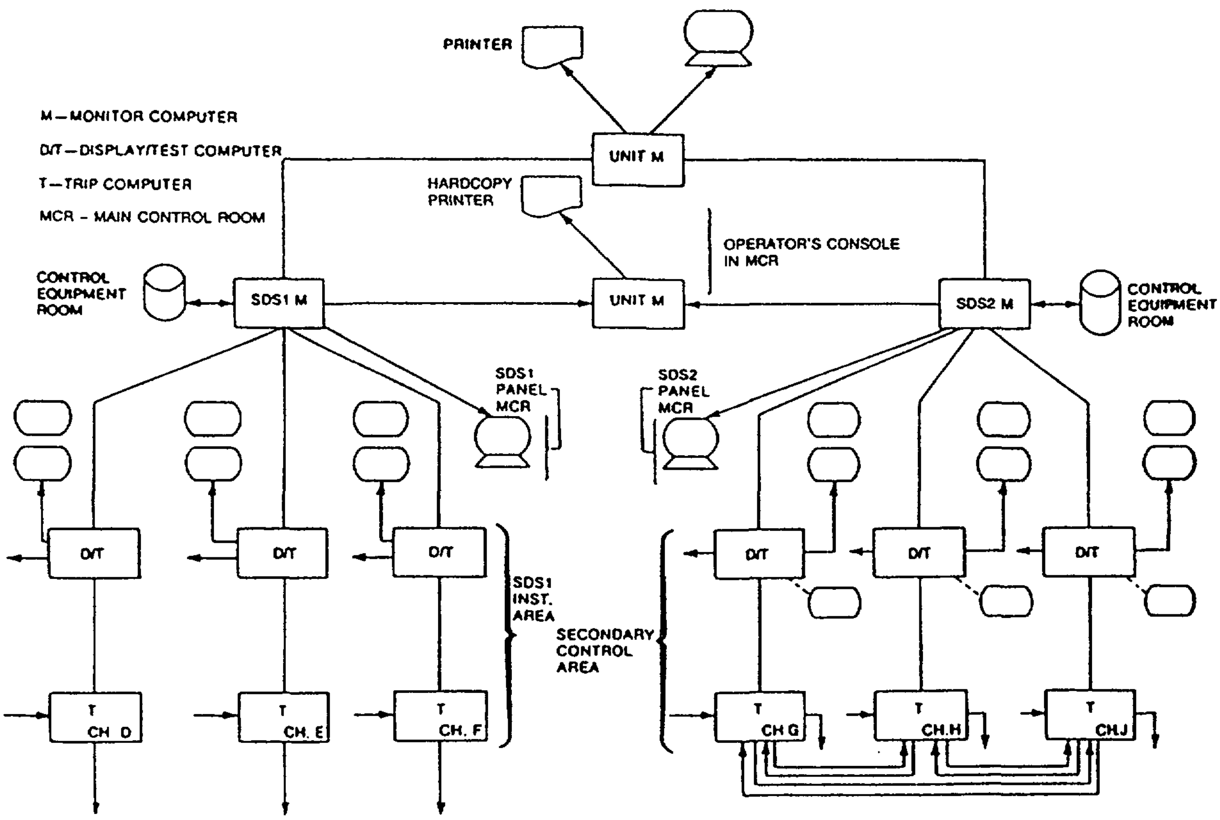


FIGURE 4 CONFIGURATION OF FULLY COMPUTERIZED SHUTDOWN SYSTEMS

- sends plant parameters and trip computer status information to the Display/Test computers via the fibre optic link,
- receives calibration data for in-core self-powered flux detectors from Display/Test computers via the fibre optic link.

The SDS1 Trip Computers are General Automation Model 220 computers, programmed in FORTRAN and GA assembler. The SDS2 Trip Computers are LSI-11 based computers programmed in PASCAL and MACRO assembler. All three channels in each shutdown systems contain identical software (except for channel identification), though SDS1 software is completely different from SDS2 software.

All process and nucleonic measurements in a single channel are connected to the trip computer in that channel. SDS1 uses general coincidence logic (i.e. any channelized parameter exceeding its setpoint can cause a channel trip). SDS2 uses local coincidence logic (i.e., a channel will trip only when the same parameter exceeds its setpoint in at least two channels). In both cases, tripping of at least two out of three channels in SDS1 or SDS2 is necessary for a reactor trip.

The second layer is also channelized. These are the Display/Test Computers. Each Display/Test Computer performs the following functions:

- communicates with the Trip and Monitor Computers,
- drives two panel mounted CRT's in the main control room so that the operator can see the values of the process trip parameters, their setpoints (bar chart display) and channel status,
- issues test signals to field devices on command from the Monitor Computers.
- provides system information in the secondary control area (SDS 2 only), which is geographically quite removed from the main control room.

The third layer is not channelized. This is the Monitor Computer, and there is one per shutdown system. The Monitor computer performs the following functions:

- drives a panel mounted CRT with keyboard that the operator uses to select and execute a system test procedure or input calibration data. This CRT also displays system operating information on demand from the operator. A second CRT/keyboard facility is located at the operator's desk,
- communicates with the Display/Test computer (communication includes test execution instructions, calibration data, system status, parameter readings, test results, echo back of calibration data etc.),
- does consistency checks on the data (e.g. cross channel comparisons of similar parameters),
- prints alarms and test results for permanent record,
- sends alarms and test results to the Shutdown System Monitor Computer (SSMC) for archiving.

The fourth layer, the SSMC (Shutdown System Monitor Computers), accepts data (alarm messages, test results) via serial links from all 8 shutdown systems at the Darlington plant (2 systems in each of 4 reactor units). Its function is archival data storage, with capability to recall data off-line.

All Display/Test and Monitor Computers are GA-220's, programmed in FORTRAN with a small amount of assembler coding for drivers. The SSMC is an industrial IBM-PCAT with a hard disc and 8 serial ports for communications and the programming language used is PASCAL.

3. FAULT TOLERANT AND FAIL SAFE DESIGN

This section outlines the current design principles of the CANDU computerized shutdown system. Sections 5-7 discuss the Darlington design in more detail.

Fault tolerance and a fail safe design would initially appear to be mutually exclusive design features. However, in the CANDU design both features are present. A fault tolerant architecture and fail-safe hardware and software are used in a complementary fashion to achieve the objective of ensuring that malfunctions result in failsafe action. Redundancy, independence, and diversity are strategies used in the design to achieve an adequate level of system fault tolerance and system availability.

The primary defense against safety system malfunction is the system architecture which incorporates failsafe design mechanisms and uses channelizaion, redundancy, and general and local coincidence decision making to achieve fault tolerance. This architecture also allows for overall shutdown system testing to be performed routinely during reactor operation. These features are preserved and enhanced by enforced diversity between the shutdown systems and the selected use of independence in the design. Computer hardware self checks features in the software are supplemented by defensive programming strategy and tactics. These aspects of system design are discussed in more detail below.

3.1 Redundancy, Independence, and Diversity

3.1.1 System Redundancy

Redundancy in the form of duplication, triplication, and channel voting are used to provide a safety shutdown system that will not cause spurious reactor shut-downs for most conceivable combinations of random faults but will initiate action whenever required.

In CANDU reactor systems, there are two redundant shutdown systems, each fully capable of safely shutting down the reactor in the event of any postulated safety–related initiating event. The systems are conceptually and physically different from each other to the extent necessary to ensure that the probability of occurrence of a common mode fault which simultaneously disables both systems unsafely is acceptably low. Redundancy is also used within each shutdown system. Each system consists of three physically separate but conceptually identical channels. These three channels vote on the trip decision and a two–out–of–three channel trip coincidence is required to trip the shutdown system.

One consequence of the combination of redundancy and coincidence in the CANDU reactor trip system is that each entire shutdown system channel (from the physical measurement of the process to the actuating signal to the shutdown device) can be selected for testing while the reactor is operating. The frequency of performing these operational tests is determined by the operations staff based on a calculation of the required demonstrable availability of the system and the maintenance history.

3.1.2 Design Independence

Independence is also used to help ensure that any faults which occur are not likely to be common mode.

For the shutdown systems, a designer for each system specifies the functional requirements for that system and performs a quality assurance and software validation test role for the execution of the computer portion of the design of that system. Independent from this functional design group, the software design group employs a separate software designer for the design of each shutdown system. This design independence is reflected in the separate documentation and testing for the two systems.

3.1.3 Enforced Diversity

The model used for the calculation of targeted system availability assumes that all system failures are independent and random. Enforced diversity is used between the two shutdown systems to ensure that it is improbable that there are common mode failure mechanisms which would affect both systems.

For the conventional instrumentation, this diversity is maintained by choosing separate instrumentation hardware. In an analogous way, separate computer manufacturers are used for each of the two trip computer systems along with separate compilers, computer languages, and development software. The manufacturers employ different computer chip families, have different board layouts, and package their products differently. This provides some assurance against common mode faults due to hardware design, manufacturing errors, compiler and development software errors.

3.2 Computer Defenses

The use of general purpose computers in these systems have allowed an impressive battery of self checking and fault detecting defenses to be built into the computers. These defenses begin with special hardware designs which convert anticipated computer faults into safe tripping actions. These hardware defenses include an external computer watchdog which trips the channel if hardware or software faults prevent it from being pulsed at a pre–determined interval. Wrap around of the process I/O is used to ensure I/O integrity. Redundant trip outputs are used to guard against mechanical and electrical faults.

Interior to the trip computer, hardware–oriented checks implemented in software continuously check the health of the processor, memory, interrupt system, program continuity, and real time clocks. Readings from each of the several sensors are checked for rationality before use. All of these system failures are turned into safe tripping actions accompanied by diagnostic indication. In the upper layer of the system, consistency checking of signals across all three channels ensures early detection of signal degradation.

3.3 Defensive Programming

Several strategic and tactical defensive techniques are used during programming to ensure fail safe action of the computer system. For example, setting parameters to their tripped state is done on every pass and requires the trip function logic to act to untrip them. Another example is avoiding complex time dependent functions to ensure that there is little likelihood of an error being built up over time which might invalidate the trip action.

Extensive rationality checking is made for all critical integer and real variables. Irrational analog inputs from sensor signals representing trip parameters cause a fail safe trip action to take place. Even simple counters are checked to ensure that they are within the proper counting range every time they are used and are treated in a fail safe manner if they are not within that range (e.g. as if they timed out).

4. HARDWARE QUALIFICATION

All the equipment used in the special safety systems has to meet stringent environmental qualification requirements. These requirements are typically included in the specifications provided to the supplier of the equipment. Not all the requirements, however, could be met by off-the-shelf hardware. In this case, modifications had to be made either by the supplier or by AECL. For the PDC's, for example, modifications ranged from chassis reinforcement, component fastening and component replacement for seismic qualification, to the addition of noise suppressing circuits and shielding for conducted transient and electromagnetic interference immunity qualification.

Environmental qualification is done by subjecting the computers and I/O equipment to seismic shaking, elevated temperatures and electromagnetic interferences, while running a test program exercising the memory, CPU and all I/O including the watchdog. When failures occurred during the tests, they were investigated, resolved and the tests repeated until no failures occurred.

5. THE PROTOTYPE FOR DARLINGTON

A basic building block of the software design program for the Darlington shutdown systems was the development of the prototype of the software.

5.1 The Development Program - The Prototype

The decision to investigate the further use of computers in the shutdown systems at Darlington resulted in an extended development program during 1982 and beyond. At that time there were a number of competing software development methodologies in common use and the decision about methodology was therefore of concern. A development program was launched with Ontario Hydro and the licensing authority. This program developed a methodology which resulted in a working prototype of the software. This prototypical effort embodied many structural and detailed decisions about the software and these decisions were the guidelines followed by the software designers in subsequent design work.

5.2 Software Structure Considerations.

One of the first design decisions made during the prototype program was the design of the basic structure, or architecture, of the software. This structure was based on emulation of the hardware design of the reactor trip system – a system composed of individual and physically separate "trips", each trip being a safety subsystem which makes a reactor shutdown decision on the basis of multiple measurements of one distinct parameter.

Our experience had been that changes to the safety system usually include adding whole trips, modifying an existing trip, or changing trip setpoints, as opposed to common changes to all trips. It is important to take into account ease of maintenance for the expected type of changes.

As a result, the software structure consists of a series of separate trip modules. The data (such as setpoints) are segregated out in dedicated data modules.

5.3 The Scheduling Algorithm

Our experience has not given us significant confidence with the use of commercial operating systems. We started using control computers in the 1960's and at that time, commercial operating systems were often defective and prone to unexpected failure. To overcome this obstacle and ensure that we would not have unexplainable phenomena in our control computers, all the software, including the operating system, was programmed in ASSEMBLER by our own designers.

Partially as a result of our control computer experience, for the Darlington trip computers, we were reluctant to use commercial software to any great extent and opted to develop simple scheduling algorithm with a few, rudimentary services. The scheduling algorithm is represented by a simple loop with a fixed execution sequence.

The proper operation of the scheduling algorithm is protected by the watchdog circuit and the software scheduling checks.

6. THE DESIGN PHASE – DARLINGTON

The following is a brief account of current CANDU computerized safety system design practices as developed and applied in the Darlington shutdown system design phase. These practices were developed over the past few years in conjunction with Ontario Hydro and the licensing authority. It should be noted that some of the activities described below were performed by Ontario Hydro to ensure independence (i.e. program function, linkage tables, hazard analysis and quality assessment – see subsections below).

6.1 Software Development Plan

The purpose of this plan is to provide a systematic approach to the software development to ensure that the software for the Shutdown System Computers conforms to established technical and functional requirements. The plan generally follows the Canadian Standard for Software Quality Assurance [reference 09] and has been influenced by International Electrotechnical Commission's standard on Software for Computers [reference 10]. The plan covers topics such as: Surveillance of Activities, Project Management, Sub–Contractor Control, Standards, Change Control, Practices & Conventions, Software Development & Testing, Technical & Design Review, Software Documentation, Software Configuration Management, and Test Control. The plan also authorizes the use of a detailed Programmer's Handbook setting out coding guidelines and a Test Overview Document which defines the test program.

6.2 Software Functional Requirements

The functional requirements for the software system are developed by analysis of the expected station response to postulated initiating events. The functional design resulting from that analysis is detailed in a series of requirements documents for the safety system. One specification in that series of documents is the trip software functional specification.

This document provides detailed information about which trips are required, what process measurements to make, what the trip setpoints and the hysteresis should be, and how these values should change as a function of the operating state of the plant. The document is informative in nature and specifies functional requirements only. It is written by the functional designer who has only a black box knowledge of the implementation of the software design.

6.3 Software Design Specification

The Software Design Specification (SDS) is a formal document prepared by the software designers to interpret the Software Functional Requirements into a precise definition of what is required to be done by the software. The document uses the notation and method developed for the U.S. Naval Laboratories [reference 6] adapted to the needs of a nuclear safety system. The notation and method consist of a standard symbology and a tabular form for writing equations defining the required functions. It allows the requirements to be specified without revealing the details of the software structure or implementation. This document is reviewed by the functional designers to ensure that the interpretation of the requirements made by the software designers is in line with the original intent of the functional design.

6.4 Detailed Design

Once the requirements of the design have been specified precisely, the detailed design can proceed. A module decomposition is performed and a pseudo–code depiction of the logic is produced and a peer technical review is held. When the basic structure and logic of the software is approved, coding and debugging by the software designer takes place. When coding is completed, the finished product is scrutinized by an independent reviewer – a software expert who has not participated in the design. This reviewer ensures that the software meets the specification and all of the project coding standards. The software is now ready for testing (see section 7).

6.5 Verification and Validation (V & V)

The V & V team reviews the software specification produced by the software designers to verify that it interprets the trip computer functional requirements correctly. The V & V team does not become familiar with the details of the computer codes but verifies that the design activities are in accordance with the Software Development Plan. This is achieved through surveillance of activities, ensuring that the project is managed correctly, that the correct Standards, Practices, Conventions and Controls are in place. The software and technical reviews at each stage of the design are conducted by independent reviewers and the V & V team reviews the test check-lists, design and technical reviews and test documentation for compliance. The V & V team also maintain surveillance of the documentation, configuration management and test control of the software.

The testing process is carried out through a series of phases. These phases are called unit, preliminary integration, validation (trip computers only) and system integration testing. Test plans describe the objective, and the methodology to be used for each test. The test plans are cross–referenced to the applicable sections of the Functional Specification to ensure that all aspects of the requirements in the Functional Specification are checked by testing. The testing process is more rigorous for the trip computers. Validation testing of the trip computer software is conducted after the software design is complete and all debugging, unit and preliminary integration testing has been performed. These tests are automated and are implemented in a high level interpreter language. Testing is described in more detail in section 7.

6.6 Program Revisions

The software undergoes revisions due to errors detected in the verification and testing stages or due to regulatory and customer requested changes. Software revision of the program is produced under the design process described above. At each revision stage the software is frozen and validated.

6.7 Program Function and Linkage Tables

When the code is complete it is analysed by two groups of independent Ontario Hydro engineers, using a technique based on suggestions made by D.L. Parnas of Queen's University. One group understands the code but is not familiar with the Software Design Specification. These individuals produce program function tables and program linkage tables which are precise mathematical and tabular representations of the code logic (including sequence dependent attributes). Using these tables and the Software Design Specification, the second group performs a rigorous comparison of the code logic versus the specification. Subsequently a systematic guided inspection of the software product can then be conducted in the presence of the licensing authority. This inspection takes the form of a formal walkthrough for the purpose of code verification.

6.8 Hazard Analysis

A hazard analysis of the trip computer software was performed by Ontario Hydro on the design using the method developed by N.G. Leveson [reference 7] and tools developed by Ontario Hydro for probabilistic risk assessment. An assessment is made of the various hazards associated with the system and a fault tree analysis is performed on the code to determine which critical processes and variables are associated with severe hazards. In this situation, the hazard is defined as failure to initiate shutdown when required and the software is examined to determine which portions of it could potentially compromise safety. Once the critical processes and variables are identified, an assessment is made whether additional error checking and software defenses need to be installed at these points in the software to mitigate against potential failure mechanisms.

6.9 Quality Assessment

A quality audit was performed by Ontario Hydro on the software development project. This audit examined the process used for the design and testing as well as the software itself. The audit made extensive recommendations and assigned a rating to all aspects of the design in the attempt to provide an independent, objective measure of the quality of the project.

7. TESTING OF DARLINGTON COMPUTERIZED SHUTDOWN SYSTEM

7.1 Unit Testing

Software testing begins at the module level with thorough debugging and testing by the programmer. This activity is a test of a software module in an environment especially constructed to provide an easy method to detect logic errors and test functional completeness. Physical inputs, real time, interaction with other modules, and other external stimuli are intentionally simulated rather than real.

Tests check specifically for logic design errors, coding errors, proper software initialization and termination condition handling, and correct software handling of abnormal conditions. In general the tests attempt to ensure "closure" of the software logic design for all conditions which the software may encounter.

7.2 Preliminary Integration Testing

The software is then integrated into the computer system and preliminary integration tests are performed by the independent reviewer as a check to ensure that the group of programs or modules operates correctly as a whole. Like Unit Testing, this test can be far removed from the environment in which the software will eventually function. Integration testing includes tests designed to verify that the data transmitted between modules within a computer and on the communications links between computers is correct and accurate.

7.3 Validation Testing

The tests leading up to the formal validation test (unit and preliminary integration testing) were white box tests which include boundary testing of the software logic. The formal validation test is a black box test that is designed to ensure that the trip computer meets the functional requirements for the design. In essence, while the preceding white box tests detect errors in software coding and execution of the design, the validation tests go back to the fundamental design and look for errors in conceptual understanding of the design.

Validation is performed by the functional designers who do not have a detailed knowledge of the design of the Trip Computer software. This degree of independence is intended to ensure that the test is of the trip function itself, unbiased by any assumptions made on the part of the software designer.

The majority of the validation tests are automated. These test cases are written by the functional designers in a high level interpreter language that is run in a special purpose validation computer which simulates the environment of the plant external to the Trip Computer. In general, it is the trip function only that is tested.

An actual trip computer is used in validation testing. The process I/O and communications port from the validation computer are connected to the process I/O and communications port of the trip computer.

7.4 System Integration Testing

The system integration test is a test of the safety system computer configuration. The test is designed to provide a high level of confidence before installation at site that the integrated system functions in accordance with the software and hardware specifications.

These tests are conducted in the specially built test rig that uses the target computers and other hardware selected for the safety shutdown system. The tests that are performed make use of the validation computer that is connected to the test rig to run test cases which simulate the external environment of the plant.

7.5 Site Testing

All of these tests are supplemented by in–situ tests during commissioning at site. These tests were developed by Ontario Hydro operations staff. One novel feature of the site tests is the use of thousands of trajectory–based randomly generated test cases to test sensitivity of the design to unexpected plant states.

8. EXPERIENCE WITH THE COMPUTERIZED SHUTDOWN SYSTEMS

8.1 Performance Record

Thirty–six PDC's have been in operation in three plants since 1982. In that time there have been no incidents of plant spurious trips due to PDC malfunctions, or failure to trip when required.

Reliability data has been kept at the Point Lepreau CANDU 6 (since first criticality in 1982) on the shutdown systems. A review of this data for a five year period from 1982 to 1987 showed that the PDC's (12 computers replacing about 1500 conventional modules) have failed 44 times. None of these failures were potentially unsafe failures (i.e. the channel failed safe). By comparison, of 146 failures in the conventional hardware (346 modules), 63 failures reduced calculated system availability. This is a clear demonstration of the computer's ability to detect anomalies or failures both in its input data and in its own operation and to fail in a safe manner [reference 5].

PDC portion of each shutdown system has consistently contributed a negligible amount to total system unavailability. At Point Lepreau reactor trip frequency with the reactor critical was 0.75/year for both systems together during the period 1984–1987. (This does not include trips which occurred during plant shut-downs as a result of maintenance activities, and also does not include the first year of operation, 1983, where high power testing and plant shakedown caused a large number of trips to occur.) This result compares favourably with conventional systems currently operating at other CANDU plants.

8.2 Off Line Design Modification

Experience has shown that, from time to time, it may become necessary to modify programmed trip setpoints, alter the conditioning logic, or to add new trip parameters. Such changes may originate from changing operational considerations, regulatory requirements, or analyses. In any case, with conventional technology, the implementation of all but the simplest of changes can be a serious problem because of the competing demands of safety and power production. If the plant has to be shut down to make the changes, a very costly loss of power production may be incurred. If it is kept operating, there can be a significant risk of impaired protection (making an on-line change highly undesirable), or of a costly spurious trip due to installer error during the installation and testing process. With a computerized shutdown system, much of the modification effort is moved off-line, into the software development laboratory, with a significant benefit in reduced unit down time and/or reduced system impairment time. In particular, the use of computers allows activities equivalent to wiring, calibration and testing to occur in parallel with plant operation, with no compromise of the safety system availability.

Recently, for example, a modification to the trip logic (without requiring additional process measurements) was implemented on Point Lepreau to meet new licensing requirements and improve operational flexibility. Because PDC's are used for the trip logic, this change was purely a software logic modification, implemented and tested off-line, with no risk of upsetting the plant. The in-situ activities, consisting principally of inserting in a new memory board and testing each trip channel, took only 2 hours of rejection time per PDC (12 hour rejection time in total). Indeed, the major portion of the rejection time was devoted to an initial round of periodic trip tests of the modified channel. Thus, implementation of this change with PDC's was only a very minor operational burden. With conventional trip logic, such a change would have to be implemented during a plant shutdown involving significant rewiring work and commissioning costs.

8.3 Maintenance/Diagnostic Testing

Based on a Point Lepreau review done in 1988, mean time to failure experienced by the PDC's was 11,000 hours,. Since there are 8,760 hours in a year and 12 installed PDC's this represents an average of 9.6 PDC failures per year. An instrumentation maintenance technician assigned to a shift crew may see no failures of a PDC in a year. As a result, few of the shift maintenance personnel become expert in the PDC repair. Therefore a different approach is used in maintaining the PDC's.

The Point Lepreau maintenance technician is provided with the special service kits containing all the circuit cards required in a PDC. When investigating a problem, the maintenance technician begins by checking the LED-based local error message display and the main control room panel meters. If the problem is in the PDC, the technician gets the service kit and carries out selective replacement of circuit boards. With these arrangements the maintainers are able to achieve a MTTR (Mean Time To Repair) of 2 to 3 hours for a PDC failure. The failed board is then repaired off-line.

9. BENEFITS OF THE COMPUTERIZED DESIGN

A large number of benefits has been achieved by the gradual introduction of computers into reactor shutdown systems. These include:

a. The data presented in Section 8.1 demonstrates that a clear improvement to plant safety has been achieved. This is a result of the computer's capability to quickly detect and annunciate internal and external faults, and then take failsafe action. Mean time to repair a fault is also significantly reduced.

b. Final trip computer software does not need to be available at the station until long after the hardware has been installed and wiring completed. It is therefore easy to accommodate relatively late changes in trip logic, after plant operation has started. Previously such changes always required modifications to the station wiring.

c. Computerized safety systems can provide the operator with more complete information, and can present it in a format that is much easier to assimilate than numerous individual panel meters.

d. Computers can simplify some repetitive, burdensome tasks for the operators such as periodic calibration of the flux detectors and regular testing of shutdown system equipment. The risk of human error is reduced.

10. FUTURE DEVELOPMENTS

Several trends are becoming evident in our present work, and could lead to new developments in the near future. The following are possible candidates for that new development.

The trend to enforced diversity between shutdown systems will continue and it is possible that in the future the shutdown systems may employ more radically different computing devices. For example, one system could employ programmable controllers while the other may be implemented in a general purpose multiprocessor configuration. With one of these configurations we might implement individual trip parameters in individual computing devices. Hardware validation tools may be used on one or both of the systems.

Automated testing will be expanded to include yet more types and varieties of test cases. Considerable effort will be expended in determining what an appropriate test suite is for a given application. Further research will be conducted into the theoretical basis for random testing of computer systems.

Computer Aided Software Engineering (CASE) tools and rapid prototyping will be used to evaluate competing computerized safety implementations and assess appropriate alternative strategies for program structure and execution.

Computer hardware self testing will be improved, possibly through the use of an outboard bus analyzer which could detect the presence of transient "glitches" in the electronics and warn of impending hardware failures.

Software metrics will be employed to measure and evaluate compliance with the software development plan and software engineering standards. In future, it is possible that such methods could form the basis for a software reliability confidence measurement.

Formal methods, already introduced in a limited way into the design process, will be expanded and used to improve the precision and completeness of program specifications. Program "proofs" will be constructed alongside the software as it is being written and these "proofs" will be used to demonstrate that the specified safety task is performed by the software. Automated tools will be used in this process to aid in the construction of proofs.

Automated static analyzers will be used as part of the program inspection and test process to provide computer assistance for conducting a thorough examination of the code. Present analysis methods, such as the hazards analysis, will be integrated into the overall development process.

Some of these developments are under study for our newest project, the CANDU-3, while others are active topics of research at AECL. Despite our excellent experience with computerized safety systems we intend to continue to develop the technology to ensure that the highest standards of safety design are maintained and the full range of benefits resulting from computer implementation are gained by the safety systems.

ACKNOWLEDGEMENTS

Much of the information in this paper has been presented previously in References 1 to 5.

The utilities New Brunswick Electric Power Commission (NBEPC) that is operating Point Lepreau Nuclear Generating Station and Hydro Quebec operating Gentilly II Generating Station are acknowledged for providing results on the performance of the PDC's (Programmable Digital Comparators) for the Safety Shutdown System computers. Design groups at Atomic Energy of Canada Limited and Ontario Hydro are acknowledged for their specific design activities and contribution to the overall design and assessment of the fully computerized Shutdown System for the Darlington Nuclear Generating Station.

REFERENCES

1 HINTON, G.J., KENDRICK, S.H., SHIELS, T.W., SCHAFER, S. "Use of Computers in CANDU Shutdown Systems – An Overview", presented at the IAEA Specialists Meeting on "Microprocessors in Systems Important to the Safety of Nuclear Power Plants" in London, England, May 1988.

2 CONDOR, A.E., HINTON, G.J. "Fault Tolerant and Failsafe Design of CANDU Computerized Shutdown Systems", May 1988, presented at the IAEA Specialists Meeting on "Microprocessors in Systems Important to the Safety of Nuclear Power Plants" in London, England, May 1988..

3 CONDOR, A.E., HINTON, G.J., KENDRICK, S.H. "Software Design Methodology for CANDU Safety Systems", presented at the IAEA Specialists Meeting on "Microprocessors in Systems Important to the Safety of Nuclear Power Plants" in London, England, May 1988.

4 KENDRICK, S.H., KEATES, A.A.G., RUSSOMANNO, S.A., SUTHERLAND, J.G. "Verification and Validation of the CANDU Safety System Computer Software", presented at the IAEA Specialists Meeting on "Microprocessors in Systems Important to the Safety of Nuclear Power Plants" in London, England, May 1988.

5 PAUKSENS, J., CONDOR, A.E., POPOVIC, J., ROSEVEAR, A., "CANDU Experience With Computerized Scram", Proceedings of the Third International Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, Seoul, November 1988.

6 HENINGER, K.L., KALLANDER, J.W., PARNAS, D.L., and SHORE, J.E., "Software Requirements for the A–7E Aircraft", NRL Memorandum Report 3876, Naval Research Laboratory, Washington D.C.

7 LEVESON, N.G., HARVEY, P.R., "Analysing Software Safety", Transactions on Sofware Engineering, Vol. SE–9, No. 5, September, 1983.

8 BERGLAND, G.D., "A guided Tour of Program Design Methodologies", Computer, October 1981.

9 Canadian Standards Association, **Software Quality Assurance Program,** CSA Q396.1, 1984.

10 International Electrotechnical Commission, **Software for Computers in the Safety Systems of Nuclear Power Stations,** IEC Standard 880.

SAFETY RECOMMENDATIONS FOR ADVANCED REACTORS IN THE NETHERLANDS

B.T. EENDEBAK
Joint Laboratories and Other Services
of the Dutch Electricity Supply Companies,
Arnhem

J.E. SPEELMAN, J.A. HEIL
Netherlands Energy Research Foundation,
Petten

Netherlands

Abstract

Following the accident in Chernobyl the Dutch authorities deferred their decision on the construction of two nuclear power plants and announced a series of so-called post-Chernobyl studies. These studies have been finalized, and are under discussion in several governmental advisory committees. One of the studies concerns the source term achievable for nuclear power plants to be built in the near future. This source term study (performed by ECN) was based on the results of recent PRA's and on possible effects of severe accident management measures.
The most important recommendations of the source term study are:

- The core melt frequency should be less than 10^{-5} per reactor year.
- The relation between release magnitude and probability satisfies at least the following requirements:
  - the probability is 10^{-6} per reactor year for a relatively small release (viz. Cs,I: 0.1%)
  - the probability is 10^{-8} to 10^{-7} per reactor year for a medium-sized release (viz. Cs,I: 1%)
  - the large releases of more than 10% of the volatile fission products (I,Cs) is ruled out, i.e. the probability of its occurrence is lower than 10^{-9} per reactor year.

The Dutch committee on reactor safety (CRV) has approved the conclusions of this source term study. However, it is recognized that the interpretation of the source term recommendations is still subject of discussion between the government and the industry. The government's risk assessment policy will be briefly presented in the paper.

The source term recommendations lead to a number of requirements for the design specification of the new nuclear power plants. Two important items in this discussion concern:

- the consequences for the design specification of new nuclear power plants and the modifications necessary to fulfil the additional requirements.
- the role that inherent and passive safety features play in the design of nuclear plants and the way these features are affected by the existing legal framework.

Presently KEMA participates in the EPRI programme on advanced reactors. A major contribution is the availability of the Dodewaard nuclear power plant. This plant is a 65 MWe natural circulation boiling water reactor that already exhibits many safety features as proposed for advanced reactors. The Dodewaard reactor is considered to be prototypical for a SBWR, and might be used to demonstrate various new features.

1. INTRODUCTION

Following the accident in Chernobyl the Dutch authorities deferred their decision on the construction of two nuclear power plants and announced a series of so-called post-Chernobyl studies. These studies have been finalized, and are under discussion in several governmental advisory committees. One of the studies concerns the source term achievable for nuclear power plants to be built in the near future. This source term study was based on the results of recent PRA's and on possible effects of severe accident management measures [1], [2], [3]. In the source term study it was concluded that for new reactors it will be achievable to request a core melt frequency of less than 10^{-5} per year. In addition a relation between release magnitude and probability has been recommended. The Dutch committee on reactor safety (CRV) has approved the conclusions of this source term study. The rulemaking for the new nuclear power stations is in progress. Attention will be given to severe accidents; a PRA will be required.

In the Netherlands the ministry of Housing, Physical planning and the Environment is developing rules concerning safety and environmental consequences of large industrial facilities. This rule making has not been finalized, however it is the general impression that reactors built according to the source term recommendation and even present operating plants will not encounter difficulties to meet the requirements under consideration. Nevertheless public opinion still rejects the building of nuclear power plants. Therefore decisions on extending nuclear power in the Netherlands are postponed.

2. SOURCE TERM RECOMMENDATIONS

The most important recommendations of the source term study are:
- The core melt frequency should be less than 10^{-5} per reactor year.
- The relation between release magnitude and probability satisfies at least the following requirements:
  - the probability is 10^{-6} per reactor year for a relatively small release (viz. Cs,I: 0.1%)
  - the probability is 10^{-8} to 10^{-7} per reactor year for a medium-sized release (viz. Cs,I: 1%)
  - the large releases of more than 10% of the volatile fission products (I,Cs) is ruled out, i.e. the probability of its occurrence is lower than 10^{-9} per reactor year.

The ECN source term recommendation requests for a core melt frequency of less than 10^{-5}. Due to the economical consequences in case of a reactor accident, this figure should be as low as practically achievable. In view of the intolerable economical consequences large releases should be ruled out. This means among others avoiding early containment failure and containment bypass without mitigating measures. The containment should be designed in such a way that it can meet all occurring loads during severe accidents. However the processes occurring during severe accidents are very complex and quantification of loads and failure pressure is difficult. The ECN source term study regards an overlap of the probability distribution for loads with the probability distribution of containment failure pressure of the magnitude of 10^{-4} as suitable to state that early containment failure will be improbable (see figure 1). Multiplying this number (10^{-4}) with the core melt frequency (10^{-5}) leads to a figure of 10^{-9}. It should be kept in mind that the number of 10^{-9} can not be regarded as an exact

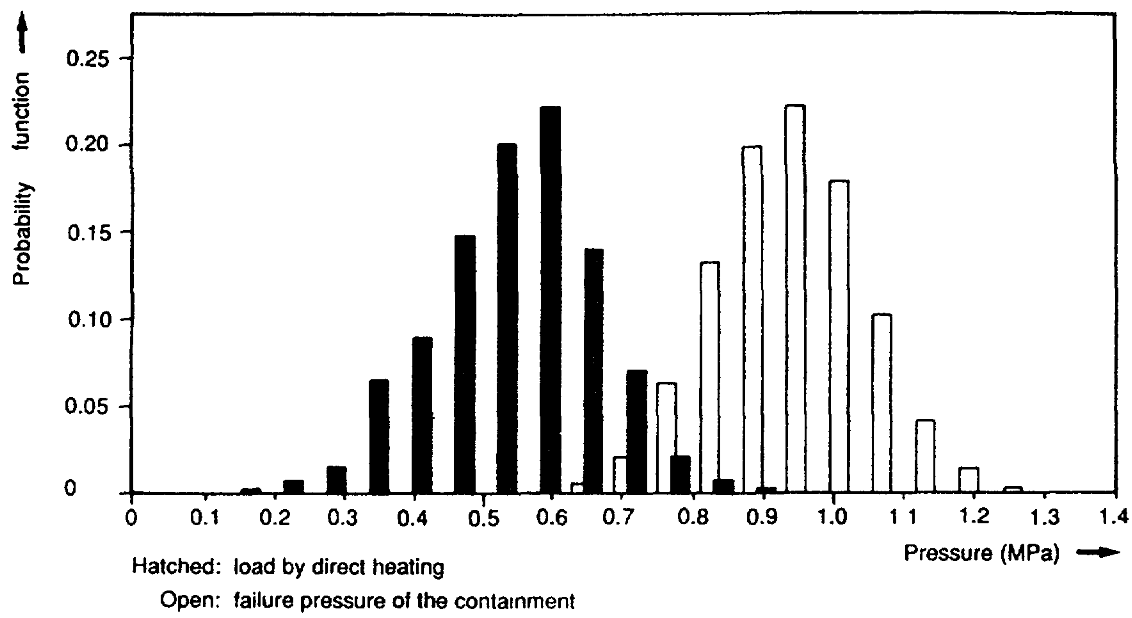


FIGURE 1: Probability distribution of pressure build up as function of direct heating and the probability of reaching the failure pressure of the containment (for ZION NPP)

frequency, however the proposed procedure leads to a very safe reactor for which can be stated that large releases can be excluded. In this domain PRA's are more suitable for comparison and system improvement.

3. THE GOVERNMENT'S RISK ASSESSMENT POLICY

The government's environmental policy [4] is aimed at promoting sustained growth while at the same time safeguarding man, animals, plants, ecosystems and property. To achieve these objectives, two lines of policy are being followed: the introduction of measures to deal specifically with known sources of pollution as well as initiatives to address the impact of contaminants. The source-oriented approach aims to prevent unnecessary environmental pollution, whereas impact-related policies are directed towards avoiding deleterious effects on man, animals, plants, ecosystems, environmental functions and property. The concept of risk assessment is therefore fundamental to impact-related policies and provides a means of defining "non-detrimental conditions". Adoption of this approach allows guidelines to be established for quantifying the harmful consequences of pollution in relation to estimated risks and threshold values.
The maximum permissible mortality risk to human beings from major accidents, exposure to substances and radiation has been defined such that the combined probability of mortality for each of these three hazards should not exceed 10^{-5}/year. For each activity or substance, the maximum permissible level has been set at 10^{-6} /year. Comparable values have been defined for diseases (effects without threshold levels) as well as for the nuisance caused by noise or unpleasant odors.
The limits chosen for the group risk specify that the likelihood of an accident with 10 deaths occurring shall not exceed one in every hundred thousand years and as such aim to prevent social disruption. Disasters with even more serious consequences lead to corresponding greater degrees of

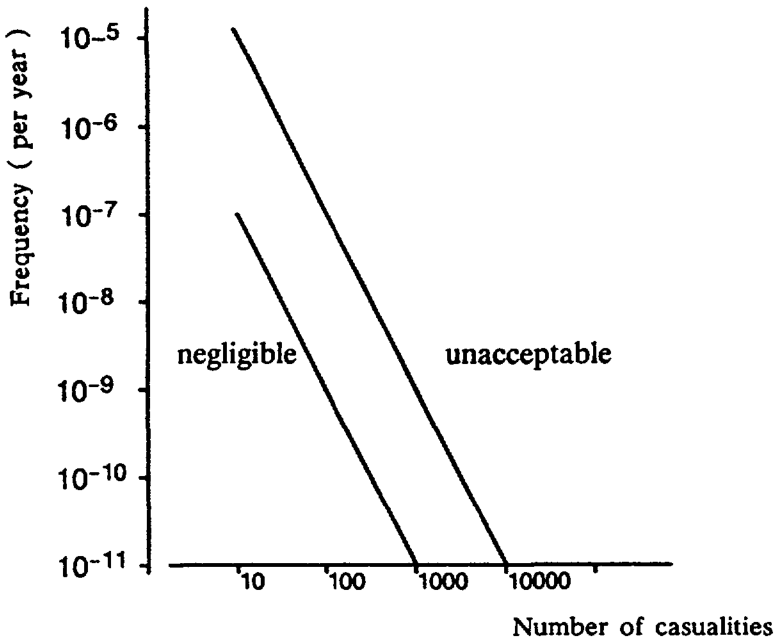


FIGURE 2: Group risk (mortality of n or more persons) limits for major accidents [4]

disruption. It is therefore assumed that an n-times larger impact should correspond with an n-squared times smaller probability of such an accident occurring (see figure 2).

When comparing perceived risks with the limits set, a distinction is generally made between existing and new activities. In the case of existing activities that give rise to situations in which the specified limits are exceeded, social considerations are often of importance when determining the period over which these hazards should be curbed. New activities, however, must comply with the specified limits immediately. In continuing to develop such policies, the government intends to further assess the risks posed to ecosystems over the coming decade as well as to investigate the financial consequences of impairing the economic functions of the environment, particular in terms of the damage to agricultural land or groundwater used for drinking water supplies.
Finally, attempts will be made to promote policies for reducing environmental risks at an international level and to encourage the use of risk assessment in conjunction with acceptable limits as a basis for decision-making.

4. INHERENT AND PASSIVE SAFETY FEATURES IN THE DESIGN OF NUCLEAR POWER PLANTS

To-day's legislation and related rules and regulations on nuclear power plants are based on existing technology used for the present day generation of plants. Claimed inherent safety features of new designs cannot be judged using the tools given by the existing legal framework. However increased safety for next generation plants may be needed in view of the societal risk caused by a substantial increase in the use of nuclear power;

passively safe reactors may play an important role in the future. For that reason the Dutch electricity companies are carrying out a study on methods suited for preliminary safety reviews of next generation plants with passive safety features. In the following some of the results will be presented and some examples derived from the Small Boiling Water Reactor (SBWR) and the Dodewaard reactor will be given.

4.1. BASIC SAFETY PRINCIPLES

The International Nuclear Safety Advisory Group of the IAEA described the main basic safety principle as follows [5]: "To protect individuals, society and the environment by establishing and maintaining in nuclear power plants an effective defence against radiological hazards". A top-level objective like this has to be followed by more detailed and/or quantitative safety principles or design criteria forming together a consistent framework. Examples of such frameworks can be found in documents of the IAEA [5], [6], of the commission of the European Communities [7] or in national policy statements like that of the United Kingdom's Nuclear Installations Inspectorate [8]. In principle, the approach to nuclear safety can be followed either in a deterministic or a probabilistic way. However, it can be stated that the safety concept of nuclear power plants is based on a deterministic approach and that probabilistic methods are used to develop better insights and as a confirmatory tool supplementing the deterministic safety case in achieving a balanced safety design. Most of the deterministic principles can be derived from the "defence in depth" concept, that provides an overall strategy for safety measures and features of nuclear power plants. According to that strategy nuclear installations have to be designed, constructed and operated in such a way that radioactive materials are contained within a succession of physical barriers. Measures have to be taken that these barriers will function during all operational states and during accident conditions as well. To minimize the probability of a break-through of these barriers the concept of "defence in depth" has to be applied. In this concept a series of echelons is established in such a way that failure of one echelon will be compensated for by the existence of the other levels.

In general the basic safety principles in use in Europe as well as in the USA are very much alike on the level of the defence in depth theory, the list or categorization of design operating conditions and the list of internal design basis accidents. Differences exist, however, in the specific deterministic rules and regulations on system and component design and on the design against external hazards.

An inventory of existing nuclear rules and regulations "derived" from the defence in depth-concept is like a moving target. It is continuously moving particular at the lower level of recommendations and guidelines. Especially the accidents in Three Mile Island and in Chernobyl has started discussions on a number of important licensing issues.

In table 1 an overview is given of some of the most important safety-related items mentioned as well as an indication of the kind of requirements that has to be fulfilled or that are under discussion. The consensus of these requirements is not yet clear but in general it can be expected that requirements as mentioned in table 1 have to be fulfilled for nuclear power stations to be built in The Netherlands. Although the basics of the concept of the defence in depth have been unchanged throughout the years, among others resulting from special requirements as mentioned in table 1, some, almost generally accepted modifications and extensions can be noticed.

TABLE 1	SPECIAL REQUIREMENTS ON SEVERE ACCIDENT CONTROL
Subject	Requirements
human failure	training, procedures, man-machine interface has to satisfy the latest state of the art
H_2-control	detection and control (e.g. by inertization or recombination) of H_2-concentrations in the containment
emergency instrumentation	instrumentation needed to be informed of and to control the accident has to be "accident proof" for the whole range of accidents
reactivity control	ATWS has to be controlled
accident management	physic state emergency procedures have to be implemented, dealing with design as well as beyond design basis accidents
fire prevention and fighting	fire prevention and fighting systems have to satisfy the latest state of the art
containment	the containment has to be protected against failure by molten core material or by steam-spikes; over-power protection has to be provided
emergency planning and preparedness	EP&P of the operator and the government has to be consistent and able to cope with all emergencies

In most recent descriptions of the defence in depth theory mitigation and prevention are mentioned separately and sometimes an extra level of defence is added dealing with emergency measures. In table 2 a scheme is presented in which the defence in depth levels are given as well as examples of the major approaches to be followed to fulfil the aimed goals. Nomenclature of the last three levels (i.e. plant-, site- and off-site emergencies) is derived from the IAEA safety series no. 50-SG-06 [9].

Table 2 shows a way to quantify the qualitative requirements as mentioned in table 1. The definition of severe accidents and therefore the criteria on mitigating and preventing measures or systems can be based on a definition of a site emergency or off-site emergency. These definitions given by the IAEA [9] can be derived easily from the relevant (national) emergency reference levels.

4.2. INHERENT AND PASSIVE SAFETY

Many designs of next generation plants are characterized by the use of passive safety systems. Therefore it is inevitable that criteria for next generation plants will deal with inherent and passive safety features.
A discussion on inherent and passive safety asks for a careful use of safety related terms. Descriptions and definitions used hereafter are based on the definitions advised by a IAEA committee [10]. Inherent safety characteristics refer to basic choices in the materials used or to other

TABLE 2 EXTENSIVE DEFENCE IN DEPTH

Level	Goal	Major approaches
normal operation	mitigate "normal" releases prevent incidents	design, quality control inspection, maintenance ventilation, rad waste control
incidents	mitigate incidents prevent accidents	alarm systems control systems
accidents (plant emergency)	mitigate accidents prevent severe accidents	reactor protection system emergency core cooling decay heat removal containment
severe accidents (site emergency)	mitigate on-site consequences prevent off-site consequences	design features accident management
off-site emergency	mitigate off-site consequences	emergency planning and preparedness

aspects of the design which assure through the laws of nature only that a particular potential hazard cannot be a safety concern in any way. The term passive safety has a somewhat different meaning. A passive component is a component which does not need any external input to operate and a passive safety function is a function to be achieved by means of passive components or systems.

Table 3 gives a number of examples of active and passive safety features. It has proved useful to break these down into 5 categories of safety systems. As a rule, it is expected that the relevant safety system going from active to passive, will increase in safety. The most appealing properties are those that form an inevitable part of nature and that some call "God-given-safety" [11]. A close second are the safety aspects that are based on the design. Independent supplies of energy and coolant are also considered to be passive safety systems. The criterion for this is that it must be impossible for passive safety systems to be endangered by a common cause or external influence. A "passively safe" reactor should thus be a reactor that contains passive safety systems only.

In such a type of reactor power control, cooling of the core, heat dissipation and containment would be guaranteed by passive safety measures only. In practice, however, the differences between the categories of safety systems mentioned does not prove to be quite so unequivocal and many safety systems will function because they form a combination of various safety categories. Favorably chosen reactivity coefficients and material properties can only work within the geometry of the construction. Natural circulation will not work without the boundaries of the construction and even the passive safety based upon material properties will have to be guaranteed throughout the plant's operational life by quality control.

It should be clear that there is no inherently safe nuclear reactor in the sense of a reactor which is absolutely safe. In that respect a nuclear reactor is not different from any other machine. Safety is still a relative

TABLE 3 EXAMPLE OF ACTIVE AND PASSIVE SAFETY FEATURES

active:	human action	* prescribed actions * autonomous actions * assessment of the situation
	safety systems	* instruments * control systems * pumps, valves, etc.
passive:	independent systems	*(water) supplies * accumulators * batteries * rupture discs * check valves
	construction	* geometry, dimensions, walls, floors, etc. * vessels, pipes
	laws of nature (inherent safety)	* heat conduction and transport * reactivity coefficients * material properties for shielding and containment

concept and the question "how safe is safe enough" should at least be answered in relation with the minimum safety requirements to be met. However, the design of a nuclear power plant with an increased number of passive safety systems can be (far) less complicated, which will result in a plant that is easy to operate and requires shorter construction time and a simpler licensing procedure. On the other hand the advanced reactor proposed so far might have drawbacks and only a careful analysis of all the pros and cons will lead to a well-considered design.

5. APPLICATION OF THE "DEFENCE IN DEPTH" CONCEPT

In general it can be stated that the current safety criteria in use are not suited for the assessment of new designs especially when passive safety features are involved. Moreover the preliminary design phase of most proposed advanced reactors does not allow a detailed comparison with existing deterministic rules and regulations nor allow the performance of a PRA level 1. So only more general safety principles can be considered for a comparison with and adaption to new safety concepts. The main safety principle involved is as explained before the concept of defence in depth together with the single failure criterion and the influence of human action. These items will now be addressed successively.

5.1. DEFENCE IN DEPTH

In the discussion on "Inherent and passive safety" an overview is given on active and passive features. From that it has become clear that it is practically impossible to achieve a 100% passive safety solution.
With a careful definition, however, most safety systems or safety features can be nominated as "passive" or "active". In view of the defence in depth theory it is of interest whether the mitigation or prevention of a certain level of defence is achieved by passive or active means.

Therefore in table 4 an overview of possible safety measures, passive as well as active, are given. Most of the safety measures mentioned in this table are realized in the light water reactor as operating today. Other features are only partially used in practice or proposed for next generation plants. This is in particular true for the passive safety measures for the levels 3 and 4 as indicated in table 4.

TABLE 4 PASSIVE AND ACTIVE SAFETY AS PART OF THE DEFENCE IN DEPTH LEVELS

Level	Safety measures passive	active
1 normal operation	design multiple barriers	inspection and maintenance procedures
2 incidents	material properties laws of nature	alarm systems control systems
3 accidents (plant emergency)	reactivity control emergency core cooling decay heat removal containment integrity	reactor protection system reactivitycontrol decay heat removal containment integrity
4 severe accidents (site emergency)	design features of primary system containment and building lay-out	accident management
5 off-site emergency	siting emergency planning and preparedness	

A nuclear reactor that claims to be a passively safe reactor therefore could be characterized by:

a inherent safety features concerning material properties and reactivity constants
b a passive solution for the four safety functions
c passive design features in order to prevent off-site consequences.

5.2. SINGLE FAILURE CRITERION

The "Single Failure Criterion" is one of the most important design criteria for nuclear power plants and has been applied from the very start. The definition of this criterion, however, has been changed from time to time and differences in application between the USA and some European countries are evident. The last remark holds especially in view of the application to passive or active systems. A recent description of the Single Failure Criterion given by the IAEA [6] reads as follows: "An assembly of equipment satisfies the Single Failure Criterion if it is able to meet its purpose despite a single random failure assumed to occur anywhere in the assembly. Consequential failures resulting from the assumed single failure are considered to be an integral part of the single failure" (art. 329). "The Single Failure Criterion shall be applied to each safety group incorporated in the plant design, where by safety group is meant that assembly of equipment which performs all actions required for a particular PIE in order that the limits specified in the design basis for that event are not exceeded" (art. 330).

Compliance with the Single Failure Criterion as defined here will certainly be a requirement by the Dutch authorities. For the design of an advanced reactor, using predominantly passive safety systems, it is important that non-failure of passive components has to be justified based on accident and failure analysis of the system and components involved. Moreover it is doubtful whether a safety function could be met by means of passive safety features only.

The preceding discussion of the concept "inherent and passive safety" has demonstrated that there are fundamental reasons that require certain exceptions to be made. The deterministic "Single Failure Criterion" could then e.g. be replaced by a "Multiple Failure Criterion", applied to the active components of the four principal safety functions: reactivity control, core cooling, heat dissipation and containment of radioactive material. For passively safe reactors an adapted requirement could therefore be that the reliability of the relevant safety system or function should not be influenced by the unreliability of the active components involved or in probabilistic terms: the contribution to the failure of a given safety function by failure of active components should be less than a specified percentage.

5.3. HUMAN ACTION

Until now two nuclear power plants have been wrecked because of accidents, viz. TMI-2 in the United States in 1979 and Chernobyl-4 in the Soviet Union in 1986. The analyses have shown that in both these accidents plant personnel was significantly involved in the cause and development of the accidents. Therefore it is important for nuclear power plants to be built in such a way that no rapid action is required on the part of the personnel to prevent the occurrence of an accident. This should be effected by safety systems that operate automatically, or better yet: through passive safety factors. An assessment of this aspect can be based partly on the time during which the power plant can be left to its own resources without any danger to the surrounding area.

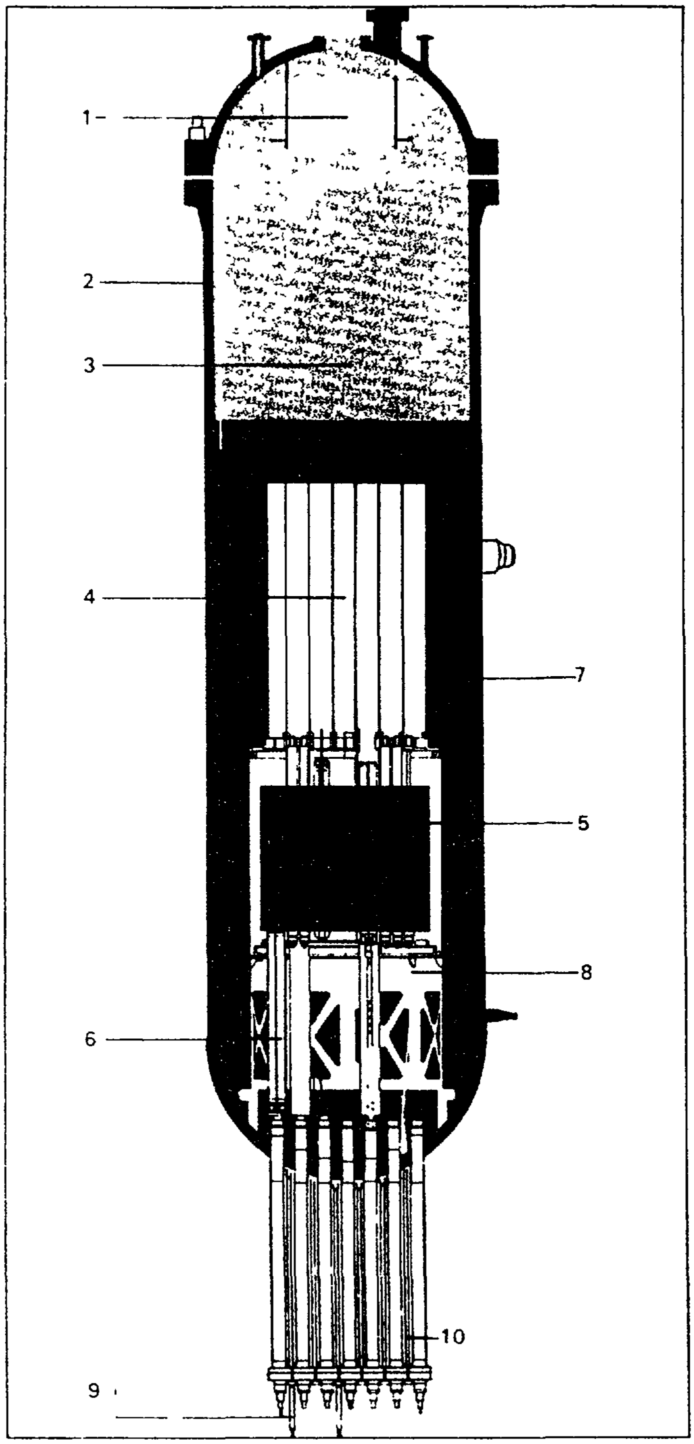
In Anglo-Saxon literature this is sometimes called the plant's "walk-away time" or "grace period". However, in such a forgiving type of power plant one will need to use specifically human ingenuity in enabling personnel to take extra safety measures on the basis of accurate information. In analogy with the definition of operating and design basis earthquakes an operating and design basis grace period can be defined as follows:

- the operating basis grace period is the period of time during which safety is ensured without the necessity of human action or attendance in the event of an incident or accident. Operation of the plant can be continued without violating technical specification limits. The off-site radiological doses during and after this period has to fulfil the relevant criteria for normal power operation
- the design basis grace period is the period of time during which environmental safety is ensured without the necessity of human action or attendance in the event of an incident or accident. The off-site radiological doses during or after this period has to fulfil applicable accident off-site radiological dose criteria (e.g. limits set for plant condition 5).

For some advanced plants grace periods of days or even much longer for the design basis grace period are claimed and can be considered feasible. The safety criteria described should be fulfilled by an improved (evolutionary) design. These designs follow a route of gradually improvements from existing, well proven reactor designs and rely upon the base of experience gathered over several decades of operating experience.

6. THE SBWR AND THE GKN (DODEWAARD) NUCLEAR POWER PLANT

The methodology described can be and was used for preliminary safety reviews of next generation plants. Presently KEMA participates in the EPRI Program on advanced reactors. One of the reasons for that participation is the fact that the Dutch electricity production companies operate since many years a small boiling water reactor at Dodewaard, that already exhibits some important safety features as proposed for advanced reactors. In that way this reactor can be considered as a kind of prototype for a SBWR and might be used to demonstrate various new features. The construction of the Dodewaard nuclear power plant was started in 1965 and at the end of 1968 the power plant was put into operation. Its thermal output was 163.4 MW and has been increased to 183 MW. The Dodewaard reactor is a thermal boiling water reactor. The constructions inside the vessel are such that core cooling by natural circulation is guaranteed during normal operation and for decay heat removal. No recirculation pumps or steam separators are needed (see figure 3). A specific safety system at the Dodewaard power plant (also proposed for the SBWR), is its isolation condenser. This system makes it possible, in case all the other cooling systems do not function, to remove the heat and thus depressurize the reactor without using pumps. The only active component in the system is the return valve, which can be operated automatically as well as manually.
Since its commissioning the Dodewaard Nuclear Power Plant has contributed to research into the various aspects of the operation of a nuclear power plant. Most of this research is done in close cooperation with KEMA, the research institute of the Dutch utilities, as well as with other national and international research institutes and organizations. So e.g. research into "noise" from reactor-parameters is done jointly with the Interuniversity Reactor Institute at Delft (The Netherlands). Incore instrumentation has been developed together with the Norwegian reactor institute at Halden. There is close cooperation with General Electric by their work on the SBWR to scale up the boiling water reactor with natural circulation concept to 600 MW. There are close connections with the US Electric Power Research Institute (EPRI), The Japanese Atomic Energy Research Institute (JAERI) and the Japanese firm Toshiba. Research projects are carried out together with the Netherlands Energy Research Foundation ECN and the Belgium Nuclear Research Center at Mol (SCK/CEN).
The experience with and the research at the Dodewaard Nuclear Power Plant have resulted in a relevant contribution to the discussion on inherent and passive safety features for next generation plants.



Legend
1 steam dryer
2 reactor vessel
3 steam separation room
4 chimney
5 fuel element
6 control rod
7 downcomer
8 shroud
9 tubes for incore instrumentation
10 control rod driving system

FIGURE 3: Longitudinal section of the GKN (Dodewaard)

7. CONCLUSIONS

In the Netherlands rulemaking for new reactor plants is in progress. The ministry of Housing, Physical planning and the environnement is developing rules concerning safety and environmental consequences of large industrial facilities, including nuclear reactors. ECN has performed a source term

study for new reactors, which has resulted in a number of recommendations. An evolution of current designs is expected to be sufficient to fulfil the governmental requirements.
The Dutch electricity companies are carrying out a study on methods suited for preliminary safety reviews of next generation plants. Two important items in this discussion concern:

- the consequences for the design specification of new reactor plants and the modifications necessary to fulfil the additional requirements.
- the role that inherent and passive safety play in the design of nuclear plants and the way these features are effected by the existing legal frameworks.

The KEMA participates in the development of the SBWR. The Dodewaard reactor, a 65 MWe natural circulation boiling water reactor that already exhibits many safety features as proposed for advanced reactors, is considered to be prototypical for a SBWR, and might be used to demonstrate various new features.

REFERENCES

[1] J.E. Speelman, J.A. Heil et al., Ernstige reactorongevallen opnieuw bezien: de bronterm, ECN-PB-87-13, Petten NL (in Dutch)

[2] J.E. Speelman, J.A. Heil, J. Heijn, Severe reactor accidents reconsidered: the source term, ECN-PB-88-16, Petten NL

[3] J.E. Speelman, J.A. Heil, Severe Accident Management in Nuclear Power Plants, proceedings of a symposium, Sorrento, 21-25 march, 1988,IAEA-SM-296/114

[4] Dealing With Risks, Risk assessment in the context of environmental policy (draft) Directorate General for environmental Management at the Ministry of Housing, Physical Planning and the Environment. (Private communication).

[5] INSAG (International Nuclear Safety Advisory Group), 1988
Basic safety principles for nuclear power plants
Safety series No. 75-INSAG-3, IAEA, Vienna, 1988

[6] IAEA, 1988
Codes on the safety of nuclear power plants:
Safety series No. 50-CD (rev. 1), Vienna, 1988; Design
Safety series No. 50-C-O (rev. 1), Vienna, 1988; Operation
Safety series No. 50-C-QA (rev. 1), Vienna, 1988; Quality Assurance

[7] CEC (Commission of the European Communities), 1981
Safety principles for light water reactor nuclear power plants
COM (81) 519 Final, Communication from the Commission to the Council

[8] NII (Nuclear Installations Inspectorate), 1982
Safety assessment principles for nuclear power reactors

[9] IAEA, 1982
Preparedness of the operating organization for emergencies at nuclear power plants
Safety Series No. 50-SG-06, IAEA, Vienna, 1982

[10] IAEA, TCM, 1988; 622-I3-TC-633
Description of safety related terms
Draft, October 1988

[11] Taketoni, Kiyoaki, Explication of inherently safe reactors
Proceedings first international seminar on small and medium sized reactors, Lausanne, Switzerland, 1987

THE SAFE INTEGRAL REACTOR
Development for the next generation

M.R. HAYNS
AEA Technology,
Harwell Laboratory,
United Kingdom Atomic Energy Authority,
Harwell, Didcot, Oxfordshire,
United Kingdom

T.A. JONES
Combustion Engineering, Inc.,
Windsor, Connecticut,
United States of America

K.R. TEARE
Rolls-Royce and Associates Limited,
Derby, Derbyshire,
United Kingdom

R. BRADBURY
Stone and Webster Engineering Corporation,
Boston, Massachusetts,
United States of America

Abstract

For any reactor to stand a chance of being accepted as a realistic contender for deployment as a next generation plant it must embody features such as simplicity, robustness against maloperation, economy in construction and operation and demonstrably reduced potential for environmental impact. By taking a fresh look at PWR design, a consortium of Combustion Engineering and Stone & Webster in the US, and Rolls-Royce & Associates and the AEA in the UK have come up with a design which is intended to satisfy these requirements. This paper describes the detailed design of the Safe Integral Reactor (SIR). It highlights the special features which make this design innovative, yet based firmly in established technology, economically viable when compared to large "current designs" and strategically attractive to utilities because of its small size, ease of construction and short construction time.

The design features highlighted are:

- an integral pressure vessel containing core, steam generators, pressurizer and pumps;
- boron free operation;
- robustness against transients;
- no large LOCA;
- simple pressure suppression containment;

- no requirement for active decay heat removal systems.

The practical attractiveness to utilities is emphasised by presenting an outline of both single and twin reactor layouts which offer great flexibility in deployment.

1. Introduction

The historical trend in the nuclear industry has been towards the development of large nuclear power plants to meet the growth in base load electricity demand. Economies of scale and the use of established LWR technology dominated the rationale behind the systems developed to meet this need. Consequently, a 'modern' LWR is typically >1000 MW(e), takes greater than 10 years to bring to operation and is a very large single investment for an electrical utility. During the summer of 1988, discussions were held between Combustion Engineering in the USA, and Rolls-Royce & Associates and AEA Technology in the UK on the prospects for future reactor deployment; later, Stone & Webster Engineering Corporation also joined the project. The situation in the UK had just been radically altered by the Government's announcement of its intention to privatise the UK Electricity Supply Industry [1]. This opened the possibility for competition within the nuclear sector. This was then coupled with the US DoE's programme for a Simplified Passive Advanced Light Water Reactor (SPALWR) which offered the prospect of a joint US-UK project to design a reactor geared specifically to the perceived needs of electrical utilities for the next generation of plants. This gave an opportunity to take a fresh look at alternatives to the current design trends. The result was the Safe Integral Reactor (SIR). It is an innovative design in that it is an Integral Pressurized Water Reactor, but its deployment does not depend upon technical developments. This paper describes the basic design criteria against which the design was developed, and gives details of the NSSS, containment and plant layouts envisaged.

2. Basic Design Criteria

Three fundamental criteria guided the choice of design:

- it must have safety features expected of a next generation reactor;
- it must be economic;
- it must utilize established technology.

A number of features are generally accepted as being necessary to satisfy the expectations for the safety of next generation plant. They include:

- reduced reliance on operator action;
- increased robustness against operator mal-operation;
- utilization of passive safety features;
- long response times to upset conditions;
- simplicity in design and operation.

In the next sections we will show how the SIR design meets these fundamental expectations.

There is no doubt that in the present, and for the foreseeable future, any new reactor must present an attractive economic proposition to an operating utility. No matter how interesting the design may be from a scientific or technical point of view it must be saleable. The traditional thinking has led to the development of very large reactors which are said to be cheaper because of economies of scale. The basic SIR NSSS is rated at only 320 MW(e), in order to compete it must have design and constructability features different from the large plant. It is generally accepted that scaling down an existing design cannot lead to a cost competitive reactor. SIR is competitive because of the following features:

- short construction time; 30 months;
- modular construction;
- off-site fabrication of NSSS;
- reduced interest during construction;
- simplicity of engineered systems using passive features;
- simplicity of design utilizing fewer components and commodities per MW(e) than a similar size convention LWR;
- unique pressure suppression containment design;

The description of the design in the following sections will show how these advantages are fully utilized.

The final fundamental criterion is that the design utilizes existing technology. Closely allied with the economic constraints is the fact that resources are not available to develop a new thermal reactor design through a prototype and demonstration phase. Therefore all components, materials and systems must be tried and tested in other reactors, or in other applications. Some of the components whose use may be innovative are described in the following sections. Here we note that the principal NSSS components are based on existing technology, particularly the Reactor Pressure Vessel which, whilst large, is within current fabrication techniques, is transportable and can take advantage of all of the recent developments in NDE now available. Figure 1 shows a size comparison between the SIR vessel and other nuclear vessels. The fuel and control systems are standard to the Combustion Engineering System 80 design.

How all of these design targets are met is now described.

3. Technical Description

The design consists of an integrated nuclear steam supply system producing a nominal station output of 320 MW(e). As we shall describe, this output was chosen because of limitations on Reactor Pressure Vessel size and because such a size was determined to have a particular market niche. Large plant outputs can be achieved by using a number of these basic units driving one or more turbo generators. A detailed design for an integrated nuclear plant consisting of two SIR modules driving a single turbine of 640 MW(e) output has been described recently [2].

Vessel Size Comparison

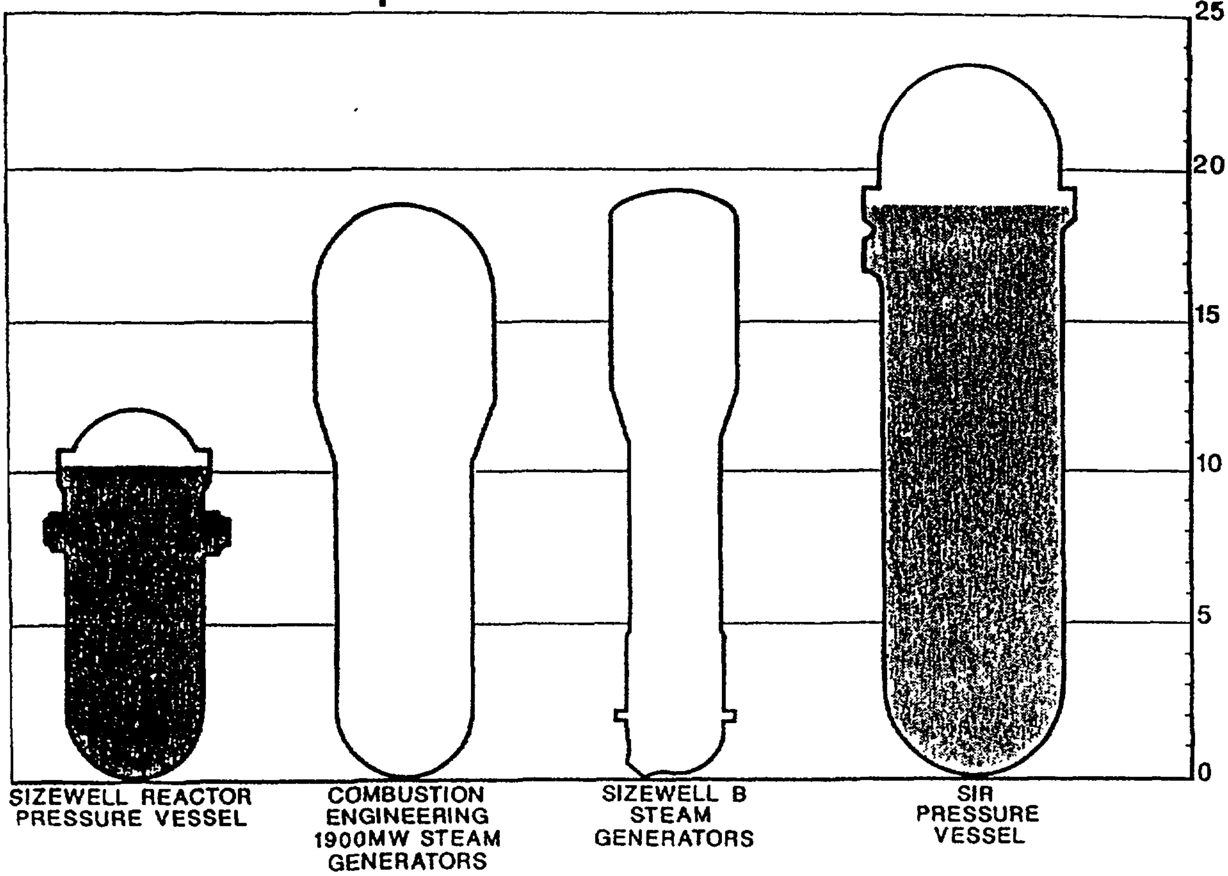


FIG. 1. Size comparison between the reactor pressure vessel and the components of 'standard' PWRs.

In this paper we concentrate on the single SIR layout. Although not discussed in this paper, the modular nature of the SIR provides an opportunity to claim economic advantages in using multiple reactor layouts [3]. The basic unit is competitive with large PWRs for the reasons outlined above, multiple units have even better economics.

4. The SIR Module

The SIR module consists of a single RPV and closure head which contains the reactor core, core support and other reactor internals, 12 once-through steam generator modules, 6 coolant pumps and an integral pressurizer. This layout is shown in Figure 2, where a number of other features are identified.

The reactor assembly is a completely self-contained reactor coolant system (RCS) within a single vessel. There are no external reactor coolant loop pipes and no surge line. The reactor coolant pumps are wet winding, glandless pumps inserted through and mounted to the wall of the reactor vessel. The

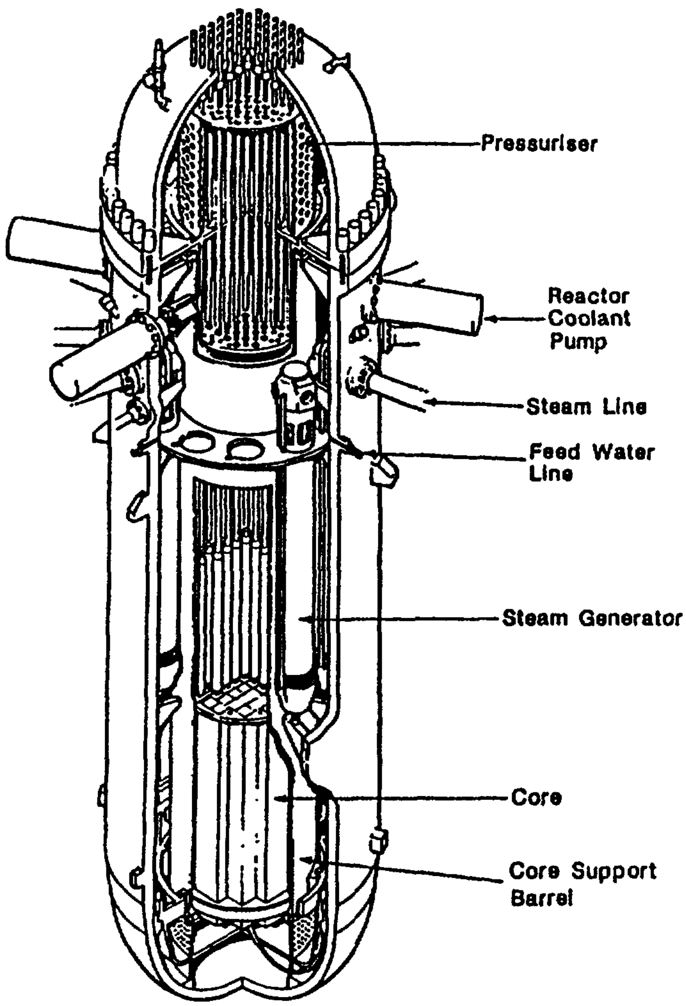


FIG. 2. Safe integral reactor: RPV and primary circuit.

pressurizer is integrally contained within the reactor vessel head. The only external primary piping connected to the reactor vessel is of small diameter (less than 7 cm or 2.8 inches) and includes 3 safety relief valves and 4 cooldown spray lines connected to the reactor head, and 2 safety injection lines connected to the side of the reactor vessel. On the secondary side, one steam and one feedwater line per steam generator are connected to the vessel. The control element drive mechanisms, 2 rector vessel level monitor probes and 6 fixed ex-core neutron flux monitor strings are inserted through nozzle locations on the head. In-core instrument and 2 movable source range ex-core neutron flux monitors are inserted through nozzles above the tops of the steam generators on the side of the reactor pressure vessel. The lowest penetration of the vessel is located approximately 29 feet (8.9m) above the top of the active core.

The SIR primary system or "primary circuit" is shown in the arrangement of Figure 3. Primary water flows up from the core and through the core support barrel or "riser". It then passes radially outward to the inlets of the reactor coolant pumps where it is pumped to the top of the steam generator modules,

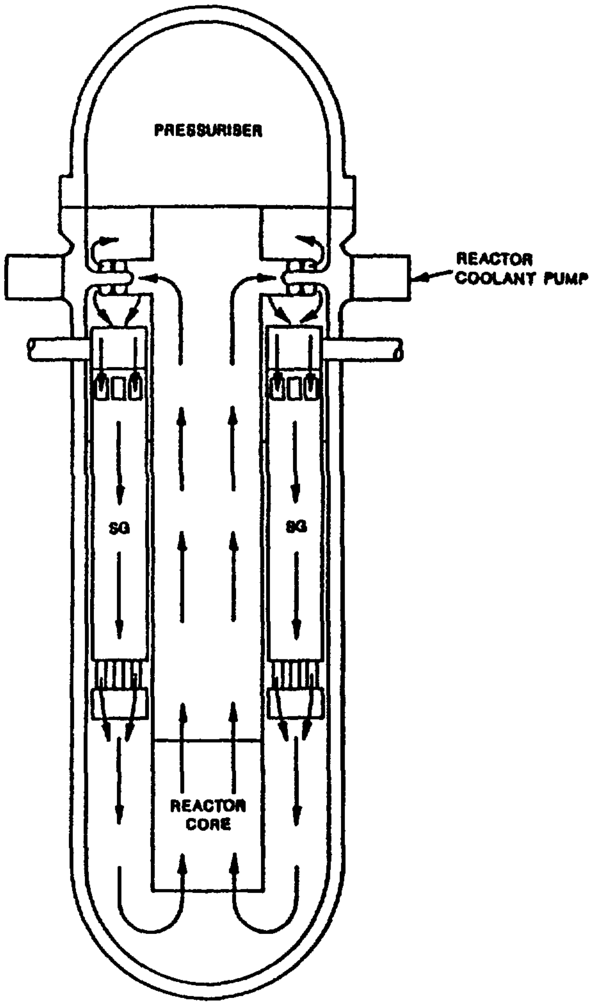


FIG. 3. Coolant flowpaths in the primary circuit.

passing down over the steam generator tubes and down into the lower plenum and core inlet. The pressurizer space above the reactor and steam generators is separated by a divider plate across which spray and surge flows are controlled by fluidic diode devices for passive control of pressure. Radial flowpaths from the riser section to the top of the steam generator region provide natural circulation. Figure 3 also shows that the RPV is separated from the core by approximately 1m of water. This arises from the need to provide the annulus for the steam generators but does mean that the neutron flux on the RPV in the beltline region is extremely low. In fact it is some 4 orders of magnitude lower than present day commercial PWR's and eliminates problems associated with irradiation damage to the vessel.

5. Reactor Core

The SIR core is rated at 1000 MW(th). The full SIR plant data are given in Table I. It is based on standard Combustion Engineering design practice and utilizes low enrichment, uranium

<u>Table I</u>

<u>Basic Parameters for the SIR System</u>

Plant data	
Design lifetime	60 years
Power output (design)	320 MWe
Reactor power	1000 MWth
Reactor type	Pressurised water reactor (PWR)
Plant style	Integral primary circuit
Primary circuit	
Design pressure	19·4 MPa (194 bar)
Operating pressure	15·5 MPa (155 bar)
Coolant flow	7500 kg/s (7·38 t/s)
Core inlet temperature	295°C (563°F)
Core outlet temperature	318°C (604°F)
Reactor core	
Moderator	Light water
Fuel	Low enriched UO_2
Fuel enrichment	3·3 – 4·0 per cent
Reactivity control	Fuel loading, burnable poison, control element assemblies, no soluble boron
Clad material	Zircaloy–4
Power density	55 kW/litre
Minimum DNBR	2·6
Refuel cycle	24 months
Steam generators (SGs)	
Number	12
Type	Modular once through
Steam temperature	298°C (568°F)
Steam pressure	5·5 MPa (55 bar)
Superheat	28°C (82·4°F)
Feedwater temperature	224°C (435°F)
Feedwater flow	516 kg/s (1138 lb/s)
Tube bundle length	8·5 m (27 ft 10 in)
Heat transfer area	11 140 m^2 (13 323 sq.yards)
Material	Inconel 690
Pressuriser	
Type	Integral with reactor vessel (in head)
Volume	80 m^3 (2825 ft^3)
Reactor coolant pumps	
Number	6
Type	Glandless, wet winding
Power (design)	1100 kW
Operating power	700 kW
Instrumentation and control	
Control complex	Based on CE nuplex 80–TM
Containment	
Type	Passive, pressure suppression
Safety systems	
Decay heat removal	Passive, through SGs using natural convection boiling condensing cycle
Emergency cooling injection	Passive, steam injectors powered by pressuriser steam
Construction schedule	
Site work to first concrete	6 months
First concrete to commercial operation	30 months
Order to commercial operation	54 months

dioxide fuel which is operated at low power density (54.6 kw/litre). This and other NSSS parameters are compared with other designs in Table II. The primary coolant flow is set to give a very conservative thermal margin, approximately 25% above that required for normal operation, with a minimum departure from nucleate boiling ratio (DNBR) of 2.6 at full design power. The requirement to use soluble boron for reactivity control has been completely eliminated by the use of moveable control element assemblies and burnable poisons. These are arranged to deal with reactivity changes arising from fuel depletion, fission product poisoning, power defect and the reactivity associated with cooldown and refuelling. The net result is a strong negative moderator reactivity feedback which provides a powerful passive response for a variety of transients and secondary side load changes.

Table II

Comparison of Selected Thermal Parameters Between Standard Plant and the SIR Design

Plant parameter	*Oconee (B&W)*	*Calvert Cliffs (CE)*	*H.B. Robinson (W)*	*SIR (CE/RR&A)*
Rated core power (MWth)	2568	2700	2300	1000
Number of core fuel assemblies	177	217	157	65
RCS fluid volume (m^3)	342	314	257	402
Pressuriser volume (m^3)	42·5	42·5	36·8	80
Effective PORV area (m^2)	$6{\cdot}05\times10^{-4}$	$1{\cdot}40\times10^{-3}$	$1{\cdot}97\times10^{-3}$	$8{\cdot}9\times10^{-3}$
Ratio of RCS volume to core power (m^3/MWth)	0·133	0·116	0·112	0·402
Ratio of pressuriser volume to core power (m^3/MWth)	0·017	0·016	0·016	0·080

6. Steam Generators

There are 12 identical steam generators in the SIR. They are of a once through design arranged in an annulus in the RPV above the core. Figure 2 shows their positions. This arrangement allows the reactor to be refuelled without the need to disturb the steam generators and steam generator replacement can be performed with the core installed. The steam generator tubes are straight, with flat tube sheet headers top and bottom. The steam penetrations are level with the top steam header; feed penetrations are a little lower, with internal pipes taking feedwater down to the bottom feed header. Secondary water circulates <u>inside</u> the tubes, so there are no crevices exposed to secondary chemicals. Furthermore, and in contrast to conventional designs, the tubes are in compression and hence any defects should not enlarge into cracks.

The steam generators are constructed from Inconel 690 to minimise corrosion and can be isolated individually, enabling the plant to be operated at high power even if a defective unit is isolated.

7. Other Primary Circuit Components

7.1 Pumps

Six reactor coolant pumps are mounted horizontally above the steam generators as shown in Figure 2. They are of a "wet winding" (ie. glandless) type with added inertia to increase pump rundown time. Each pump is installed as a complete unit and, with the primary water level lowered, can be removed with the RPV head in place and without disturbing the reactor core. Space is provided for this operation within the header gallery position of the reactor compartment. The pumps discharge into the steam generator annulus, but when natural circulation is being used to remove decay heat, a flow bypass route is provided by vortex diodes.

7.2 Pressurizer

In this design the free volume of the vessel head is used for the pressurizer function. It maintains the primary coolant pressure at 2250 psia to give adequate pressure to suppress pump cavitation and to avoid bulk boiling. Unlike standard designs, there are no external spray lines or surge lines. Spray and surge behaviour is induced entirely by primary circuit volume changes and is therefore entirely passive. The normal water level is such that there is $40m^3$ of space for both the heated water and the steam bubble. This is very much larger (in terms of specific volume/power ratio) than standard designs, as indicated by the figures in Table II.

8. Safety Features and Systems

In this section we describe why we believe this design offers significant improvements in safety margins and why it can truly be described as an "advanced" plant with passive safety features.

One of the principal advantages of the SIR design lies in the robustness of the core and primary circuit to fluctuations in both power and flow. Table II shows that for all of the important core and thermal performance parameters the design is superior to typical large PWRs. Thus, with a low power density core, the fuel (which is a standard large reactor design) can sustain up to 125% overpower before its operating margins would be exceeded. This is coupled with a very strong negative moderator temperature coefficient and means that for all identified transient events the reactor is essentially 'self regulating'. We believe there are no transient events which threaten the core and hence no diverse emergency shutdown system should be necessary.

All reactors require systems to remove decay heat and to provide an emergency source of coolant. SIR is no different in this respect but, because the demands on these systems are much reduced, their needs can be satisfied more simply. Figure 4 shows in outline the basic safety systems on the reactor.

8.1 Emergency Core Cooling System (ECCS)

Elimination of all large diameter primary circuit pipework outside the RPV has very significant safety ramifications. The largest penetration to the RPV is 70mm diameter (the control element drive mechanism nozzle). Thus there is no possibility of rapid emptying of the main vessel requiring massive and early injection of ECCS water. Furthermore, the lowest penetration of the vessel is 29 feet (8.9m) above the core. Hence there remains a large head of water to cover the core. Additionally, loss of steam through such a break is a far more efficient way of removing energy than by losing solid water. All of this leads to a much reduced requirement for emergency core cooling. There is no requirement for a low head high volume system and high pressure injection can be provided for by a completely passive 'steam injector' which uses primary side steam and obtains its water supply from the containment pressure suppression pools. These are above the vessel and so if the system is depressurized, coolant flow can be guaranteed by gravity drain. Therefore we have an Emergency Coolant Injection System which is simple, completely passive and of low capacity requirement.

8.2 Decay Heat Removal

Figure 4 also shows the principal connections for the decay heat removal circuits. Normally, when cooling down for maintenance and refuelling, the steam generators with turbine bypass are used and heat is rejected through the condensers. This can be achieved by natural circulation on the primary side but requires feed pumps and other equipment on the secondary side. If the temperature and steam pressure are too low for this mode of cooling, then heat is removed using water circulated and cooled by the component cooling water system. Should there be no a/c power available, heat is removed by a closed cycle, natural convection, boiling and condensing system which only requires battery power to operate the initiation valves. The heat sink for the system is sized to provide a minimum of 72 hours heat removal without operator intervention. Decay heat removal is also available without using the steam generators at all. This uses the safety relief valve lines and containment pressure suppression tanks.

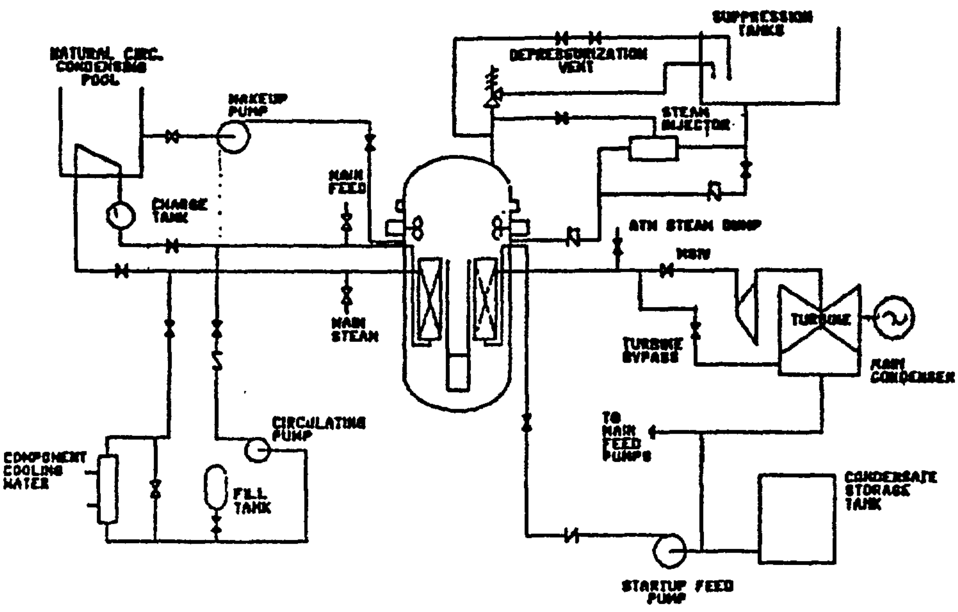


FIG. 4. Basic heat removal systems.

In summary, we can say that decay heat removal is provided for by active, active/passive and totally passive systems which are both redundant and diverse. In this, the decay removal systems show the features we would expect to have on a next generation plant.

9. Containment and its Safety Systems

The possibility that one of the large primary coolant pipes in a standard PWR design might fracture has determined their

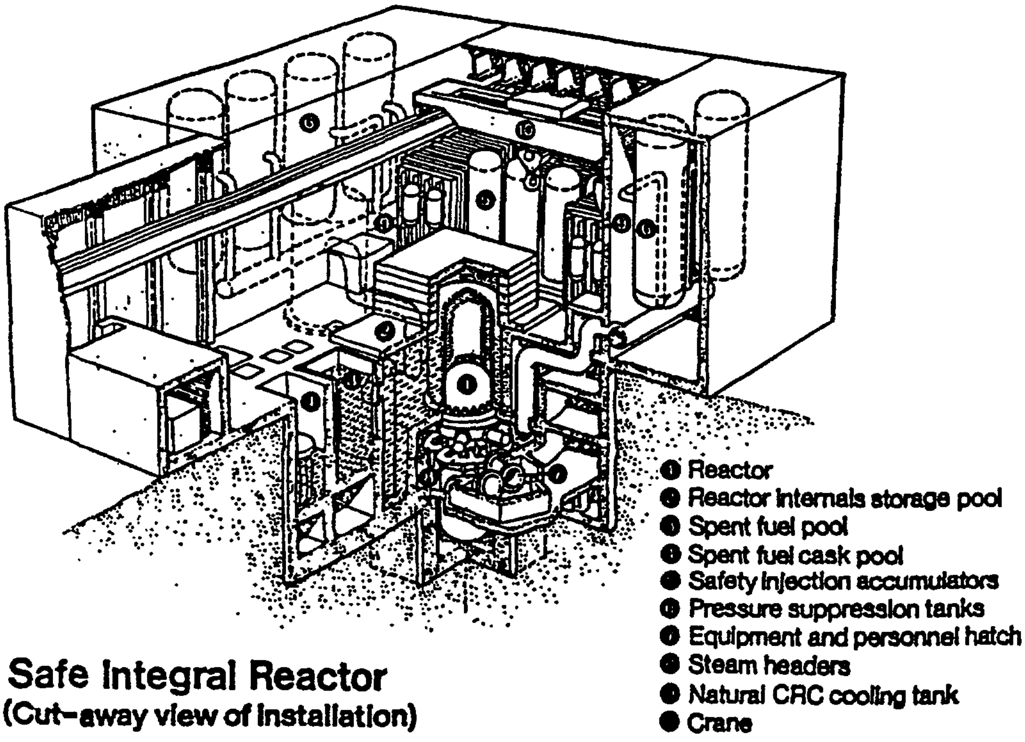


FIG. 5. 3D cut away drawing of the single STR containment arrangement.

requirements for containment. If an instantaneous fracture of the 30" dia. main coolant pipes was to occur, then the contents of the primary circuit would rapidly be blown down, and this calls for a large strong building to contain it. The so called 'large dry' containment is typical of standard PWR plant. For SIR, we have no equivalent to the large break and can take a different route to containment design. In many ways the integral nature of SIR gives it features more akin to the direct cycle Boiling Water Reactors in terms of its containment requirements. The maximum pipebreak is small, hence the rate of pressurization is small. Energy can be removed using a simple pressure suppression concept in which steam is condensed in a large pool of water. In order to take full advantage of the small size of SIR the pressure suppression system water pool is contained in steel tanks. There are 8 of them and their positions are shown in the 3D cut away drawing in Figure 5. This system has a number of advantages:

- using steel tanks and enhancing the surface to volume ratio by having 8 of them means that heat can be rejected via natural circulation. The principles of the flow paths are shown in Figure 5. This allows for 72 hours of heat removal with no need for operator intervention;
- the pressure suppression pools act as 'scrubbers' for any fission products which may be in the steam, thus providing an effective filter;

- steel tanks can be guaranteed to be leak tight much more easily than lined concrete structures with many penetrations;
- the steel tanks are sized for transportability, hence adding to the overall 'constructability' of the plant.

A summary of all the technical data for the plant is given in Table I.

10. Economic Attractiveness

One of our 3 fundamental criteria for this design is that it is competitive. In order to claim this we must demonstrate how we have beaten the economies of scale arguments which have become almost sacrosanct for the justification for large plant. The principal reasons why our cost estimates show SIR to be competitive with current large standard designs are:

10.1 Speed of construction

This reduces finance charges and the time before which a utility could expect a revenue stream. At 320 MW(e), the financial investment is less, and under US conditions, the impact on the rate base is much less. This is achieved by

- Modularization. All of the principal components are fabricated in factory conditions where full quality control and production line techniques can be used.
- No requirement for nuclear grade on-site welding of the primary circuit components and pipework.
- Constructability. The unitized NSSS, containment and the concrete cubicles of the main structures reduces the critical path schedule duration. The fuelling, auxiliary and reactor buildings utilize a common structure. Segregation of safety and non-safety related areas allows standard construction methods for the latter. There is 50% less Category 1 concrete and reinforcing steel as compared to a standard PWR of the same power rating.

10.2 Simplicity of safety systems

The safety system requirements are less, because of the intrinsic safety characteristics of the reactor. The following contribute to the cost savings:

- no requirement for low head/high volume ECCS;
- no requirement for boron chemistry control for reactivity;
- no requirement for safety grade A/C diesel supply;
- no requirement for large strong containment sized for the large LOCA;
- simplified control and operating systems;

All of these elements contribute to a design which beats the economies of scale, but fully utilizes passive safety features in a smaller design, less demanding civil engineering works for a smaller plant and greater availability through using low power density fuel with a 2 year refuelling cycle.

10.3 Reduced station doses

As well as economic and engineering safety advantages, the integral design, the simplicity of the systems and hence the reduced requirement for maintenance means that the anticipated station dose levels should be much lower than for standard designs. In particular, the ease of replacement of steam generators means that any major repairs can be performed away from the reactor. Simple tube plugging is performed entirely remotely. The lack of a chemical control system for boron not only reduced potential station dose, it reduced by up to 40% the relative production of intermediate level waste.

11. Flexibility

As described in this paper, 'SIR' is a 320 MW(e) plant. However, as we mentioned in the introduction, the SIR design lends itself well to modularization at the "quantum" of 320 MW(e). Reference [2] describes the layout of a two reactor single turbine configuration rated at 640 MW(e). Reference [2] gives the general arrangement drawing for this layout. The SIR design therefore offers the operating utility a degree of flexibility not available from larger plants, not only is the 'quantum' of financial investment smaller, the generating capacity requirements can be tuned at the level of increments of 320 MW(e).

12. Summary and Conclusions

In designing SIR, the 4 partners in the project met 3 principal goals:

- it must have safety features expected of a next generation plant;
- it must be economic;
- it must use existing technology.

We believe that we have met all 3 of these requirements. In particular, the safety features of the plant reflect the lessons learned in recent years from accidents and near accidents and from the intense technical and public debates which have followed. However, it would be very unwise to either oversell, or be complacent, about the safety features of any plant. Therefore, there is a continuing search for further safety margins and refinements.

We believe we have achieved a competitive design by the allowance for modern manufacturing techniques, design for speed of construction and the utilization of the simplifications available from a small plant with passive safety features. Multiple unit plants show significant economies of scale, but baselined to a single unit which is itself competitive when compared to present designs.

Finally, we note that the design relies entirely on components materials, control systems and fabrication techniques which are well established and proven. What is new is that they have been brought together in this way for the first time. There is no requirement for a prototype reactor, or for a long development programme. As we say in the title, SIR has been developed for the next generation.

REFERENCES

[1] "Privatising Electricity: The Government's Proposals for the Privatisation of the Electricity Supply Industry in England and Wales", Cm 322, HMSO, (February 1988)

[2] BRADBURY, R., LONGO, J., STRONG, R., HAYNS, M.R., "The Design Goals and Significant Features of the Safe Integral Reactor", (ANS annual meeting, Atlanta, Georgia, USA, June 4-8 1989), paper no 134, (June 1989)

[3] The SIR project, ATOM, 392, United Kingdom Atomic Energy Authority, London, (June 1989), 2-8

SAFETY AND SIMPLICITY IN A NEW ERA OF NUCLEAR PLANT DESIGN

H.J. BRUSCHI
Energy Systems Business Unit,
Westinghouse Electric Corporation,
Pittsburgh, Pennsylvania,
United States of America

ABSTRACT

Westinghouse is designing the AP600 (Advanced Passive 600 MWe) as part of a cooperative program by the United States Department of Energy (DOE) and the Electric Power Research Institute (EPRI) to develop innovative light water reactors. Emphasizing passive safety system in the design for future nuclear power plants improves safety, operability and economics which are paramount in obtaining greater acceptability with the public. In addition, modular construction techniques permit further improvements in construction, schedule and costs. This paper describes the impact of emphasis on passive safety systems, modularization and the resultant overall plant simplicity. Simplicity applied to construction methods has led to the use of transportable modules manufactured at a central, remote facility -- gaining higher quality from a permanent cadre of skilled labor. Use of transportable modules offers both quality and safety advantages in constructing this plant, not only in countries with advanced development, but also in areas of the world which have fewer skilled workers and many unskilled construction workers. The advanced digital instrumentation and control system and Advanced Control Room further simplify operation and allow more efficient operator action during both normal and abnormal operation.

---

1. A NEW ADVANCED LIGHT WATER REACTOR DESIGN BY 1995

The United States Department of Energy (DOE) has taken the lead in a joint effort with America's electric utilities, reactor manufacturers, and supporting industries to gain Nuclear Regulatory Commission design certification for an advanced light water reactor design by 1995. The Electric Power Research Institute (EPRI) has played a major role in this effort, working in two parallel areas -- evolutionary near-term advances in large plants of the 1000-megawatt class, and in more advanced, simplified passive plants in the 600-megawatt class. This paper will concentrate on the Westinghouse role in the latter effort, with emphasis on the impact that safety advances play on total plant design.

2. THE WESTINGHOUSE AP600

Safety is the primary goal in the Westinghouse response to the challenge put forth by DOE and EPRI. The logic behind this thrust is compelling: Without convincing safety characteristics, no new reactor design will gain public acceptance in America, and, therefore, no new nuclear plant is likely to gain NRC design certification and, ultimately, the financial support needed for construction. For the American public and Westinghouse alike, safety is the bottom line for nuclear power plants.

Conceptual design of the Westinghouse AP600 (Advanced Passive, 600 megawatt) is now complete. All of its basic design concepts are established, and all have been analyzed and tested. The design team has completed its plant arrangement drawings, and established a projected construction schedule and estimated costs. The Westinghouse Electric Corporation has committed resources toward having an AP600 plant built and in operation before the turn of the century.

3. AP600: A DESIGN BASED ON LONG EXPERIENCE

For all its innovation, the AP600's safety and performance are based on a highly conservative design philosophy. The plant is based on an optimized progression in the well-proven Westinghouse two-loop, 600-megawatt PWR technology. It retains the successful concepts and equipment that Westinghouse has refined in its more than 1000 reactor-years of experience and safety, and on the pressurized water reactor technology that is today the primary choice of nations and utilities around the world. The equipment includes styles of pumps, valves and heat exchangers that have been steadily improved and made more reliable over a quarter of a century.

4. SIMPLIFICATION FOR SAFETY SYSTEMS TO RESPOND TO DESIGN BASIS ACCIDENTS

AP600 also incorporates the same "defense in depth" design philosophy which has proven to be very successful in current operating reactor plants. This philosophy ensures that several redundant and diverse systems are available to keep a plant in a safe condition for a wide variety of transients which the plant may undergo. For the extremely low probability of occurrence design basis accident events (such as a loss of coolant accident), most commercial nuclear plants built to date have relied on active, redundant, mechanical safety systems to replace coolant in the reactor vessel and to remove decay heat. The AP600 design takes an innovative approach in performing the same two functions by relying on passive systems (Figure 1).

The AP600's safety injection system requires no safety grade pumps or diesels to perform its function. Instead, it supplies cooling water from large storage tanks located inside the containment vessel. Natural forces and pressurized gas drive the flow of this water when normal water level and pressure in the reactor system reach a pre-specified condition.

5. SIMPLIFICATION: PASSIVE COOLANT REPLENISHMENT AND REMOVAL OF DECAY HEAT

In the AP600 design, two tanks of borated water are located above the RCS loop piping, at full reactor coolant system pressure. If the water level in the pressurizer reaches a pre-set low level, the reactor trips automatically, discharge isolation valves open automatically, and the pull of gravity forces water into the core. For major transients, such as a large break in the main loop pipe lowering the system pressure below 700 psia, two gas pressurized accumulators supplement the flow. In addition, an in-containment water refueling storage tank provides a large long-term source of water sufficient to flood the entire lower portion of the containment.

After some 10 hours in this loss-of-coolant-accident scenario, long-term heat decay removal begins as the water storage tanks have emptied, completely flooding the lower containment and reactor vessel. Steam condensation on the inner surface of the containment shell constantly replenishes the boil-condensation cycle which transfers core decay heat into the containment plenum.

Water from this emergency core-cooling system can also be utilized to replace coolant in the reactor system should the normal makeup system be unavailable if small leaks occur during normal operation.

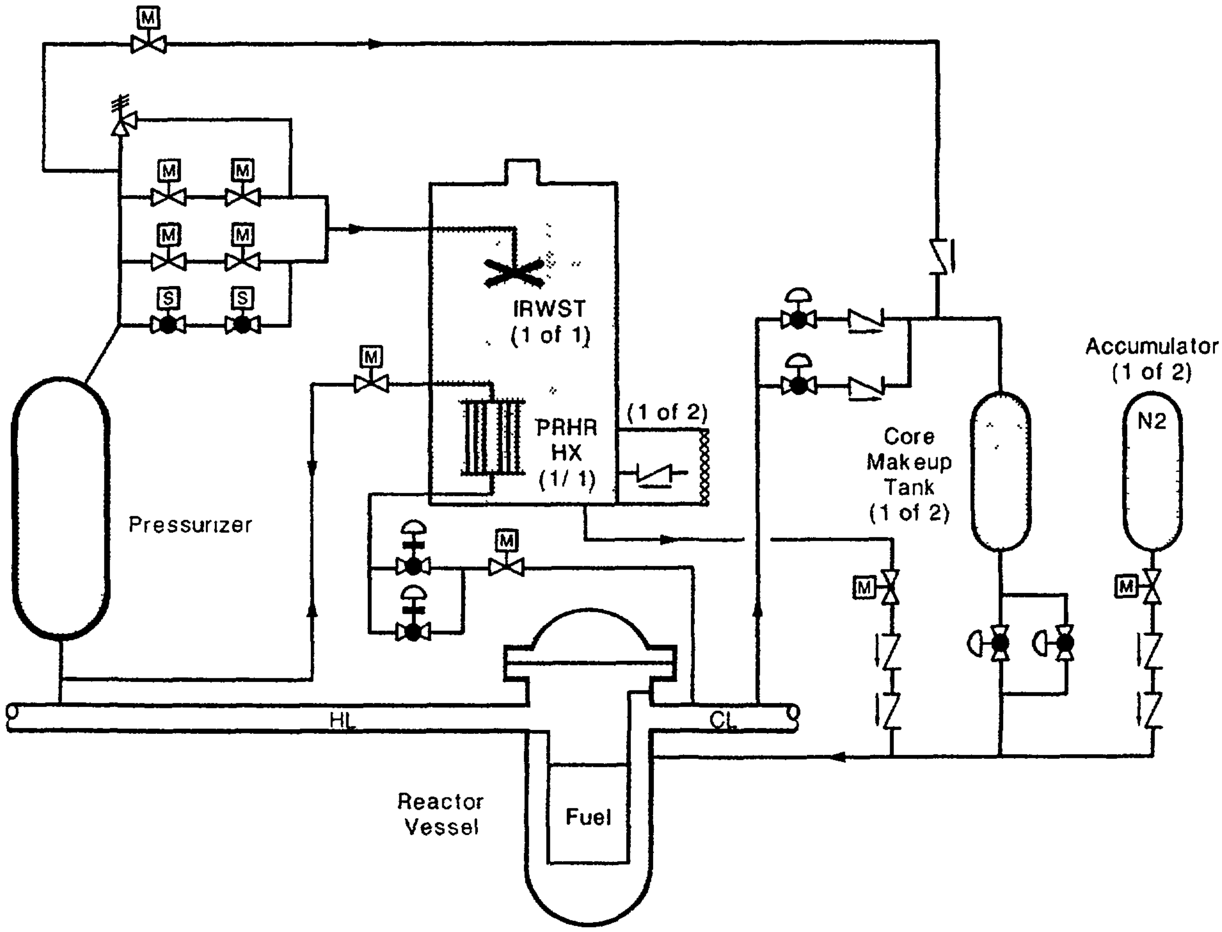


FIGURE 1: PASSIVE SAFETY INJECTION SYSTEM

6. SIMPLIFICATION: REMOVAL OF DECAY HEAT FROM THE CONTAINMENT

The AP600 design calls for a rugged steel containment, which is, in turn, surrounded by a non-contiguous concrete shield building, leaving a space for air to flow between the steel and the concrete. Heat inside the containment is ultimately transferred through the steel containment. Air flows over the outer steel surface by natural convection, thus removing the heat. As the vessel heats up, the more pronounced the cooling effect provided by the moving air (Figure 2). To supplement this natural air cooling system following a LOCA, the AP600 design incorporates water tanks above the steel containment to assist in cooling.

The release of this water is automatic. It flows at a controlled rate across the outer surface of the steel, cooling it by evaporation. The combination of evaporative and convective cooling is more than adequate to address the heat dissipation demands of the LOCA. Analysis has shown that after three days, convective air cooling alone will maintain internal containment temperatures within design limits indefinitely.

Whether a break is large or small, the reactor operator need take no action at any time for these safety systems to function. No AC power is required from an external source or from diesel generators. The restoration of reactor coolant and decay heat removal are automatic. They function under the reliable forces of gravity, convection, evaporation and condensation, instead of traditional pumps,valves, electricity and operator actions.

The safety of the AP600 design is enhanced to a significant degree by these passive reactor protection systems. Simplicity, in this design, is a major source of safety.

7. AP600: ADDED MARGINS IN PERFORMANCE OF THE NUCLEAR STEAM SUPPLY SYSTEM

Another example of the conservative nature of the AP600 design is its nuclear steam supply system which incorporates a low-power density core, offering more operating margin and an 18-month refueling cycle (Figure 3). The plant's availability factor is targeted to reach 90% and its capacity factor 85%. It will provide more than 700° F of fuel rod clad peak temperature margin for the design basis double-ended cold-leg pipe break -- a major contribution to safety (Table 1). The AP600's passive core cooling systems produce large safety margins, keeping the core covered following postulated breaks in pipes as large as eight inches in diameter.

8. AP600: ECONOMICAL AND COMPETITIVE

The AP600 design carries the theme of simplicity throughout the plant. When compared to similar facilities that use active safety systems, Westinghouse has eliminated 60% of the valves, 75 % of the pipe, and 80% of the control cables from the power block. Fewer components relate to lower costs and greater reliability (Figure 4).

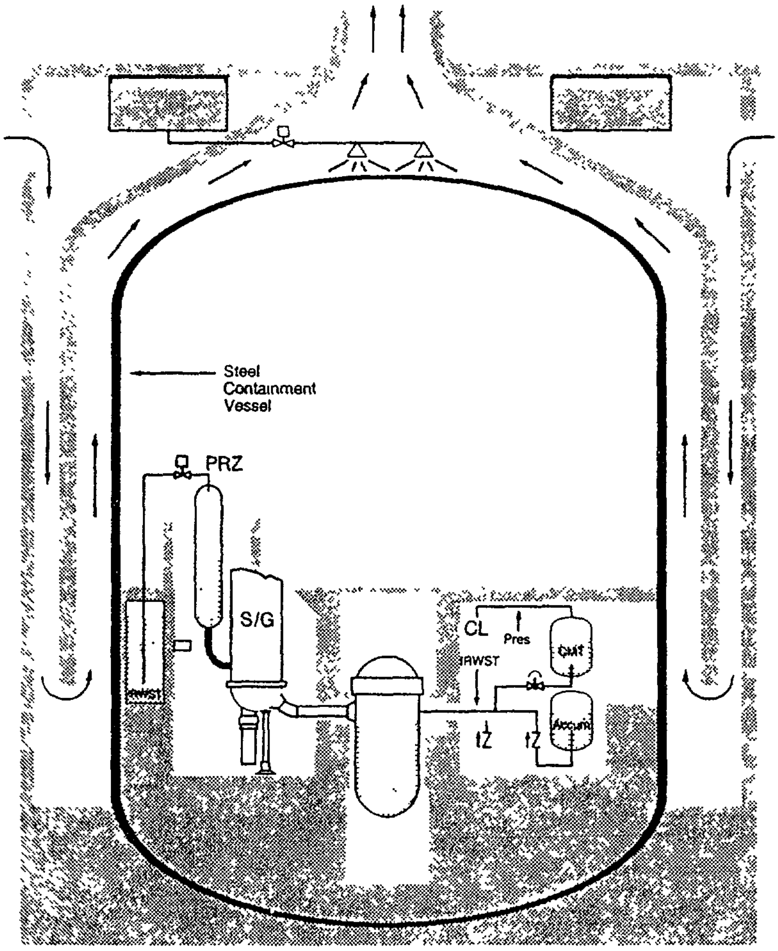


FIGURE 2: PASSIVE CONTAINMENT COOLING SYSTEM

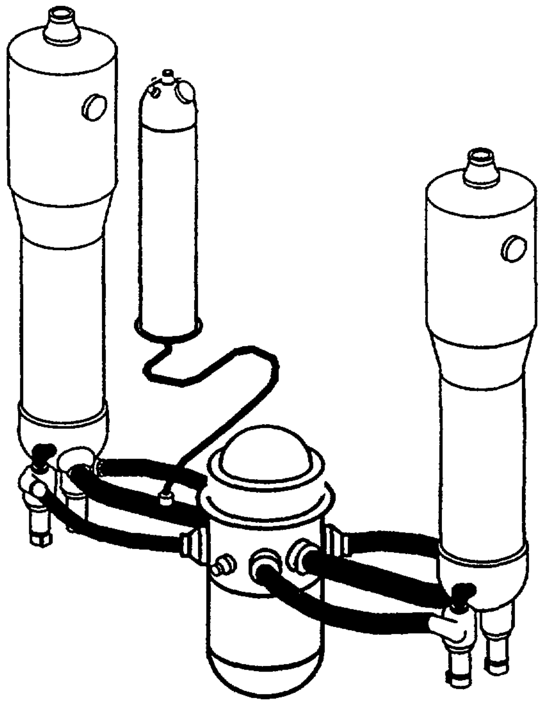


FIGURE 3: SIMPLIFIED REACTOR COOLANT SYSTEM

TABLE 1: AP600 PRELIMINARY SAFETY ANALYSIS

Event	Acceptance Criteria	Results
Loss of Forced Reactor Coolant Flow	No departure from nucleate boiling	Met
Loss of Normal Feedwater Flow	No safety valve lift	Met
Feedwater System Pipe Break	No safety valve lift	Met
Steam System Piping Failure	No departure from nucleate boiling	Met
Small Break LOCA	No core uncovery	Met
Large Break LOCA	Peak clad temp < 2200°F	Met, peak < 1500°F
Steam Generator Analysis	Peak pressure < 45 psi	Met, peak < 40 psi
Large LOCA	Pressure at 24 hr < 22 psi	Met, 24 hr < 10 psi
Anticipated Transient without Scram	RCS pressure < 3200 psi	Met, < 2900 psi
Loss of External Load	No safety valve lift	Met
Offsite Thyroid Dose Following LOCA Event	10 CFR 100 offsite dose limits	Met, < 200 rem

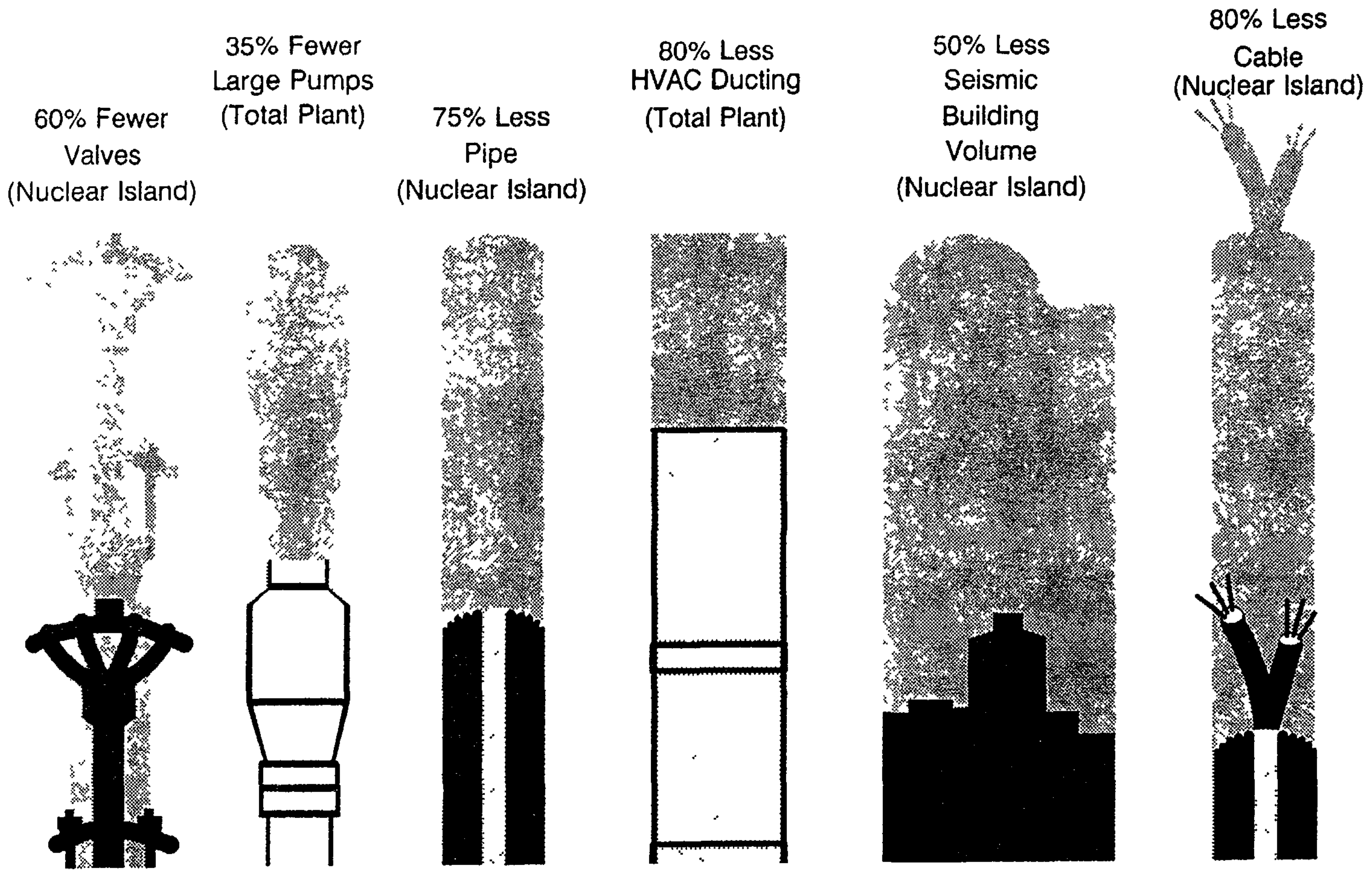


FIGURE 4: SIMPLIFIED PWR DESIGN

In addition, the AP600 design targets a much shorter construction period of 36 months. Shop and field modular designs and construction techniques are being incorporated for their lower costs and shorter construction time (Figure 5).

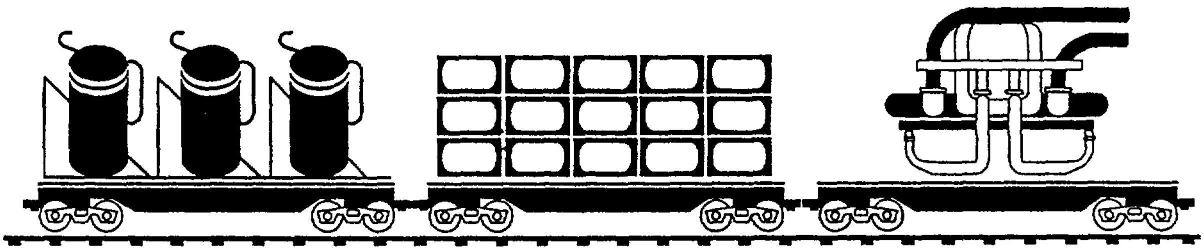


FIGURE 5: MODULARIZATION CONSTRUCTION TECHNIQUES

A key element in the plans for a short, effective construction cycle is a more predictable licensing process. All AP600 construction time estimates assume that greater than 90% of the plant and site specific engineering can be completed and the plant can be given regulatory approval for both construction and operation before the first concrete is poured. They also assume that once construction begins, inspections will be carried out to confirm that the plant is being constructed in accordance with the design certified by the NRC, but regulatory changes will end.

9. AP600: PUBLIC ACCEPTANCE AND LICENSABILITY

The emphasis of the AP600 design is on the passive safety systems. To a very great degree, this safety orientation is a primary reason to believe that the AP600 design will have a significant and favorable impact on public acceptance and licensability. A plant designed to use natural forces in its safety systems is desirable and understandable.

INHERENT SAFE HEAT REMOVAL IN ADVANCED MEDIUM-SIZED HIGH-TEMPERATURE REACTORS

K. KUGELER, P.-W. PHLIPPEN,
P. SCHMIDTLEIN, R. SWATOCH
Institute for Energy Technology,
University of Duisburg,
Duisburg, Federal Republic of Germany

Abstract

One of the main points for the inherent safety of a pebble bed high temperature reactor (HTR) is to guarantee the safe removal of the after-heat in case of a break-down of all active cooling systems like heat-exchangers or liner-cooling. This will be necessary because it is well known today that graphite pebble bed fuel elements stay intact, if the accident temperature is below 1600 °C. Therefore the heat must be taken out of the reactor system by passive, natural lawed heat-transfer mechanism so that the maximum fuel temperature stays below the specified limit. Today medium-sized HTRs with a power of 750 MW_{th} and more (THTR- 300, HTR 500) reach temperatures of more than 2400 °C in small parts of the core in such hypothetical accidents. A possible way to realize the inherent safe heat removal in advanced medium- sized HTRs is to change the form of the core. Instead of employing the standard cylindrical geometry a plate shaped core should be preferred, described by the proportion of width to depth of approx. 6 : 1, causing short distances for heat transfer to the side reflectors within the core and due to the reduction of the mean core power density less than 3 MW/m^3. A further improvement of the passive heat removal in case of a failure of the liner-cooling can be achieved by adding cast iron and/or metal granulated material to the concrete of the reactor vessel increasing the thermal conductivity. In case of a total failure of the liner-cooling, heat removal within the prestressed concrete vessel is also possible using installed vertical ducts which make it possible that fresh air runs through the ducts by natural convection cooling the reactor vessel. Even the total removal of the after-heat is possible by suitable arrangement, number and shape of such ducts.

1. INTRODUCTION

The discussion about the Safety of nuclear power plants is often limited to the demand of a safe enclosure of the radioactive fission products. You can observe, that safety depending on active mechanisms will no longer be accepted by a lot of people. Presently used nuclear power plants have a probabilistical based possibility of catastrophical accidents. With regard to the utilization of nuclear power in the future, it should be a demand to base the safety of nuclear power plants on passively working mechanisms. The modified safety requirements may be based on the following clains:

1. The reactor must shut down itself from all operating and accident situations by physical principles. Inadmissible increases of power must be excluded by natural laws.

2. The integrity of the fission product barriers must be guaranteed in all accident conditions, so that the release of high amounts of fission products will be inherently excluded.

3. The after-heat must be removed from the reactor core at a temperature level which ensures the retention of fission products in the fuel element.

4. The heat emission, taking up the after-heat from the reactor core, must be based on natural-lawed phenomena, so that there is no requirement of external acts or energies.

Carrying out these inherency principles, a safe enclosure of the radioactivity in the nuclear power plant is guaranteed and, based on physical laws, a nuclear technology without the possibility of catastrophic accidents, caused by internal or external events, seems to be realisable. The following will show, that a modern designed high temperature gas cooled reactor offers a technical solution, which fulfills the safety requirements and which is already available.

2. RETENTION OF FISSION PRODUCTS

Like all constructed thermal reactors, the high temperature reactor has a strong negative temperature coefficient of reactivity, so that the first mentioned inherency principle is met. The other inherency principles will also be kept by the HTGR by an effective protection against influences from outside and by the realisation of a passive after-heat removal (figure 1). Whereas the protection against influences from outside may be realised by constructional means, the after-heat removal must be guaranteed at an allowable temperature level by the nuclear and heat engineering design. In this context, the fuel element is the most important barrier against a release of fission products.

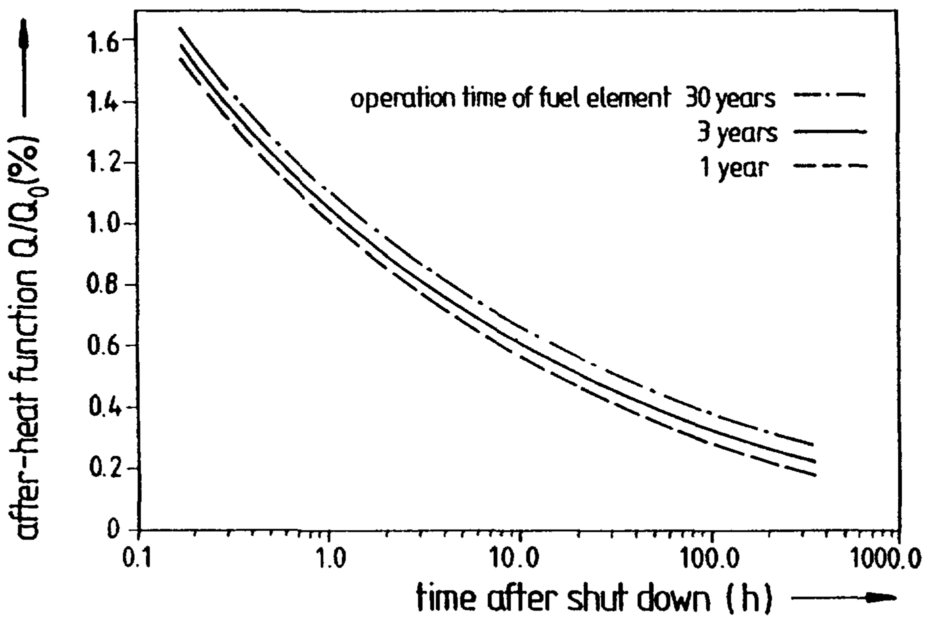


Fig. 1: After-heat Production

The core of the pebble bed reactor consists of a charge of spherical fuel elements of 6 cm diameter. Each of them contains coated particles with fissionable material dispersed into the matrix. From annealing experiments on pebble bed fuel elements which contain the fuel in TRISO-coated particles, it is very well known today that the pebble bed fuel elements stay intact, if the accident temperature is below 1 600 °C [1,2].

The evaluation of long termed radiological consequences of accidents will often be carried out using the isotop Caesium 137 as a tracer because of its long half-life period. Figure 2 shows the experimental results for this important fission product. By use of TRISO-particles only 10^{-4} of the Cs-137-content of the fuel element is released, if the temperature will be limited to 1 600 °C and the annealing time will be 400 h. At temperatures of 2 000 °C for instance, more than 10^{-1} of the fission product Cs-137 would be released. Today similar results are available for other important fission products like Sr-90 and Kr-85. Therefore, related to the state of coated particle technology and according to the experimental facts, an upper limit of 1 600 °C of fuel temperature should not be exceeded under all accident conditions. In this case there will be no considerable fission product releases and for that reason also no catastrophic consequences after nuclear accidents on the environment. Each core design, which fulfills these requirements meets the inherency principles and can be called inherent safe.

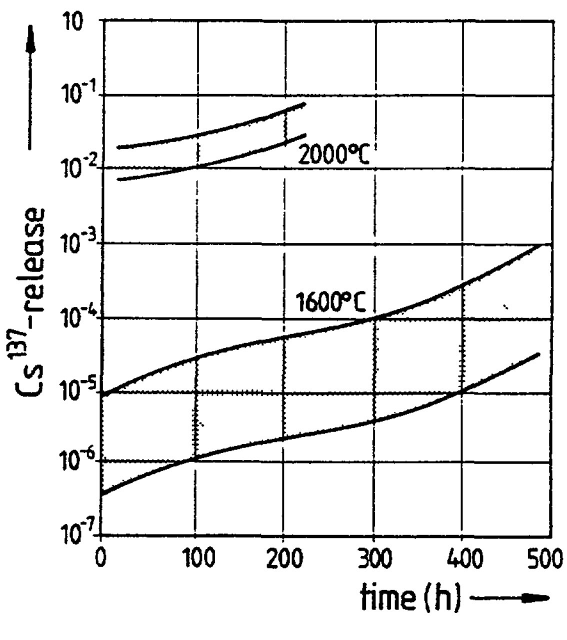
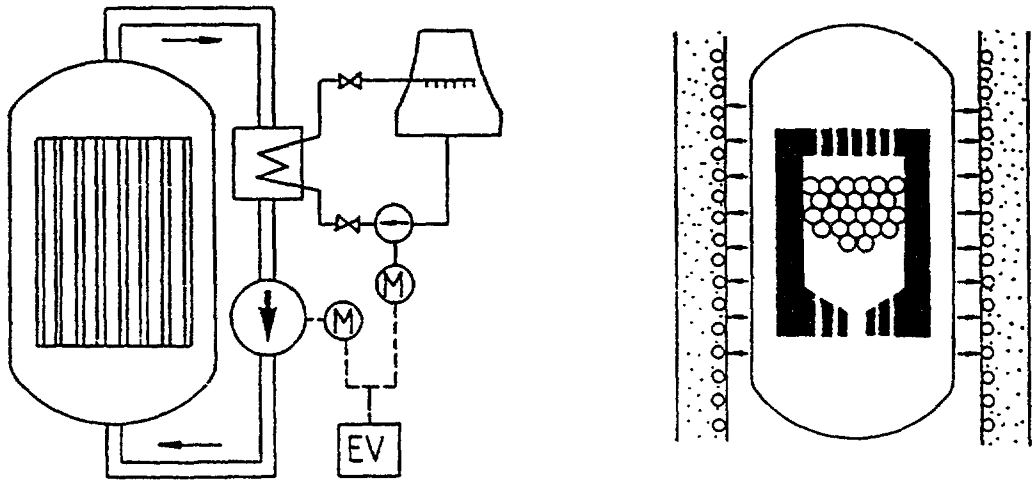


Fig. 2: Release of Caesium 137 from TRISO-Particles dependent on time and annealing temperature

3. REMOVAL OF AFTER-HEAT BY MACHINES OR BY INHERENT MEANS

Today the removal of the after-heat of nuclear reactors is usually carried out by heat-exchanger-loops, which are connected to active cooling chains (figure 3 a). These systems contain a great number of components like plumbings, heat- exchangers, pumps, cooling devices, valves, energy providing devices as well as measuring and controlling systems. All these components show endable sizes for the failure rates, so that this whole system of after-heat-removal has an endable size for the nonavailability in case of demand. The use of an HTGR-reactor opens a completely different way for the solution of this problem (figure 3 b).



a) heat removal by loops with machines   b) heat removal by heat conduction and radiation

Fig. 3: After-heat removal by engineered and inherent principles

An adequate design of the reactor core gives the possibility to remove the after-heat using inherent transport mechanisms like heat-conduction and heat-radiation in case of hypothetical loss of coolant accidents in the primary system as well as of the breakdown of all active cooling systems. By the mentioned effects, the after-heat is transported out of the core area through the side reflector structures to the outside of the reactor pressure vessel and from there to a very simple outer cooling system without the use of machines (figure 4). If this proper active part of the cooling chain

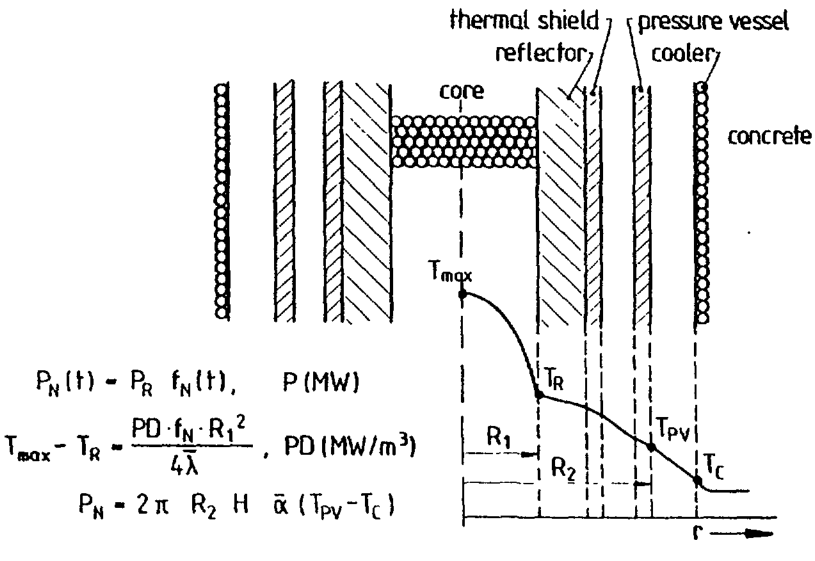


Fig. 4: Heat removal by inherent principles

fails too, the outer concrete structures of the reactor cell take up the after-heat. In this case the whole heat transporting system is absolutely passive and shows according to this fact no nonavailability.

This consideration of the reactor pressure vessel made of steel is similary valid also for prestressed pressure vessels made of concrete with inner insulation. More effective in the view of the removal of heat are prestressed vessels made from cast steel without inner insulation (figure 5).

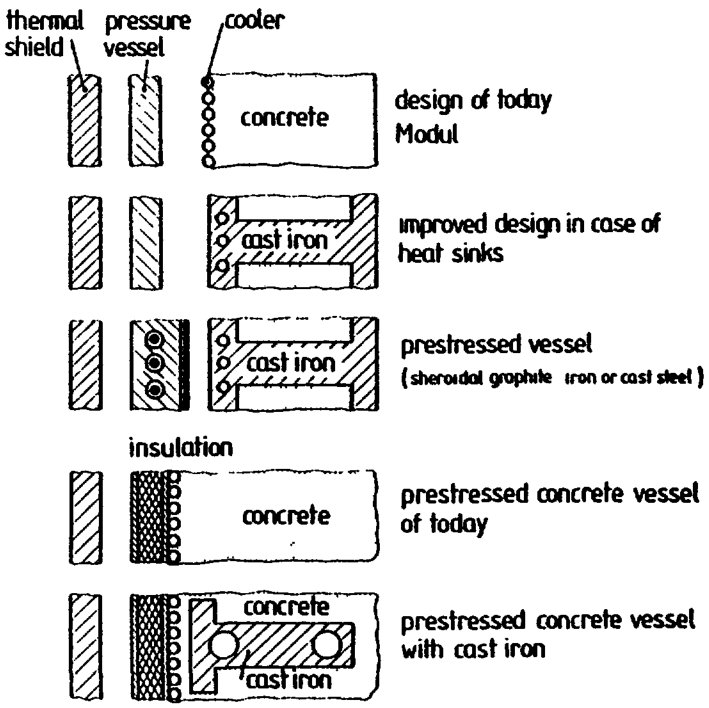


Fig. 5: Concepts of external heat sinks

4. SHAPE OF THE CORE IN VIEW OF PASSIVE AFTER-HEAT REMOVAL

If we postulated a stop of all active after-heat removal systems combined with a depressurization, medium sized HTGRs, which are built or planed until now, would reach temperatures much higher than 1 600 °C (figure 6). In this accident case, the german pototype plant THTR-300 at Schmehausen (with a thermal power of 750 MW) would generate temperatures of more than 2 300 °C in a small part of the core, and more than half of the core would pass over 1 600 °C for a long time. The planned HTR-500 reactor plant (with a thermal power of 1 400 MW) shows a similar behaviour in that case of accident.

Taking into account some special considerations, for example that the shutdown and trimming has to be done from the boundary of the reflector and if the core pressure drop has been restricted to 0,8 bar (in order to use radial blowers with one stage) it has been shown, that the thermal power of a cylindrical pebble bed core is limited to 230 MW, if you intend to guarantee an inherent stabilization of the maximum fuel temperature below 1 600 °C [3].

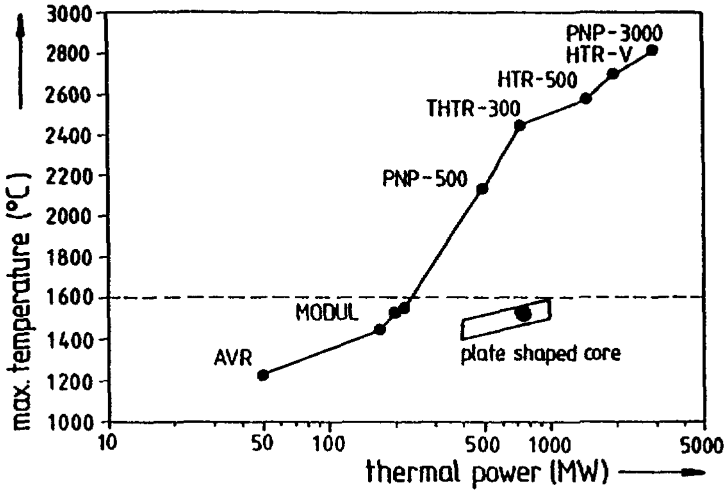


Fig. 6: Maximum fuel temperature in case of loss of coolant accident for different HTR-plants

The choice of another core shape seems to be a possible way to realize HTGR plants with medium power in a safe way without leaving the requirements mentioned above. Since the beginning of the utilization of nuclear energy, the geometry of the reactor core has been cylindrical. This is mainly stipulated by the choice of a cylindrical reactor pressure vessel. Some modifications of the cylindrical shaape are also existent in the case of water-cooled reactors, stipulated by the form of its fuel elements. The AVR reactor is equipped with graphite noses, which extend into the core to lead the control rods without forces by the pebble bed. Neutron physical considerations show the sphere as the optimal form for a core and the cubic cylinder with H/D app. 1 as the second-best and technically realisable geometry. Refering to the point of the passive after-heat removal for larger cores, other core geometries than the cylindrical may be more profitable.

In order to overcome the power restriction, one can choose a plate shaped core geometry [4]. It allows a separation of the dimension, which fixes the total power (the long side of the plate) and the safety and neutron physical behaviour esp. trimming and shut down (the short side of the plate). Therefore, one can realize any power level and at the same time keep the established safety requirements. The only limitation is the realisable size of the pressure vessel to enclose the reactor core and the reflectors.

5. 750 MW HIGH-TEMPERATURE REACTOR WITH A PLATE SHAPED CORE

Figure 7 shows a horizontal and a vertical cut of a plate shaped reactor core, located in a modified prestressed concrete reactor pressure vessel. The power density is chosen to 2,64 MW/m^3 and the plate thickness to 2,25 m by means of wich the maximum accident temperature remains below 1 550 °C. Fixing the core height with 9,5 m the established construction requirements are fulfilled. With regard to the dimensions of the prestressed concrete reactor vessel of the THTR-300 at Schmehausen/FRG the length of the core may be chosen to 13,3 m which yields a total power rating of 750 MW (table 1).

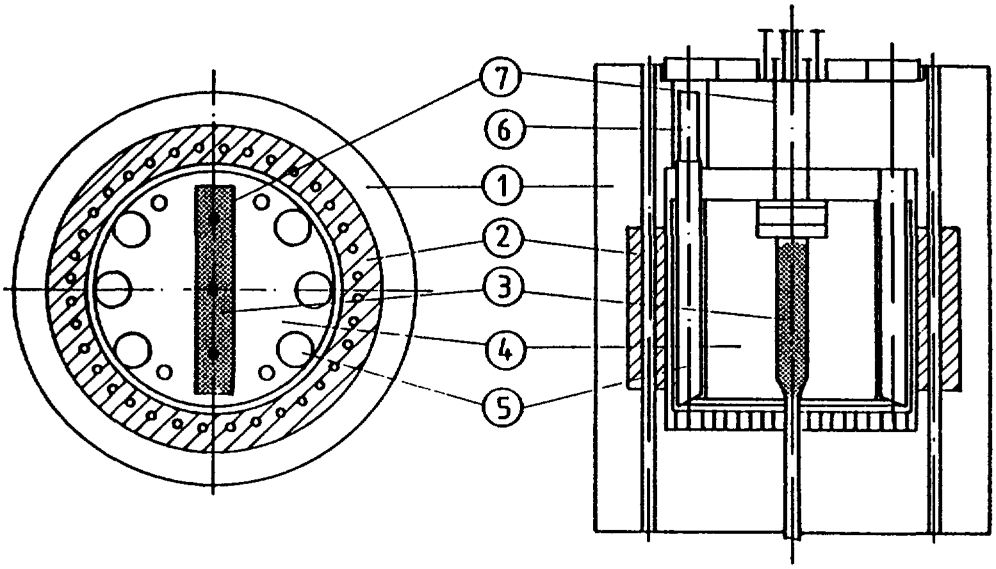


Fig. 7: Core design for a 750 MW_{th} inherent safe core: 1. modified prestressed concrete vessel, 2. cast iron structures with air passage ways for heat storage and convective heat removal, 3. core (plate shaped), 4. graphite reflector, 5. steam generator, 6. helium circulator, 7. control rods

Table 1: Data of an inherent safe HTR with medium power

Parameter	Data
thermal power:	750 MW
mean core power density:	2,64 MW/m^3
height of core:	9,5 m
length of core:	13,3 m
width of core:	2,25 m
inner diameter of reactor vessel:	16 m
max. fuel temperature: in hypothetical accidents:	1 530 °C

With respect to the inner vessel diameter of 16 m, there is enough space to realise a reflector of 1 m thickness surrounding the core. Regarding a maximum spread of 2.25 m, the top reflector structure may be constructed self-supporting, so that there will be no need of any steel-structures near to the core.

This arrangement allows the accommodation of all control and shut down elements of the first and of the second system in the graphite reflector. The discharge of the pebbles is guaranteed by several outlets at the bottom. The whole outer area of the reactor within the thermal shield is filled by graphite blocks. Due to the location of the plate into a cylindrical thermal shield, there remains enough space to arrange six steam generators and four active after heat removal systems, which are designed for working pressure, in the two circle sectors besides the core. By these circumstances a very low non-availability of the active after-heat removal is guaranteed without the necessity of qualifying the production loops especially for this task.

In case of depressurisation and stopping of all circulators, the after-heat removal is carried out by heat conduction through the graphite structures and from the outer wall of the core-container to the redundantly designed liner cooling-system by radiation, as shown in figure 4. This way of heat removal is very efficient because of the use of materials with excellent thermodynamical properties. For example, figure 8 shows the very well heat conductivity of a single graphite pebble and of a pebble bed.

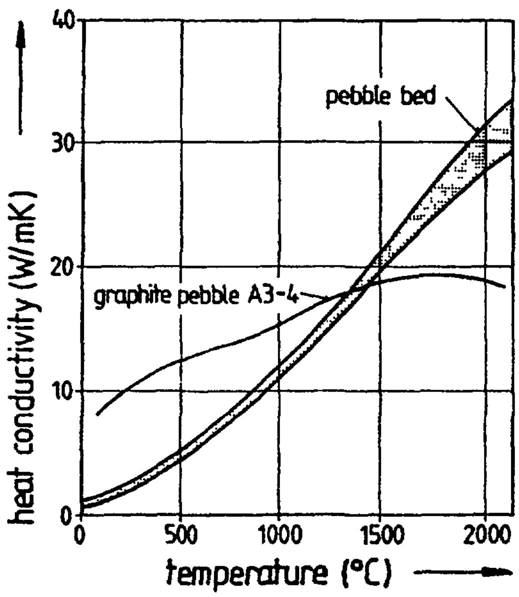


Fig. 8: Heat conductivity of a single graphite pebble and of a pebble bed

At the worst none of the active cooling-systems works. Now the heat must be taken by the reactor's pressure vessel itself. To avoid inadmissible high temperatures in the concrete structures, the wall behind the liner is built by a cast iron structure over the highness level of the core. This structure contains a lot of vertical cooling channels with openings at the top and at the bottom of the concrete vessel (figure 7). By means of this structure the after-heat is removed from the reactor core by storage of heat and finally by natural convection of air through the channels forced by stack draft.

The results of extensive analyses for loss of coolant-accidents with plate shaped cores are shown in the next three figures. Figure 9 and 10 show the maximum fuel temperature in the core in dependence of time and different places. Figure 11 shows the relative volumetric temperature distribution in the core. The fuel elements reaches temperatures above 1 400 °C only in a small part of the volume of a inherent safe plate shaped HTGR core of 750 MW thermal power. Therefore, we can expect a very low release of fission products during the stated hypothetical accident.

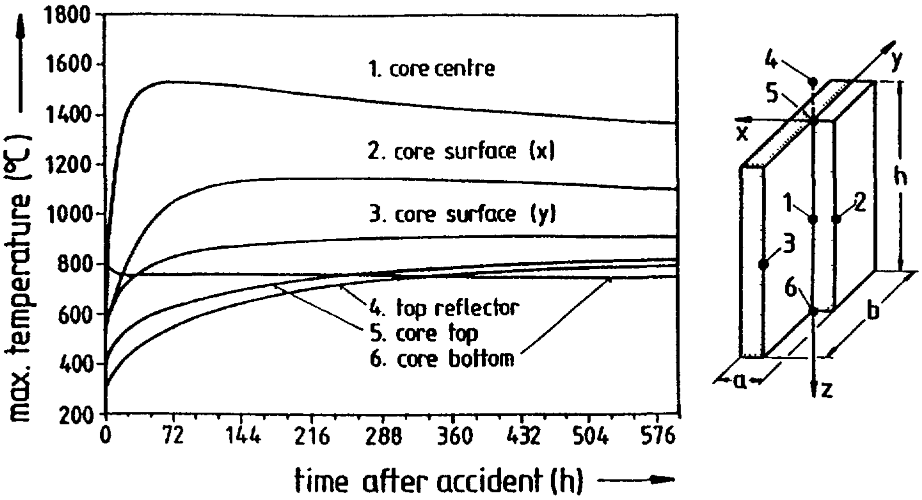


Fig. 9: Maximum fuel temperature in hypothetical accidents

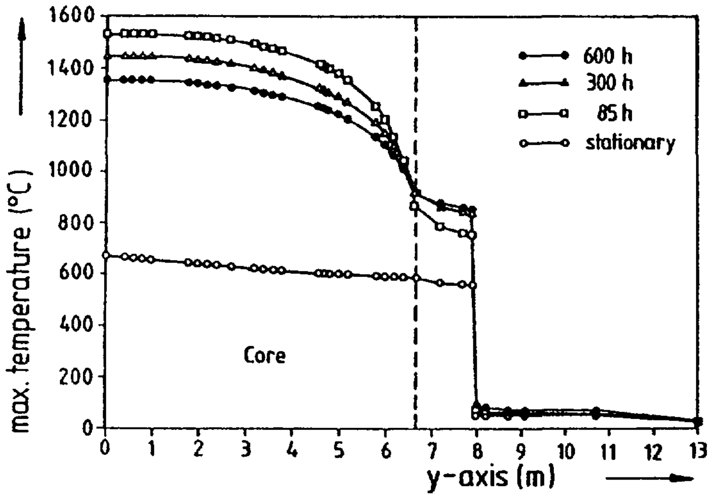


Fig. 10: Maximum fuel temperature in hypothetical accidents

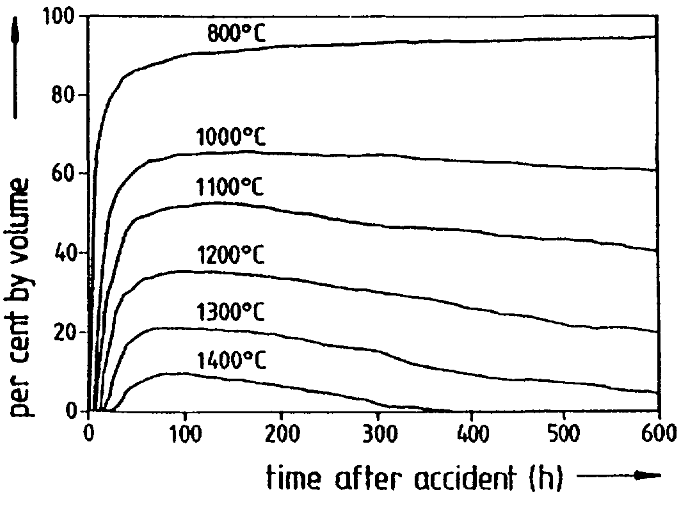


Fig. 11: Relative volumetric temperature distribution in hypothetical accidents

6. CONCLUSION

The maximum fuel temperatures of HTR can be limited to admissible values, even at a stop of active after-heat removal systems, by the choice of adequate thermodynamical and constructional data. Therefore, only a small fraction of the fission products may escape from the coated particles. Choosing a plate shaped core geometry, the reactor power may be fixed independent from those data which determine the accident behaviour. In this way a further development is achieved, because the safety principles, which are restricted to small reactor powers until now, are also valid for medium and high reactor power levels. Using the well developed prestressed concrete pressure vessel, the required reactor cavern is available and because of its burst protection the failure scenario of a massive ingress of air into the core is going to be meaningless.

In addition to the multiple build and long- term tested prestressed concrete reactor vessels, prestressed vessels of spheroidal graphite iron or cast steeel will also cover the requirements. Hence, the presented solution shows a possible way to realize a reactor technology without the possibility of catastrophic accidents.

REFERENCES

/1/ D. T. Goodin:
A Single Model for the Performance of HEU/LEU Fissile and ThO_2 Fertile Fuel under Hpyothetical Accident Conditions,
GA-A16291, General Atomic 1981

/2/ W. Schenk, et al:
Spaltproduktfreisetzungsverlauf von Kugelbrennelementen bei Störfalltemperaturen, KFA Jülich, JÜL-2091, Oktober 1986

/3/ U. Fricke:
Untersuchungen zur Leistungssteigerung von inhärent sicheren Hochtemperaturreaktoren durch Optimierung der Coreauslegung,
Dissertation Universität -GH- Duisburg 1987

/4/ K. Kugeler et al:
Hochtemperatur-Kernreaktor, Patentschrift DE-P 35 19 935.
Core für einen Hochtemperatur-Kernreaktor, Deutsche Patentanmeldung DE P 35 19 934

LOBI-MOD2 RESULTS RELEVANT TO PASSIVE SAFETY FEATURES OF PROSPECTED PWRs

C. ADDABBO, A. ANNUNZIATO, G. LEVA, R. WAMPACH
Safety Technology Institute,
Commission of the European Communities,
Joint Research Centre,
Ispra Establishment,
Ispra

Abstract

Salient results from LOBI-MOD2 tests emphasizing phenomenologies relevant to passive safety features of prospected power reactors are outlined. Specific reference is made to the mitigation of postulated accident consequences using deliberate primary coolant system depressurization and passive safety injection from the accumulator injection system. Although test conditions are strictly pertinent to pressurized water reactors of current design, the underlying phenomenologies are nevertheless of general interest also for next generation reactor concepts.

1. INTRODUCTION

The conceptual development of pressurized water reactors (PWRs) especially in the small and medium-size power range, relies mainly on passive safety features to guarantee adequate safety margins in both loss-of-coolant accidents (LOCA) and Special Transients conditions. Specifically, emergency-core-cooling systems (ECCS) are being designed to use gravity or gas driven injection. Also, provisions are made for eventual automatic depressurization of the primary system to enhance injection rates whenever the primary system stagnates at high pressure. Within this context experiments have been conducted in the LOBI-MOD2 test facility to assess the governing phenomenologies of such safety concepts for a range of highly degraded accident conditions.

The LOBI-MOD2 test facility is a high pressure integral system test facility designed, constructed and operated in the Ispra Establishment of the Commission of the European Communities Joint Research Centre. It represents the essential features of a 1300 MWe PWR of current design. The main objectives of the experimental programme are:

- to investigate overall system thermal-hydraulic response for a range of postulated PWR accident conditions
  - . Small Break LOCAs
  - . Special Transients
  - . Recovery Procedures
  - . Accident Management Strategies

- to provide experimental data for the assessment of the predictive capability of system codes used in PWR safety analysis.

The experimental results described in this paper refer to the mitigation of accident consequences in the event of loss of safety injection from engineered safety systems and unavailability of secondary system heat sink. Under these conditions the adopted safety procedures consisted in automatic primary system depressurization and passive safety injection from the accumulator injection system. Specific reference is made to a small break LOCA and to a Special Transient originated by the loss of main feedwater. Although test conditions are pertinent to PWR of current design, they are nevertheless also relevant to advanced reactor concepts.

Clearly, due to simulation and operational constraints inherent in the acaled test facility, the reported results cannot be directly extrapolated to a full-size plant; they provide, however, a reference data-base for the understanding of the governing phenomena and for the verification of the predictive capability of analytical tools used in reactor safety analysis.

2. THE LOBI-MOD2 EXPERIMENTAL PROGRAMME

The LOBI-MOD2 experimental programme is the result of an international cooperation in the field of water reactor safety research. It comprises two test matrices defined A and B.

- The test matrix A is being performed in the framework of an R&D contract between the Commission of the European Communities and the Bundesminister für Forschung und Technologie of the Federal Republic of Germany.

- The test matrix B is instead being performed in the context of the Commission of the European Communities Reactor Safety Research Programme with indipendent contributions from several EC member countries.

Originally, the research programme was mainly conceived for the parametric investigation of large break LOCAs in PWRs with emphasis on the performance of the ECCS safety systems. Large break LOCA tests covering the large to intermediate break size spectrum and small break LOCA scoping tests were performed from December 1979 until June 1982 with the test facility in the MOD1 configuration. As the perception of priorities in water reactor safety research changed early in 1980, the programme was then redirected towards the investigation of small break LOCA and Special Transient phenomenologies with inclusion of recovery procedures and accident management strategies. To comply with the new simulation requirements the test facility was modified and upgraded in the MOD2 configuration which became operational in April 1984.

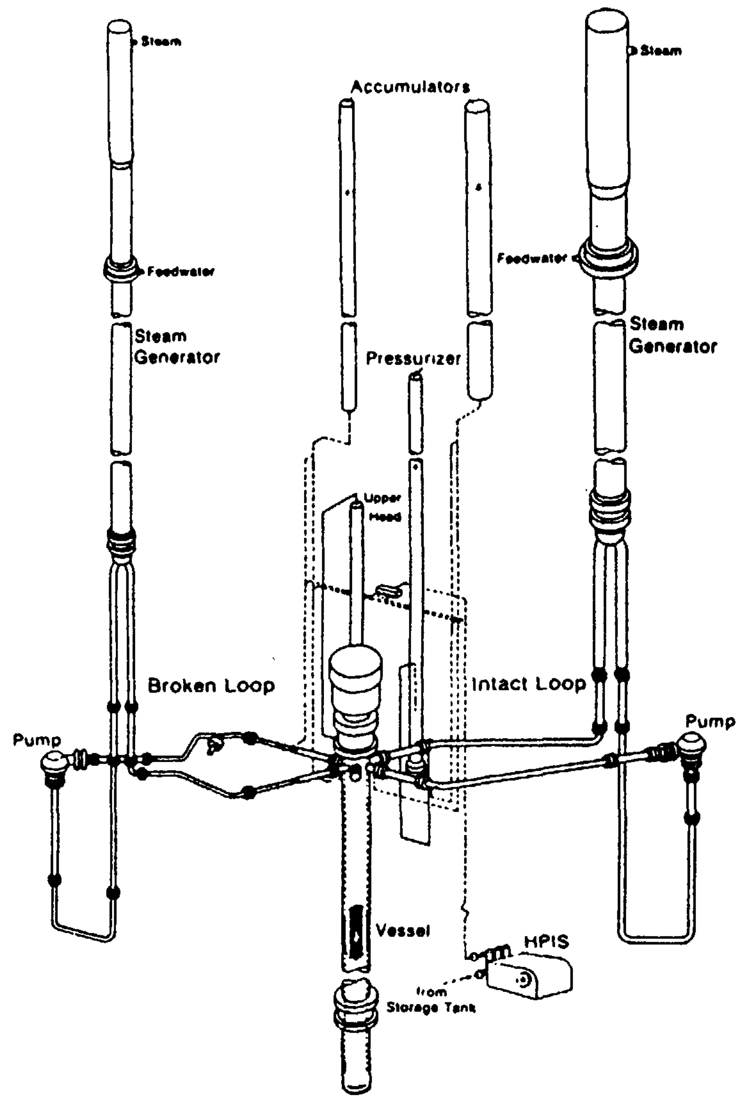
The international context in which the research programme is carried-out enables a close collaboration among the various EC member countries and provides a forum for the exchange of technical information and safety concerns in the field of reactor thermal-hydraulics. Within this framework, the tests of the B matrix are defined by experts of the EC member countries assembled in the LOCA and Special Transients Task Forces. Although the test profiles of the A matrix are exclusively defined by the German contract partner, the test results are however freely available to all EC member countries.

3. THE LOBI-MOD2 TEST FACILITY

The LOBI-MOD2 test facility is a high pressure integral system test facility representing an approximately 1 : 700 scale model of a 4-loop, 1300 MWe PWR. It has two primary loops, the intact or triple loop representing three loops and the single or broken loop representing one loop of the reference PWR. Each primary loop contains a main coolant circulation pump and a steam generator. The simulated core consists of an electrically heated 64 rod bundle arranged in an 8 x 8 square matrix inside the pressure vessel model; nominal heating power is 5.3 MW. Lower plenum, upper plenum, an annular downcomer and an externally mounted upper head simulator are additional major components of the reactor model assembly. The primary cooling system which is shown schematically in Fig. 1, operates at normal PWR conditions: approximately 158 bar and 294 - 326 ^{o}C pressure and temperatures, respectively.

Each heater rod of the simulated core consists of an internally pressurized hollow tube with an active heated length of 3.9 m, outer diameter of 10.75 mm and a pitch of 14.3 mm. The wall thickness is varied in 5 steps to provide a cosine shaped axial heat flux distribution.

The shell and inverted U-tube type steam generators have geometrical configuration similar to that in the reference plant. Each steam generator consists of a single cylindrical pressure vessel with an annular downcomer separated from the riser region by a skirt tube. This tube is supported above the tube plate, and carries the coarse separator. A fine separator is mounted in the uppermost part of the steam dome. The U-tubes (8 for the single loop and 24 for the triple loop steam generator) are arranged in a circle within the riser region, around an axially mounted filler tube. Feedwater is directed into the downcomer by a 'J nozzle' feed ring sparger and flows downward mixed with the recirculating water returned by the coarse and fine separators.



SYSTEM	loops	2 (1:3)
VOLUME	total-m^3	0.6
	scale reduction	700
CORE	power-MW	5.28
	length-m	3.9
	no. rods	64
	matrix	8x8
	heating	electrical
DOWNCOMER	configuration	annular
	gap width-mm	12
SGs	type	U-tube
	no. tubes:1-loop	8
	3-loop	24
MCPs	type	centrifugal
	n_q	29.2
OPERATION	pressure-MPa	15.8
	temperature-C	294/326

Fig. 1: LOBI-MOD2 Test Facility; Primary Cooling System and Major Design Characteristics

Heat is removed from the primary loops by the secondary cooling circuit containing a condenser and a cooler, the main feedwater pump, and the auxiliary feedwater system. Normal operating conditions of the secondary cooling circuit are 210^{o}C feedwater temperature and 64.5 bar pressure. The secondary cooling circuit is, however, designed for pressure of up to 100 bar.

The measurement system currently consists of a total of about 470 measurement channels. It allows the measurement of all relevant thermohydraulic quantities at the boundaries (inlet and outlet) of each individual loop component and within the reactor pressure vessel model and steam generators.

The whole LOBI-MOD2 test facility and individual components were scaled to preserve, insofar as possible or practical, similarity of thermohydraulic behaviour with respect to the reference plant during normal and off-normal conditions. A process control system allows the simulation of both the reactor main coolant pump hydraulic behaviour and the core decay heat; for the latter, however, on line nuclear-thermohydraulic feedback cannot be simulated at the present.

4. ASPECTS OF PWR PASSIVE SAFETY

New reactor concepts which are being developed to provide a viable nuclear option for deployment in the near future, are conceived to use passive bleed and feed of the primary coolant system as an effective emergency operating procedure. This safety system features intentional depressurization of the primary coolant system via the pressurizer power-operated relief valves (PORVs) and emergency injection from the passive accumulator system. Clearly, proper matching of relief capacity and fluid make-up is required to preclude excessive loss of fluid inventory and eventual core dry-out.

Recently, passive bleed and feed of the primary coolant system is being considered as a potential accident management strategy during the evolution of beyond design basis accidents in PWRs of current design. Here, the main concern is that in the case of severe core degradation a highly energetic melt ejection could occur if the primary system stagnates at high pressure. While there is still considerable uncertainty on the cut-off pressure, that is the pressure level below which debris dispersal is no longer a threat to direct containment heating, there is however a general consensus of opinions on the additional level of protection which could be provided by primary system depressurization.

Also, to mitigate the consequences of a small break LOCA in the event of loss of safety injection from engineered safety systems, it is envisaged to enhance the effectiveness of accumulator injection through the deliberate increase of primary system depressurization rate using the pressurizer PORVs. For reactors of current design this is not a straightforward operation and requires proper planning in order to avoid compounding failures. In perspective, for reactors of advanced design the effectiveness of such a procedure could be enhanced by optimizing plant lay-out and components operation such as capacity and location of depressurization line, accumulator actuation pressure and discharge characteristics.

5. LOBI-MOD2 PCS PASSIVE BLEED AND FEED

The main features of potential plant cooldown via primary system passive bleed and feed were investigated in the terminating phase of LOBI-MOD2 test BT-03 / 1 /, an anticipated transient without SCRAM (ATWS) originated by the loss of main feedwater (LOFW).

This test which was defined by the Italian delegation participating in the LOBI Project / 2 / comprised two distinct phases. While the first phase was aimed at reproducing LOFW-ATWS phenomenologies, the second phase was specifically designed to represent a passive recovery procedure being studied for the Italian PWRs / 3 /. Such a procedure consisted in intentional primary system depressurization through an equivalent 6" PORV located at the top of the pressurizer and passive safety injection from the 42 bar accumulator system.

At the end of the first phase the primary system was in hot conditions with the pressure at 95 bar and the primary fluid slightly subcooled. The main coolant pumps were not operational and the secondary system heat sink was intentionally not used to simulate prevention of positive reactivity insertion resulting from plant cooldown. Under these conditions the simulated PORV on the top of the pressurizer was latched open to depressurize the primary system.

Primary and secondary system pressure evolutions are shown in Fig. 2. As the PORV was latched open, single-phase steam at high enthalpy was discharged causing a fast depressurization and pressurizer liquid insurge with rapid liquid level increase as shown in Fig. 3. Following the attainment of saturated conditions in the primary system a two-phase insurge into the pressurizer was established. The depressurization rate was then partially reduced due to two-phase discharge through the PORV. As the primary system continued to void single-phase steam discharge was eventually reestablished through the PORV leading to an increase of primary system depressurization.

Depletion of primary system mass inventory was in time sufficient to cause core uncovery and dryout which progressed from the upper to the lower elevations of the simulated core as depicted in

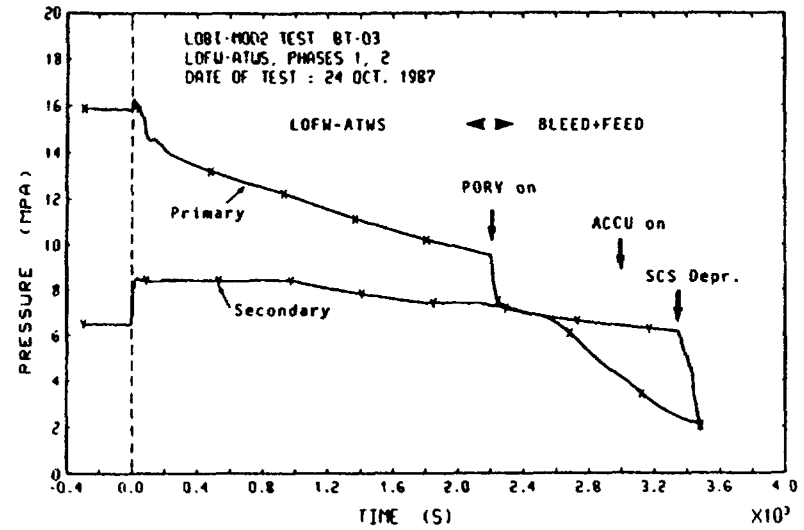


Fig. 2: LOBI-MOD2 Test BT-03: Primary and Secondary System Pressures

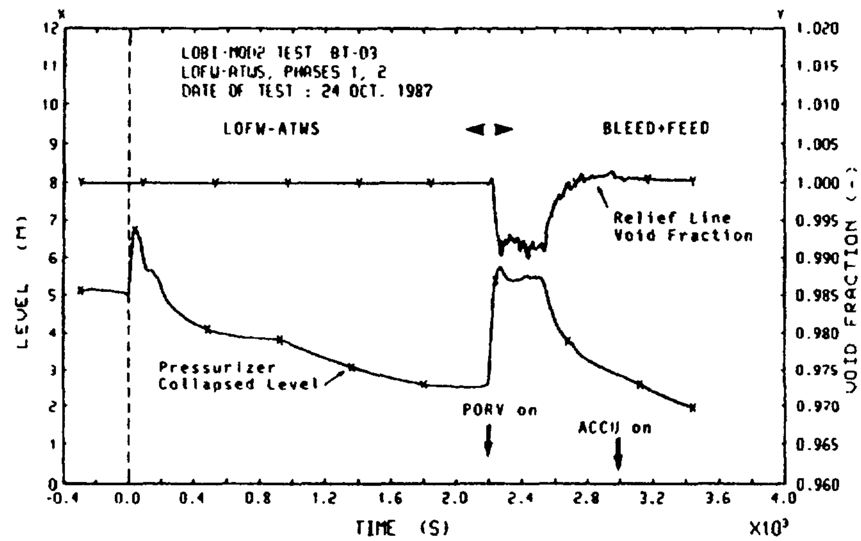


Fig. 3: LOBI-MOD2 Test BT-03: Pressurizer Level and Relief Line Void Fraction

Fig. 4. The onset of core dryout preceded the intervention of the accumulator injection system which became active only few seconds later. Thereafter, the reduction of primary inventory ceased as shown in Fig. 5 and, before the test was terminated on high heater rod temperature (c. 650°C), partial core rewetting was observed.

An attempt was made during the test to increase primary system depressurization and hence accumulator water injection by secondary system depressurization. This, however, had no discernible influence on primary system behaviour since condensation within the steam generators U-tubes was not effective. The fluid distribu-

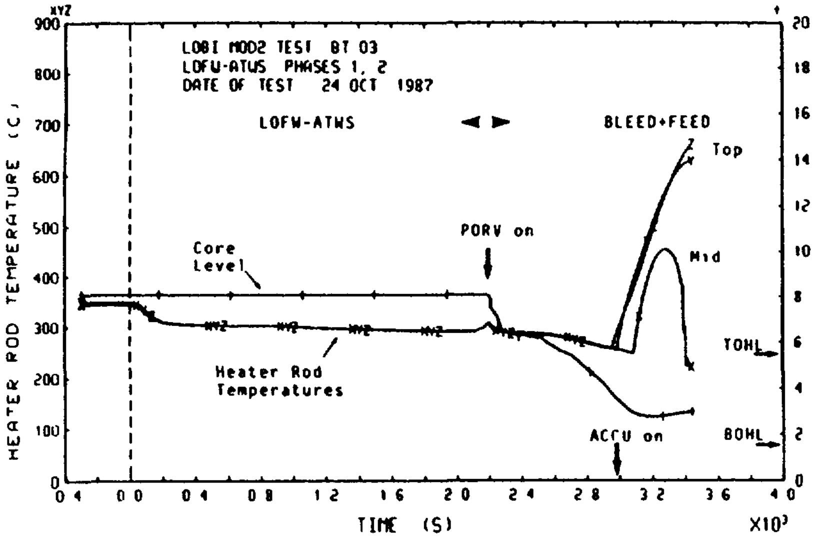


Fig. 4: LOBI-MOD2 Test BT-03: Core Level and Heater Rod Temperatures

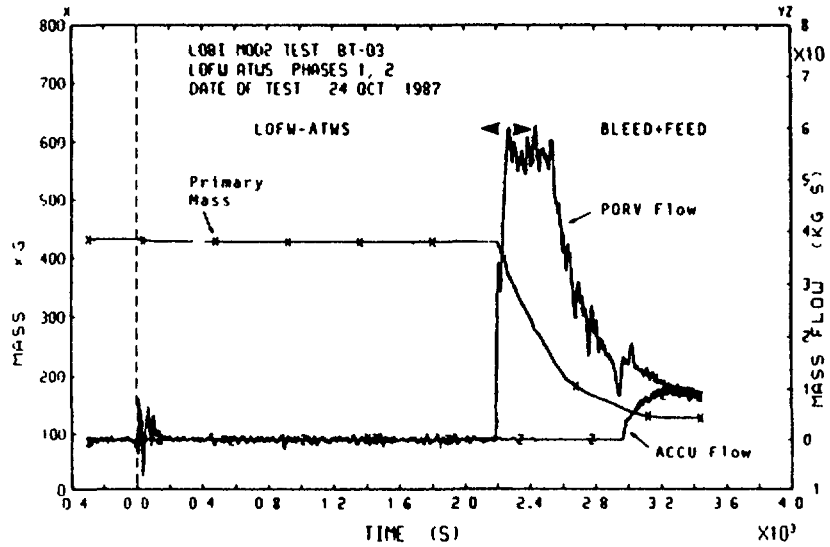


Fig. 5: LOBI-MOD2 Test BT-03: Primary Mass with PORV and Accumulator Flows

tion within the primary and secondary system at the start of the recovery procedure and at the time of accumulator injection initiation is shown in Fig.s 6 and 7.

As previously mentioned, the test was terminated on high heater rod temperature by tripping the core heating power. This precluded a full assessment of the prospected recovery procedure. On the basis of the acquired experimental results it is possible, however, to identify a tendency to full core rewetting. Also, the effectiveness of passive bleed and feed appears to be largely influenced by PORV discharge and pressurizer swelling as well as accumulator operational characteristics such as gas pressure and gas-to-water volume ratio.

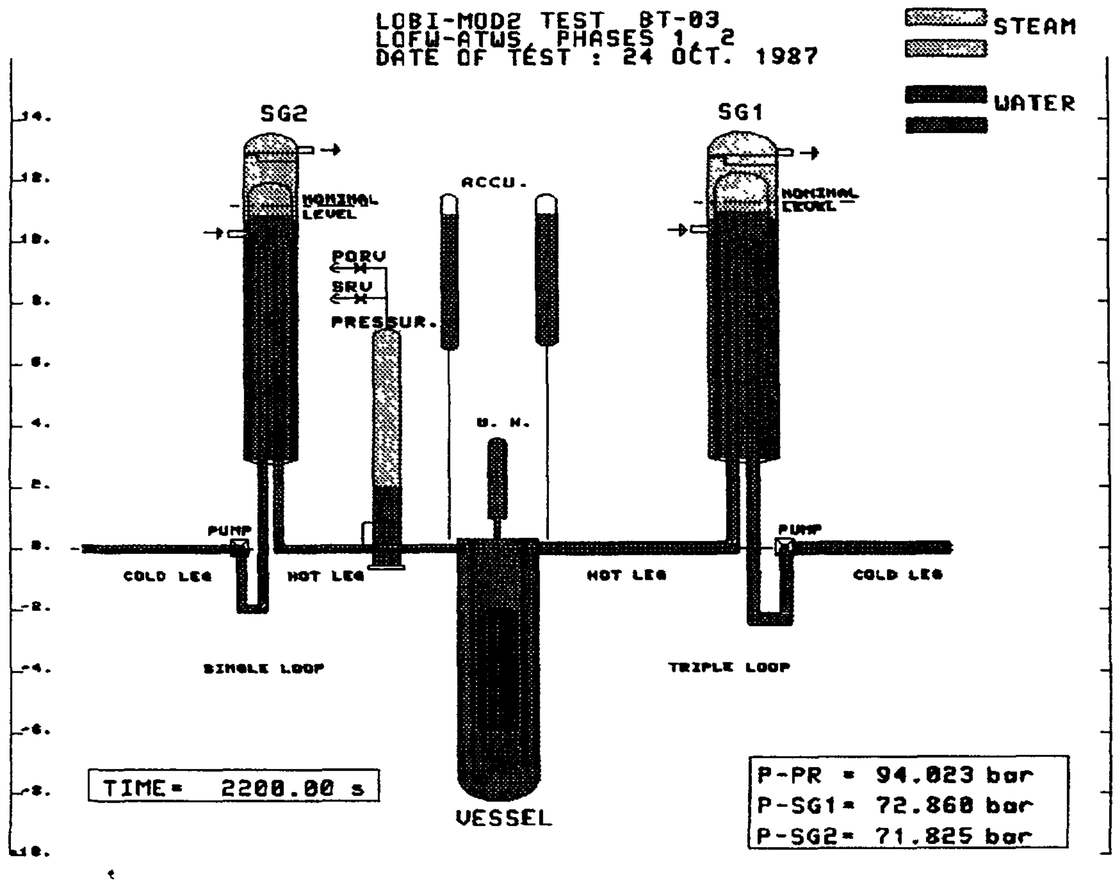


Fig. 6: LOBI-MOD2 Test BT-03: Fluid Distribution at the Start of Bleed and Feed

6. LOBI-MOD2 PORV OPERATION IN SMALL BREAK LOCA

To mitigate the consequences of a small break LOCA in the event of loss of safety injection from engineered safety system, it is possible to envisage the enhancement of ECC safety injection from the passive accumulator injection system through the intentional increase of primary system depressurization using the pressurizer PORVs.

LOBI-MOD2 test A1-93 / 4 / was specifically designed to verify phenomenologies pertinent to this eventual accident management procedure. The test represented a 2 % cold leg break LOCA with the high pressure ECC injection system assumed not operational. The accumulator ECC injection system was aligned with the hot legs and the gas pressure was set at 26 bars which is typical of a PWR of German design / 5 /. A first pressurizer PORV with an aperture equivalent to 100 cm^2 in the reference PWR was specified to be tripped on high heater rod temperature (c. 100 ^{o}C above saturation). In a full-size reactor this trip would probably occur on high core exit fluid temperature. An additional PORV equivalent to an aperture of 40 cm^2 was set to be tripped if heater rod temperatures would exceed about 600 ^{o}C.

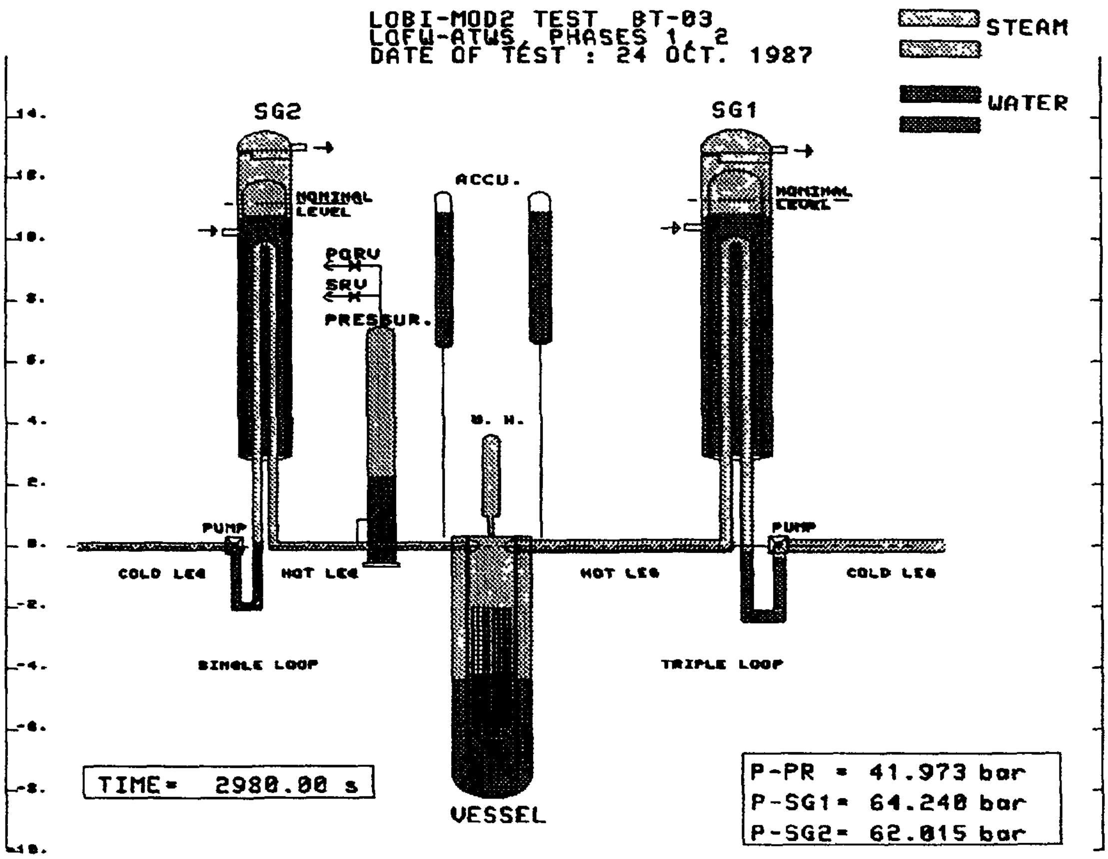


Fig. 7: LOBI-MOD2 Test BT-03: Fluid Distribution at the Start of Accumulator Injection

Primary and secondary pressure responses following initiation of the simulated rupture are shown in Fig. 8. With the high pressure injection disabled, the primary system mass inventory became in time sufficiently depleted to cause core uncovery and dryout as illustrated in Fig.s 9 and 10. Opening of the first PORV, Fig. 11, caused an insurge into the simulated core which led to a temporary rewetting at the lower elevations (Fig. 9) and to a decrease of heater rod temperature rise at the uppermost elevations (Fig. 10).

Operation of the first pressurizer PORV led to an enhancement of primary system depressurization rate. The accumulator injection system was thus anticipated. Thereafter, hold-up of temperature rise and localised rewetting was observed at the uppermost elevations of the heater rod bundle. Since accumulator injection was aligned with the hot legs, the downflow into the simulated core was certainly limited by the core updraft; also, on the basis of local heater rod temperature response especially at the uppermost instrumend levels, flow channeling can be postulated with the core updraft and the accumulator safety injection moving in a countercurrent fashion.

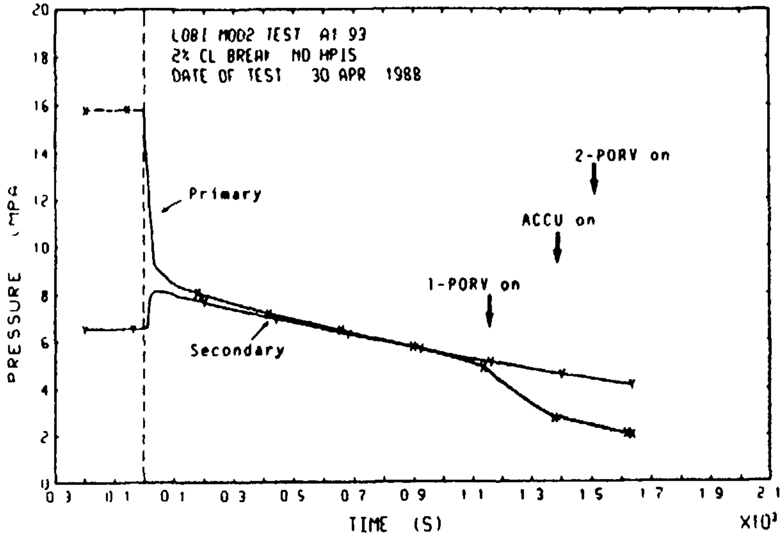


Fig. 8: LOBI-MOD2 Test A1-93: Primary and Secondary System Pressures

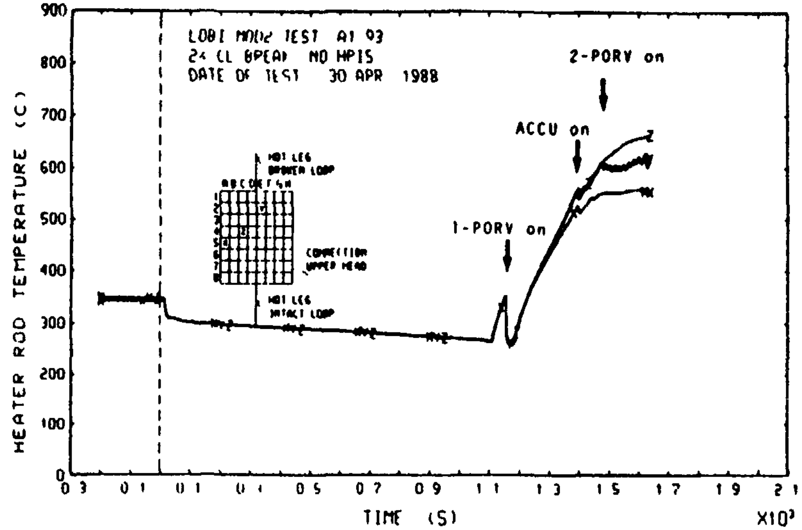


Fig. 9: LOBI-MOD2 Test A1-93: Heater Rod Temperatures at Core Mid Elevation

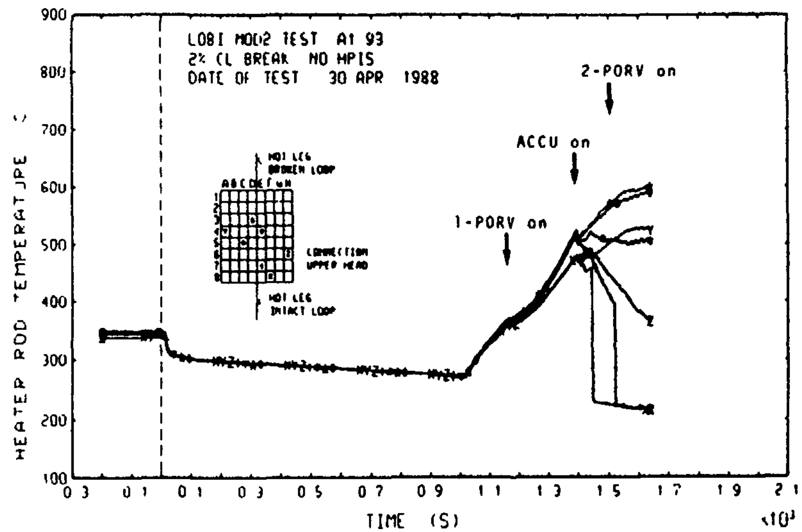


Fig. 10: LOBI-MOD2 Test A1-93: Heater Rod at Core Top Elevation

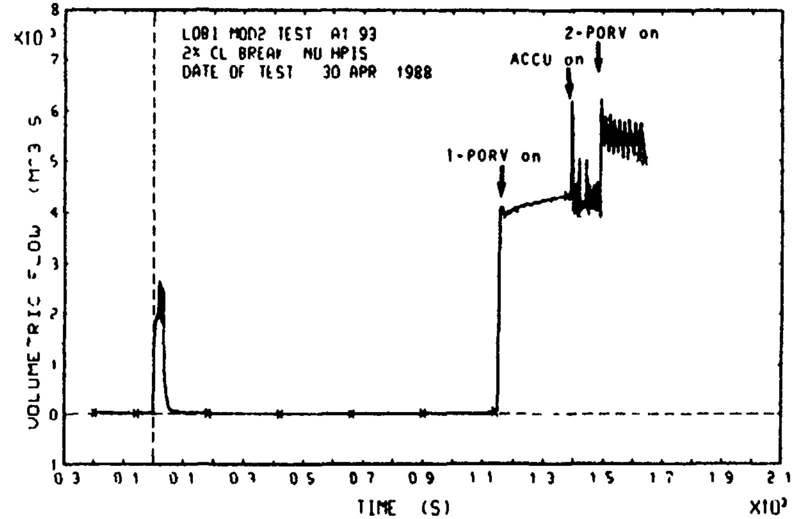


Fig. 11: LOBI-MOD2 Test A1-93: Surgeline Volumetric Flow

The effectiveness of accumulator safety injection was however not sufficient to terminate the heater rod temperature excursion. As heater rod temperature at certain elevations was approaching 600°C, the second pressurizer PORV was latched open in an attempt to increase primary system depressurization and hence accumulator safety injection. At 1646 s into the transient, the rod bundle heating power had to be terminated since heater rod temperature at local hot-spots went above the pre-set 650°C safety limit. Probably, full core rewetting could have been achieved without termination of core heating power if the 650°C limit was set at a higher value. Primary and secondary fluid distribution at the times of first PORV opening and accumulator injection initiation is shown in Fig.s 12 and 13.

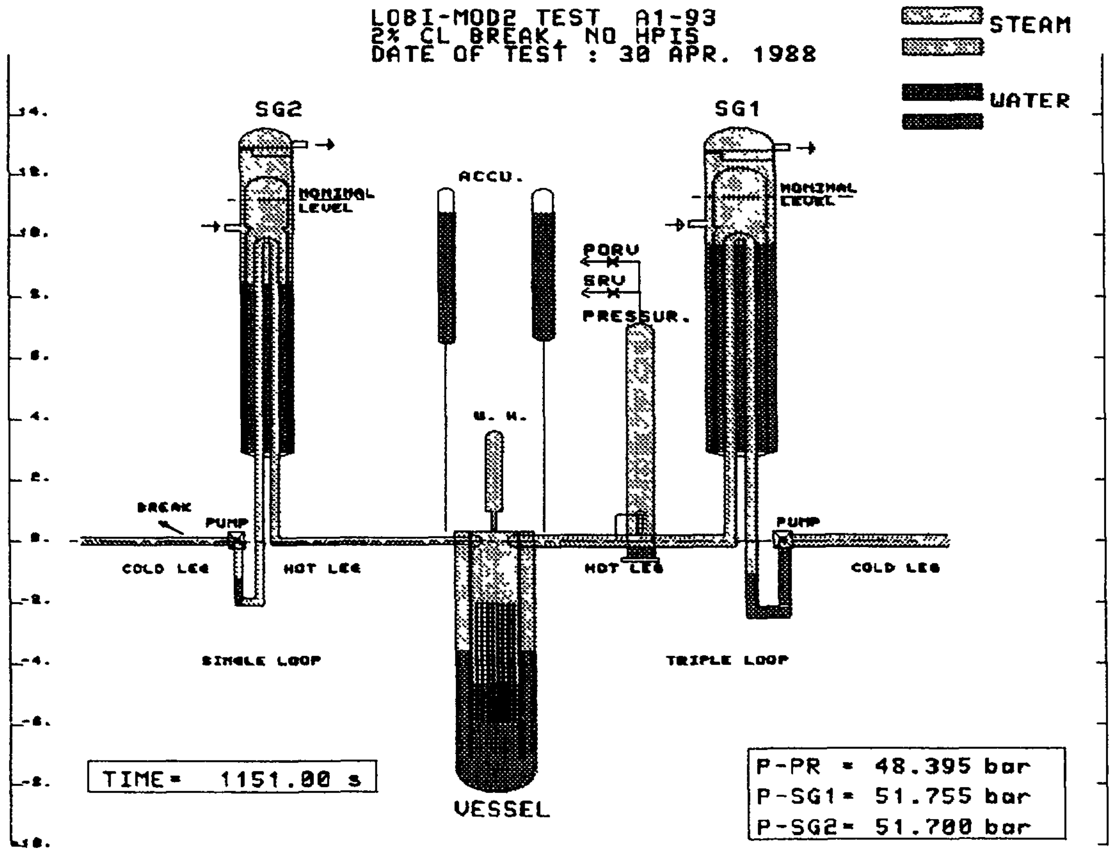


Fig. 12: LOBI-MOD2 Test A1-93: Fluid Distribution at the Time of Opening of the First PORV

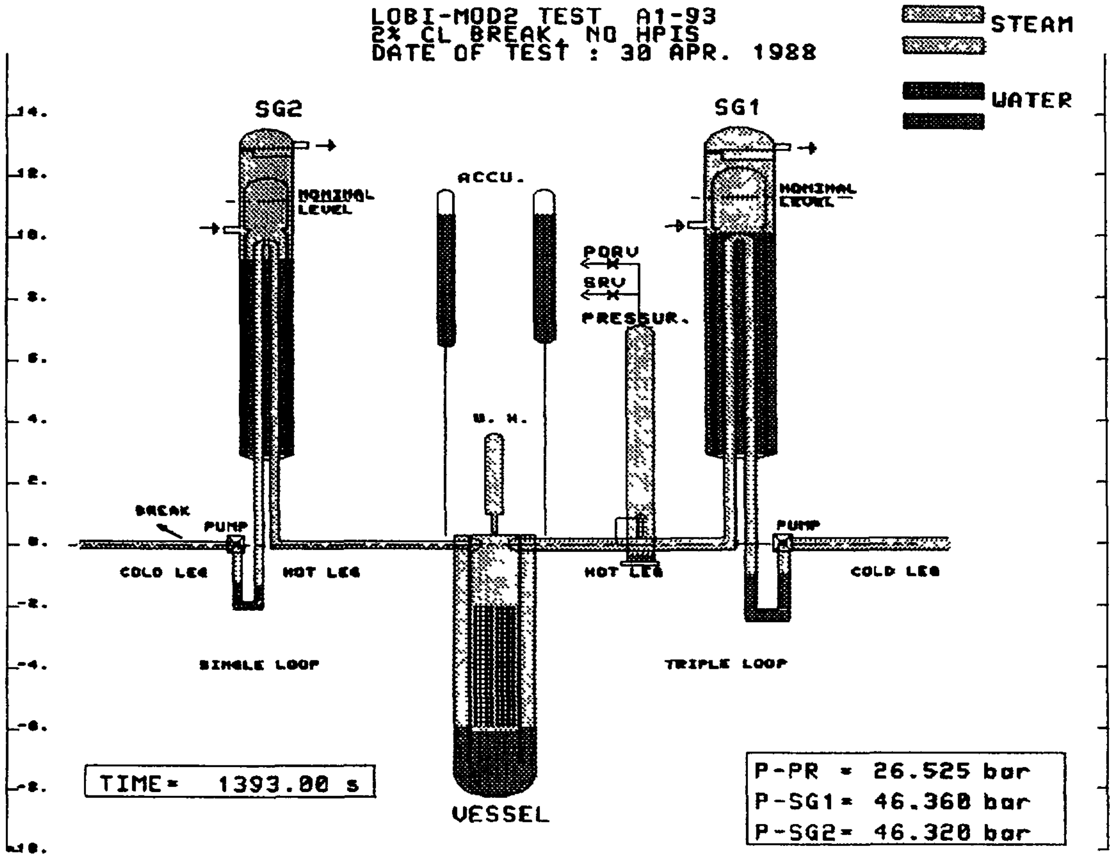


Fig. 13: LOBI-MOD2 Test A1-93: Fluid Distribution at the Time of Accumulator Injection

7. CONCLUDING REMARKS

A preliminary investigation of a class of phenomenologies relevant to potential passive safety features of present and, in perspective, of next generation power reactors has been carried-out in the LOBI-MOD2 test facility.

On the basis of the acquired experimental results, it is possible to assert that the effectiveness of the prospected safety concepts are largely influenced by the PORV discharge capacity and by the accumulator injection characteristics.

REFERENCES

1. Sanders, J., Ohlmer, E., "Experimental Data Report on LOBI-MOD2 Test BT-03", Communication No. 4219, CEC-JRC, June 1988.

2. D'Auria, F. et al., "Planning of the BT-03 LOFW-ATWS test in the LOBI-MOD2 test facility", DCMT NT 54 (1987).

3. Petrangeli, F. et al., "A core rescue system (SSN) for the implementation of preventive defence-in-depth safety criteria", CSNI Specialist Meeting on Decay Heat Removal Systems, Würenlingen, April 1983.

4. Jedrzejczak, D., Ohlmer, E., "Experimental Data Report on LOBI-MOD2 Test A1-93", Communication No. 4233, CEC-JRC, January 1989

5. Kirmse, R., "Definition of LOBI-MOD2 Test A1-93", GRS-Garching, Working Document, April 1988.

SAFETY OF EMERGING NUCLEAR ENERGY SYSTEMS: CRITERIA AND WAYS TO MEET THEM

V.M. NOVIKOV, I.S. SLESAREV
I.V. Kurchatov Institute of Atomic Energy,
Moscow, Union of Soviet Socialist Republics

Abstract

The first stage of world nuclear power development based on light water fission reactors has demonstrated not only a rather high rate but at the same time a too optimistic attitude to safety problems. Large accidents at Three Mile Island and Chernobyl essentially affect the concept of NP development. As a result the safety and social acceptance of NP became an absolute priority among other problems. That's why emerging nuclear power systems should be first of all estimated from this point of view.

In the paper some quantitative criteria of safety derived from estimations of social risk and economic-ecological damage due to large accidents are formulated. On the basis of this criteria we define enhanced safety NES, ultimate safety NES and asymptotic high safety ENES. The limits of tolerated expenses for safety are regarded. The basic physical factors determining hazards of NES accidents are considered. This permits to classify the ways of safety demands fulfilment due to physical principles used.

---

1. INTRODUCTION

Emerging nuclear energy systems (NENS) include all physical and design studies of new energy system based on nuclear phenomena. Each of them could be associated with its own specific problems, solution of which will define a future role for energy production. But at the same time all of them face common problems of extreme importance. It is safety and social acceptance of ENES. This problem is indeed a common one as each of ENES is associated with a new kind of risk due to nuclear radiation danger.

It is natural that safety criteria should be based on the experience gained in nuclear power (NP) development. Particularly it is true because advanced fission reactors and their combinations with different kinds of nuclear fuel breeders are an essential part of ENES.

In the history of NP development two stages may be definitely outlined. Nuclear power plant (NPP) large accidents took place at Three Mile Island (TMI) and Chernobyl (Ch) became a landmark which divided these stages. This time safety and social acceptance of NP are of absolute priority among other problems. It means that a concept of safer nuclear systems of new generation should be worked out.

Safety of any energy capacious technology cannot be absolute, this is a technical "nature" of safety. Improvement of safety means permanent movement and apportionment of technically reachable intermediate goals. The experience gained at TMI and Ch accidents may serve as "experimental data" for this purpose.

2. SOCIAL AND ECONOMIC-ECOLOGICAL CRITERIA OF SAFETY

The main goal of the nuclear plant safety can be achieved on condition of:

- conformance to the basic principles of safety elaborated in 1987-1988 by the international body of specialists generalizing the world experience to the current idea of the acceptable safety of a NPP
- unconditional fulfilment of the national rules and regulations on ensuring the safe operation of nuclear power facilities
- implementation of a new concept of NPP stability against large (ultrasevere) accidents.

The knowledge about the detriments from the large accidents occurred allows the reduction of the requirements for stability against large accidents to their permissible frequency (probability).

2.1 ESTIMATION OF NPP LARGE ACCIDENTS SOCIAL DAMAGE

To formulate social criterion of NPP safety it is necessary to take into account that even a few large accidents with radioactive release to the environment could completely blow confidence to NP and put a question of its elimination. So social criterion consists of demand, that during forecasted period of NP development (approximately 50 years) no large accident with possible radioactive release to the environment occurs within confidence limits of probability.

This demand correlates with psychological barrier of human unacceptance dangerous events repetition and some smoothing it after change of generation. Quantitative estimations of P_S - probability of large accident to a NPP with possible radioactive release to the environment are obtained on the base of this criterion [1].

[P] = 1/(reactor year):

$$nP_S \leq 10^{-2} \qquad (1)$$

where n-number of reactor years worked out up to the end of forecasted period of time.

This signifies that the probability to have no accident is 99%, the probability of numerous accidents is 0,01%, and mean number of accidents is less than 0,1 with 68% probability. All this could be taken as social acceptable level of NP safety.

To estimate n the following assumptions were used:

- in the middle of the next century the specific energy consumption will be about 5 kW per capita; total world population will be 8 billions; nuclear power will be about 20-30% of total. This leads to

$$P_S \leq 10^{-7} \qquad (2)$$

Nowadays NPP are far from this restriction.

2.2 ESTIMATION OF ECONOMIC-ECOLOGICAL DAMAGE DUE TO NPP LARGE ACCIDENT

Economic-ecological damage is connected with that of reactor, reactor building or NPP itself, impossibility of land use around NPP and so on. Damage may result in full loss of repairability of NPP, even when all radioactivity (r/a) is localized inside it.

Economic-ecological criterion consists of demand that economic losses from large accidents will not exceed a certain part of income from energy production. The latter is comparable with γ - economic growth and equal to some percent. It follows from this criterion [2,3]. The equation:

$$\sqrt{n}\, P_e + n\, P_e \le \frac{\gamma\,\lambda}{\beta} * \frac{k}{C} * n \tag{3}$$

here

C - damage due to a large accident

β - factor of income excess compare to damage

k - capital cost

λ - discount rate

P_e - permissable probability of NPP large accident derived from economic-ecological criterion.

To estimate P_e quantitatively the following two types of large accidents are taken as "reference" ones.

Type A. Large accident following core disruption and r/a release to the environment. Ch could be a model for such accident. For this case we have $C \approx 10*k$.

Type B. Large accident following core melt and r/a localized inside containment. TMI is a model for this type and we have $C \approx k$.

Taking for other parameters $\gamma = 0.1$; $\beta = 10$; $\lambda = 0.1*yr^{-1}$ we obtain the solutions P_e^A and P_e^B.

3. SAFETY DEMANDS TO NUCLEAR REACTORS OF NEW GENERATION

The necessity to satisfy both criteria leads to the conditions:

$$P^A \le \min\,(P_s,\ P_e^A)$$

$$P^B \le P_e^B \tag{4}$$

From (2) and (3) it follows that for large enough period of time one can take as necessitive the following values:

$$P^A \le 10^{-7} \text{ (reactor yr.)}^{-1}$$

$$P^B \le P^B_e \qquad (5)$$

and as a sufficient

$$P^B = P^A \le 10^{-7} \text{ (reactor yr.)}^{-1} \qquad (6)$$

It must be definitely said that modern reactors do not satisfy these demands. Therefore the conditions (5) and (6) may serve as bearings in development of nuclear reactors of a new generation. Following this way it is possible to distinguish two steps. The NPP of the first step have $P^B = 10^{-5}$ for core disruption and external facilities to localize r/a release inside the containment down to $P^A = 10^{-7}$. We call such NPP as enhanced safety NPP.

The NPP of the second step have $P^B = 10^{-7}$ for core disruption. We call such NPP as ultimate safety NPP.

4. WAYS TO MEET SAFETY DEMANDS

It is natural that working out of high safety NPP will go in the framework of traditional approaches with maximum use of reactor technology developed. This extensive way obviously results in more expensive NPP and one cannot exclude that NPP advantage before traditional PP will be used up. (For European part of USSR this cost advantage for modern NPP is about 20-40% [2]).

In this case the transition to asymptotic high safety reactors is accompanied by very strict cost demand. To characterize it let us introduce a - the effectiveness of cost investment in safety defined by

$$\alpha = (\Delta P/P) \ / \ (\Delta k/k), \qquad (7)$$

where ΔP - reduction of P value, which costs Δk; P and k are the corresponding basic values. It was shown in [2], that for type B accidents and NPP with $P^B = 10^{-5}$ we have a $\alpha \ge 10^4$. It means that transition from NPP with $P^B = 10^{-5}$ to ones with $P^B = 10^{-7}$ must practically leave the capital cost of NPP the same.

There is no real hope to fulfil it by using only additional active safety facilities. The proper way is to use simple physical (but not complex engineering) principles of fission phenomenon; that of natural convection of coolant; perhaps quasi-continuous fuel reprocessing and so on.

Therefore some new approaches should be carefully analyzed. Bearing this in mind, let us consider the basic physical factors determining the nuclear and radiation hazards of accidents resulting in reactor disruption (danger factors).

4.1 EXCESS REACTIVITY

The propability of the uncontrolled chain reaction appears to be a monotonously increasing function of the initial reactivity margin. In the modern reactors this parameter is very high, about 20% for LWR and about 6% for HTGR.

Different ways for reduction of the hazard associated with the existence of the reactivity margin can be roughly reduced to three basic ones.

(1) Incoproration into the reactor design some additional active external means for reduction for the uncontrolled chain reaction risk, such as new types of speedy regulators, increase of the reliability of the existing ones, some standby regulators, etc.

(2) Incorporation of some passive internal means of the critical control. By the passive inherent ones are meant physical and chemical control means so that the criticality control is provided on account of the internal physical and chemical properties of the system.

(3) Use of the reactor having such a design and operation mode which ensure very low excess reactivity with any core configuration change.

4.2 RESIDUAL SHUTDOWN HEAT AND RADIOACTIVITY STORED IN THE CORE

Radioactive fission products and associated residual heat release are the inevitable of the fission processes in the nuclear reactor. It may be the main cause of radioactivity release to the environment. The hazard of such consequences increases monotonously with increase of radioactive products stored in the core.

The ways of reducing the hazard associated with the residual shutdown heat can be presented by the same scheme.

(1) Additional active external means of emergency cooldown of the reactor (for example, additional tanks with water for emergency cooldown of VVER etc.)

(2) Internal passive cooldown means enabling the core temperature to be reliably kept of a permissible level for quite a long time required for repair or dismantling of the reactor.

(3) Use of such a reactor design and such a fuel cycle which would essentially reduce the accumulation of radioactive products in the core. Though the total amount of radioactivity remains the same, a significant fraction of it is transferred and kept under lower power density. Besides, such distribution of radioactive products may reduce even more the total risk of severe accidents in the total system if the principle of hazard "subdivision" is satisfied [1].

Therefore to increase the safety of the total system it is profitable to use the reactor with on-line preprocessing.

4.3 STORED NON-NUCLEAR ENERGY

The preference given to the maximum efficiency of nuclear fuel utilization leads to use of materials which in accidental situations might interact chemically with the air and/or water giving off large amounts of energy. For example, in the VVER-1000 the energy released in interaction of the zirconium clads with the steam at high temperatures to about one TJ. In HTGR with power 400 MW(e) burning of graphite results in release of about 4 TJ heat, and the energy of pressurized helium coolant adds about 1.5 GJ.

The ways of reduction of potential hazard from the stored non-nuclear energy can also be presented in terms of the scheme used above.

(1) Additional active external means for blocking chemical reactions.

(2) Passive internal safety means. For example, fireproof coolant, intermediate inert coolant in the sodium-water heat exchanger, etc.

(3) Transition to the reactor designs which exclude or extremely reduce use of chemically active components or high pressure gas.

4.4 QUALITATIVE LEVELS TO MEET SAFETY REQUIREMENTS

It is evident that any combination of conditions to lessen danger factors implies movement in higher safety. However it is more natural to group them by the main attribute. The first level is characterized by the emphasis on additional active external safety means. The NPP's of recent generation belong to this qualitative level of safety maintenance. The basis of the second level is rejection of the priority of active, technological safety means in favor of inherent and passive ones. The NPP belongs to this qualitative level, if these means are capable to block up subsystem failures and operator errors and no positive response required to subsystem malfunction.

The PIUS, NDHP and other reactors could be referred to the second level.

The opinion has been recently established that the guaranteed high potential of safety is ensured in case of reaching the total self-protection of a reactor, i.e. the capability of the reactor itself to conserve its core undamanged during practically all accident events of internal origin even without using any active protection means and involving any operating personnel (the third level).

Modular high-temperature reactors of limited power and modular fast reactors with low-temperature fuel can reach the third level.

The use of the total self-protection makes real the achievement of the highest probabilistic boundary (limit) equal to 10^{-7} $year^{-1}$ for core non-degradation under the action of internal initiators and, therefore, the meeting of all requirements for stability against severe accidents.

The fourth level can be characterized by additional feature-minimization of potential danger factors: reactivity excess, residual heat, radioactivity, stored non-nuclear energy. Reactors of this level are suitable for NPP of highest (asymptotic high) safety, for which the estimated probability of large accidents is essentially lower than the introduced boundary for ultimate safe reactor ($P^{A,B} \ll 10^{-7}$).

Now it is apparently impossible to indicate unambiguously the reactor designs which could be referred to the fourth level. Though the progress in this direction is possible, for example, ENES with on-line reprocessing allow, in principle, the minimization of the factors of potential risk due to nuclear nature (MSR, MS - accelerator breeder, hybrids with fission-suppressed blankets).

To avoid any misunderstanding the following should be noted: the fact that a certain type of NPP refers to a low quality level of meeting safety demands does not yet mean that this power unit cannot reach the required level of safety (for example, $P < 10^{-7}$ reactor year^{-1}). The transition to the higher quality level implies the better use of the simple physical principles for ensuring safety and the lesser significance of purely engineering features. All of this improves the reliability of attainment the safety level and that of the quantitative evaluations of risk making them more evident and convincing.

As development of ENES is believed to be important for imparting stability to NP and the alert and often sceptical public attention in some countries to NP should be taken into consideration, it is reasonable to join the efforts of developers in the international associations under the aegis of IAEA.

A good example is work on the concept of thermo-nuclear reactor ITER. In our opinion, the similar work should be arranged to promote the development of new concepts of breeders, molten-salt nuclear system and modular HTR, which possess high safety potential.

REFERENCES

[1] LEGASOV, V.A., NOVIKOV, V.M., "Safety and efficiency of the nulcear power: Criteria, ways of improvement", preprint IAE-4479/3, Moscow-Atominform, 1987.

[2] NOVIKOV, V.M., SLESAREV, I.S., IGNATJEV, V.V., et al., "The concepts of nuclear reactor of high safety", edited by Ponomarev-Stepnoj, N.N., Atomenergoizdat, Moscow, 1989, (in Russian).

[3] PONOMAREV-STEPNOJ, N.N., SLESAREV, I.S., "Atomic Energy", v. 64, N1, 1988.

SUMMARY OF THE WORKSHOP

H.J.C. Kouts

Brookhaven National Laboratory
Upton, New York
United States of America

I will report on the Workshop that took place in Chicago, Illinois, in the United States, on 28-31 August, sponsored by the IAEA and the government of the United States through the Argonne National Laboratory. The title of the Workshop was, "The Safety of Nuclear Installations of the Next Generation and Beyond." Almost two hundred participants were present, from countries around the world. They included numerous leaders in government and the nuclear industry in these countries. I might add that the government of the United States made its general support known through presentations contributed personally by high officials of the Department of Energy, the Department of State, and the Nuclear Regulatory Commission.

The logic behind the Workshop and its agenda were as follows. The news media now carry numerous stories on global environmental problems. These stories are based on what is perceived as a growing scientific consensus as to the causes and the effects of changes taking place. Two of the more severe concerns are impending warming of the earth through a greenhouse effect, and increased acidification of atmospheric moisture and its precipitation through rain and snow. These environmental problems are reported to be linked in large measure to the burning of fossil fuels.

Methods to be used in meeting the problems have been discussed in a number of places. It is stated that the response by people everywhere must involve changed patterns of generation and use of energy in its many forms.

The questions that were taken up in designing the Workshop started with increased realization that greater dependence on nuclear energy must be considered as part of the contemplated change, because nuclear energy does not contribute to these environmental problems. What, then might be the type and extent of the future requirement for heightened use of nuclear energy? How must the matter of public concern over safety of nuclear energy be addressed if this technology is to be returned to its previous state of active growth? What lines of development of future types of nuclear plants are being pursued throughout the world, that can affect the safety and acceptability of nuclear energy in the decades to come? What associated changes pertaining to safety will be needed in the nuclear field if the challenge is to be met positively?

These questions were addressed through an agenda structured on the lines of my next slide. The items listed are the topics covered by the nine sessions of the Workshop. At each session several invited presentations were made by distinguished scientists and engineers from around the world. The speakers were then joined by equally distinguished scientists and engineers in panel discussions on the topic covered by the session. There were only invited presentations, though added discussion from the floor was vigorous, substantive, and important.

The first session, during which the environmental problems were defined for the participants, was addressed by specialists in environmental sciences. The expert who recounted the situation on future greenhouse warming was Pierre Morel, of the World Meteorological Organization. The situation on acid rain was described by Bernard Manowitz, who is chairman of the US Department of Energy's interlaboratory consortium on acid rain. The panel had as further members Anthony Malinauskas of the Canadian Climate Center, Jill Jaeger of the Beijer Institute in the FRG, Carlos Velez of the National Institute for Nuclear Research in Mexico, and Bruce Hicks of the Oak Ridge laboratory of the National Oceans and Atmospheres Administration in the United States. The goal of the Workshop at this session was to determine from such scientists of impeccable environmental credentials whether the problems are real, their severity, and the measures being considered for their solution. It was found from the experts that the problems are indeed real and severe, that they are steadily becoming more severe, that electricity generation through burning fossil fuels is important in its contribution to future greenhouse warming, and it is a major contributor to acidification of rain.

It was made clear to the Workshop that these problems, especially future greenhouse warming, will demand all reasonable contributions to their solution. Even then the problems will not be completely solved but only reduced. After receiving this information, the Workshop turned to reviewing the extent of need for safe nuclear energy in the future in the next session.

The energy analysis presented in this session included a range of scenarios, based on present and anticipated trends in energy requirements and usage, and on population growth patterns throughout the world. The Workshop was informed that the requirements for new electricity generation are expected to continue to grow, and restraint of carbon dioxide emissions to their present levels could only lead to a need for extensive construction and operation of nuclear power plants. Typical estimates based on level CO_2 emission implied increasing the number of nuclear plants throughout the world by a factor of about 5 in 40 years, and a factor of about 10 in 70 years.

The first two sessions were a backdrop to the real purpose of the Workshop, and simply served to verify that environmentalists and energy analysts do foresee conditions that are expected to lead to resumption of substantial growth in the nuclear energy industry. If the growth is to take place, the safety of the industry must be addressed. The Workshop therefore concentrated on this topic. The first subject taken up was that of safety objectives and criteria. Safety of present nuclear plants was considered in the context of INSAG's publication, "Basic Safety Principles for Nuclear Power Plants," which I discussed in the scientific programme at last September's General Conference. There was a general agreement by the Workshop's participants that in most respects the existing nuclear power plants meet the current safety objectives, though they may not yet meet the INSAG principles in all detail. There was also a wide consensus that today's criteria will have to be made much more demanding if the number of nuclear plants is to be greatly increased. An order of magnitude reduction in probability of a severe accident would then be appropriate and desirable. This improvement in level of safety was also called for by the INSAG document.

The next few sessions of the Workshop included a series of descriptions of designs and design concepts of future nuclear plants, focused on their safety features. The nuclear plant concepts that were discussed were divided into two classes: evolutionary developments from current types of operating plants, that designers expect to be available on a near time basis, and more innovative concepts that might show promise after a longer period. The near time concepts included pressurized water and boiling water plants to generate from 600 MWe to 1500 MWe each. The developments of fast breeder reactors were also discussed, particularly in France, the Soviet Union, and Japan.

Among the more innovative plants, the ones that drew the most attention were the high temperature gas cooled systems under development in the United States and the Federal Republic of Germany, and variations on fast reactor designs in the United States. The PIUS design of ASEA-Brown Boveri was covered in an exhibit in parallel with the general Workshop sessions. Most of these advanced concepts were modular, where one plant would contain several reactor cores operating independently but supplying steam to a single turbine-generator. Part of the motivation for the modular designs was the introduction of engineering and manufacturing simplicity and economy. The Workshop participants who described the concepts emphasized numerous safety benefits which they believed would follow from their designs, especially simplicity, passive heat removal capability, and freedom from vulnerability to various kinds of accidents that must be considered in connection with more conventional plants.

Though there was a spectrum of views on the safety aspects of the designs discussed, the weight of opinion seemed to take certain lines. Most participants believed that the evolutionary design concepts will have to be used in satisfying near term requirements, and ensuring the safety of these plants should receive the primary attention at this time. There was strong interest in new and innovative concepts. Yet many participants counseled caution to avoid excessive claims of extraordinary safety. There was strong opposition to use of such terms as "inherently safe." There was widespread agreement that before novel safety features are accepted, they must be demonstrated in operation of prototype plants. It was also agreed that all nuclear plants for the foreseeable future will require tight and sturdy containment buildings. Many expressed the view that smaller plants are not necessarily safer, and that passive safety may not always be preferable.

One conclusion on which all agreed was that future nuclear plants of whatever type should be designed to be simpler and less dependent on human factors than the present ones. These features would substantially improve safety.

Discussion of the nuclear fuel cycle emphasized the need to get on with settling questions as to disposal of radioactive waste. It was agreed that problems faced are more political than technical. Progress toward their solution will call for better understanding and appreciation by the public as to the effects of low level radiation.

The meeting ended with discussion and acceptance of observations and conclusions, as follows:

1. No single form of generation and use of energy can all by itself prevent all greenhouse emissions or eliminate acid rain. But nuclear energy is already making a contribution to doing so, and can do much more if its use is extended. Failure to use nuclear energy to the extent it can be brought to bear would be short-sighted, because all feasible

ways to use or conserve energy wisely are necessary in reducing the environmental problems.

2. The environmental problems and the energy growth patterns that were outlined will require early planning and initiation of a substantial programme, that is estimated to require an increase in nuclear power plants by a large factor by the year 2030, and perhaps a factor of ten in the next sixty years. This growth in numbers of nuclear plants will increase the need to close the nuclear fuel cycle, primarily for assurance of continued fuel supply.
3. The future rate of deployment of nuclear energy will be greatly affected by society's perception of needs and acceptability. Nevertheless, considering the amount of time required to bring new nuclear plants into existence with the improved technology now available, resolution of public concerns must be pursued vigorously. Improved acceptability of nuclear power will depend on reliable and accident-free operation of nuclear plants everywhere, and by better public understanding of the health impact of radiation environments.
4. There have been two lines of development of advanced technology for nuclear plants. One consists of evolutionary improvements, especially of safety features, of some existing kinds of nuclear plants. The other has taken the line of innovative concepts that fulfill safety requirements through implicit characteristics. Both will be needed, the former for the near term and the latter in the more distant future, after the promise of the innovative concepts can be tested and confirmed by operation of prototype plants. The enhanced safety from the two lines of development is

necessary for a world with many more nuclear plants than now exist.

5. To ease the demands of a programme of extended use of nuclear power, technical improvements will be effected in each line of development, that will simplify designs and operation. Unnecessary complexity is being eliminated, and quality fabrication and manufacture of components are to be enhanced by greater use of prefabrication and construction controls.

6. In the longer term, breeder types of nuclear plants will be required, that would reduce demands on natural resources. The reliance on breeding will of course require means for extracting fission products and transuranic elements from spent fuel.

7. The rapid expansion of nuclear energy that the workshop found necessary will make heavy demands on the available world-wide reservoir of technical ability. This reservoir must be enlarged. In the meantime, it is important to maintain existing skills and capabilities.

It was concluded that enhanced technological exchanges should take place among nations, to facilitate rapid realization of concepts and dissemination of the results to a growing community of nuclear power developers and potential users around the world. Deep and thorough international analysis should be the basis for assurance of the soundness of technological choices and decisions. The workshop was a gathering of the individuals whose agreement and technical contributions were the start of a necessary movement to the developments that were urged. Now it is necessary to determine what further steps are needed.

CHAIRMEN OF SESSIONS

Session I	A. Gauvenet	France
	W. Loewenstein	United States of America
Session II	S. Finzi	Commission of the European Communities
	J.F. Marchaterre	United States of America
Session III	R. Carle	France
	V.A. Sidorenko	Union of Soviet Socialist Republics
Session IV	E. Beckjord	United States of America
	H.J. Teague	United Kingdom
Session V	A.A. Abagyan	Union of Soviet Socialist Republics
	P. Bystedt	Sweden
Session VI	G. Petrangeli	Italy
	S. Rosen	United States of America
Session VII	J. Beranek	Czechoslovakia
	K.B. Stadie	Nuclear Energy Agency of the OECD
Session VIII	Y. Kishimoto	Japan
	W. Stoll	Federal Republic of Germany
Closing Panel	H.J.C. Kouts	United States of America
	M. Rosen	IAEA

SECRETARIAT OF THE WORKSHOP

TECHNICAL PROGRAMME COMMITTEE:

Herbert J. C. Kouts	USA, Chairman
J. Terence Rogers	Canada
Sergio Finzi	Commission of the European Communities
Jiri Beranek	Czechoslovakia
André Gauvenet	France
Wolf Häfele	FRG
Gianni Petrangeli	Italy
Yoshitsugu Mishima	Japan
Miguel Medina	Mexico
Klaus B. Stadie	OECD-NEA
Agustin Alonso	Spain
Lars Högberg	Sweden
Harry J. Teague	UK
Victor A. Sidorenko	USSR
Armen A. Abagyan	USSR
Eric Beckjord	USA
Walter B. Loewenstein	USA
John F. Marchaterre	USA
Sol Rosen	USA
Morris Rosen	IAEA

Scientific Secretaries:

Ahmad Karbassioun	IAEA
Lester R. Rogers	USA
Jan B. van Erp	USA

US Advisory Committee:

Sol Burstein	WEP
Byron Lee, Jr.	NUMARC
Cordell Reed	CECO
Chauncey Starr	EPRI
Charles E. Till	ANL

Local Organizing Committee:

Henry E. Bliss	CECO
Miriam L. Holden	ANL
Dina M. Lawrence	CECO
Arne P. Olson	ANL
Jan B. van Erp	ANL

LIST OF WORKSHOP PARTICIPANTS

Armen A. Abagyan
Director
All-Union Research Institute for
Nuclear Power Plant Operations
Ferganskaya, 25
109507 Moscow
USSR

Joseph Alter
Director, Nuclear Engineering Division
Israel Atomic Energy Commission
P.O. Box 7061
61 070 Tel-Aviv
ISRAEL

Carmelo Addabbo
Scientific Officer
Commission European Communities
Joint Research Centre
21020 Ispra (Varese)
ITALY

Alfred Amorosi
Argonne National Laboratory
Building 315
9700 South Cass Avenue
Argonne, IL 60439
USA

John F. Ahearne
Executive Director Sigma Xi,
Past Chairman, U.S. Nuclear
Regulatory Commission
1834 Dalmatian Drive
McLean, VA 22101
USA

Jeanne D. Anderer
Technical Writer
IAEA
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna
AUSTRIA

Frank R. Allen
Head of Research and Methods Division
Safety & Reliability Directorate
United Kingdom Atomic Energy Authority
Wigshaw Lane, Culcheth
Warrington WA3 4NE
Cheshire
UNITED KINGDOM

Robin E. Ashwell
Manager, Control Center Design CANDU-3
Atomic Energy of Canada Limited
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2
CANADA

Agustin Alonso
Professor of Nuclear Technology
Polytechnical University of Madrid
Jose Gutierrez Abascal, 2
28006 Madrid
SPAIN

Robert Avery
Senior Physicist
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

Saleem Azeez
Manager
Process & Safety Engineering
Atomic Energy of Canada Limited
Sheridan Park Research Community
Mississauga, Ontario L5K 1A2
CANADA

Pierre Bacher
Vice President
Engineering and Construction Division
Electricite de France
22 Av. de Wagram
75382 Paris
FRANCE

Yuriy E. Bagdasarov
Head of Safety Division
Physics and Power Engineering Institute
Bondarenko Square
249020 Obninsk
USSR

Eric Beckjord
Director, Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
USA

Jiri Beranek
Inspector General
Czechoslovak Atomic Energy Commission
Slezska 9
Praha 2
CZECHOSLOVAKIA

Robert C. Berglund
Manager, Advanced Nuclear Technology
GE Nuclear Energy - Advanced Nuclear Technology
6835 Via Del Oro
Box 530954
San Jose, CA 95153-5354
USA

Victor M. Berkovich
Deputy Chief Engineer
Atomenergoprojekt Institute of the USSR Ministry of Atomic Energy
Bakuninskaya Street, No. 7
Moscow
USSR

Frederick M. Bernthal
Assistant Secretary
Bureau of Oceans and International Environmental and Scientific Affairs
U.S. Department of State
Washington, DC 20520
USA

Henry E. Bliss
Director, Advanced Technologies
Commonwealth Edison Company
P.O. Box 767
Chicago, IL 60690
USA

Ira Bornstein
Nuclear Engineer
Reactor Analysis & Safety Division
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

James H. Bottcher
Engineer
EBR-II Division
Argonne National Laboratory
Building 310
9700 South Cass Avenue
Argonne, IL 60439
USA

Gordon L. Brooks
Vice President & Chief Engineer
Atomic Energy of Canada Limited
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2
CANADA

Samuel P. Bowen
Program Leader
Division of Educational Programs
Argonne National Laboratory
Building 223
9700 South Cass Avenue
Argonne, IL 60439
USA

Sol Burstein
Consultant
7475 North Crossway Road
Milwaukee, WI 53217
USA

Robert Edward Boyar
Nuclear Engineer
Reactor Analysis & Safety Division
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

Per E. Bystedt
Head, Division of Reactor Technology
Swedish Nuclear Power Inspectorate
Box 27106
S-102 52 Stockholm
SWEDEN

Frederick C. Boyd
Vice-President
Wild and Boyd Management Advisors Ltd.
9 Sandwell Crescent
Kanata, Ontario K2K 1V2
CANADA

Antonio T. Calleja
Deputy General Manager
Iberduero, S.A.
Gardoqui, 8
48008 Bilbao
SPAIN

Robert B. Bradbury
Chief Engineer
Nuclear Technology & Licensing Division
Stone & Webster Engineering Corporation
P.O. Box 2325
Boston, MA 02107
USA

Remy L. Carle
Deputy Director General
Electricite de France
32, rue de Moneau
75384 PARIS Cedex 08
FRANCE

Rafael Caro
Commissioner
Consejo Seguridad Nuclear
Calle Sor Angela de la Cruz 3
28020 Madrid
SPAIN

L. Walter Deitrich
Associate Director
Reactor Anaylysis and Safety Division
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

Jean-Luc Caron
Engineer
CEA/CEN-FAR
60-68 Avenue du General LeClerc
B.P. 6
92265 Fontenay-aux-Roses Cedex
FRANCE

Dag Djursing
Manager, Nuclear Safety
Swedish State Power Board
Vattenfall
S-162 87 Vallingby
SWEDEN

Ira Charak
Project Manager
Reactor Analysis & Safety Division
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

Eryk J. Dluzniewski
Gesellschaft fur Reaktorsicherheit
Suite 1050
1747 Pennsylvania Avenue, NW
Washington, DC 20006
USA

Pierre P. Clauzon
Chef du Service
Etudes et Expertises
Framatome
Tour Fiat
Cedex 16
92084 Paris-La-Defense
FRANCE

Zig Domaratzki
Director General
Directorate of Reactor Regulation
Atomic Energy Control Board
P.O. Box 1046
Stn. B
Ottawa, Ontario K1P 5SP
CANADA

Emmanuel Creissels
Inspector Nuclear Installations
SCSIN
Centre d'Etudes Nucleaire
Bat. 01
B.P. No. 6
92265 Fontenay-aux-Roses
FRANCE

Thomas Downar
Professor
Purdue University
West Lafayette, IN 47906
USA

John T. Dunn
Director, Advanced CANDU Project
Atomic Energy of Canada Limited
Chalk River, Ontario K0J 1J0
CANADA

Sergio Finzi
Director
Commission of the European Communities
200, rue de La Loi
1049 Brussels
BELGIUM

Raymond W. Durante
Executive Consultant
AECL Technologies
Suite 500
1129 20th Street NW
Washington, DC 20036
USA

Jorg Fischer
Division of Nuclear Safety
IAEA
Wagramerstrasse 5
A-1400 Vienna
AUSTRIA

Juan Eibenschutz
Deputy Director General
Comision Federal de Electricidad
Rio Rodano 14
Mexico City, DF
MEXICO

Konstantin G. Foskolos
Staff, Laboratory for Reactor
Physics and Systems Engineering
Paul Scherrer Institute
Wuerenlingen and Villigen
CH-5232 Villigen-PSI
SWITZERLAND

Johan Engstroem
OKG AKTIEBOLAG
Box 1746
S-111 87 Stockholm
SWEDEN

Akira Fukuda
Manager, Nuclear Safety Engineering
Section
Toshiba Corporation
8, Shinsugita-cho, Isogo-ku
Yokohama 235
JAPAN

Ralf G. Espefaelt
Manager, Accident Analysis
and Management
Swedish State Power Board
Vattenfall
S-162 87 Vallingby
SWEDEN

Giovanni A. Gadola
Safety Group Manager
Nuclear Research Division
Ente Nazionale per l'Energia Elettrica
Direzione Degli Studi e Ricerche
Viale Regina Margherita 137
00198 Roma
ITALY

Andre J. Gauvenet
Inspector General for Safety (Emeritus)
Electricite de France
13-27 Esplanade Charles de Gaulle
92060 Paris la Defense
FRANCE

Robert S. Hall
Manager, Safety Technology Branch
Central Electricity Generating Board
Barnett Way, Barnwood,
Gloucester GL4 7RS
ENGLAND

Fred Gigliotti
Westinghouse Energy Systems
Business Unit
P.O. Box 355
Pittsburgh, PA 15230
USA

James Hannaford
Deputy Chief Inspector
Health and Safety Executive
H. M. Nuclear Installations Inspectorate
St. Peter's House
Balliol Road
Beotle, Merseyside
UNITED KINGDOM

Claus Goetzman
Senior Director
Siemens Aktiengesellschaft, UB KWU
Hammerbacherstrasse 12+14
8520 Erlangen, Bavaria
FRG

Richard W. Hardy
Program Manager
GE - Nuclear Energy
6835 Via Del Oro
San Jose, CA 95153-5354
USA

Gerald H. Golden
Associate Director
Reactor Analysis & Safety Division
Argonne National Laboratory
Building 310
9700 South Cass Avenue
Argonne, IL 60439
USA

John R. Harrison
Branch Head
National Power Company (CEGB)
18 Warwick Lane
London
ENGLAND

Wolf Haefele
Director General
Kernforschungsanlage Juelich GmbH
Postfach 1913
5170 Juelich
FRG

Michael R. Hayns
Deputy Director
Water Reactors Programme Directorate
AEA Technology
Harwell Laboratory
Didcot Oxon. OX11 ORA
UNITED KINGDOM

Hans-Henning Hennies
Member of the Executive Board
Kernforschungszentrum Karlsruhe GmbH
Postfach 3640
D-7500 Karlsruhe 1
FRG

Neill T. Howey
Nuclear Safety Administrator I
Illinois Department of Nuclear Safety
1035 Outer Park Drive
Springfield, IL 62704
USA

Enno F. Hicken
Head, Division of Thermohydraulics
Gesellschaft fuer Reaktorsicherheit mbH
Forschungsgelaende, 8046 Garching
FRG

James A. Hunter
Manager, Program Development Support
Westinghouse Hanford Company
Mail Stop LO-18
P.O. Box 1970
Richland, WA 99352
USA

Bruce B. Hicks
Director, Atmospheric Turbulence and
Diffusion Laboratory
National Oceanic and Atmospheric
Administration (NOAA)
Oak Ridge, TN 37830
USA

Toshio Ishii
Deputy Director
Nuclear Safety Research Center
Japan Atomic Energy Research Institute
2-4 Shirakata, Tokai-mura
Ibaraki-ken 319-11
JAPAN

David J. Hill
Section Head
EBR-II Safety Analysis
Reactor Analysis & Safety Division
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

Jill Jaeger
Beijer Institute
Eichenstrasse 2a
D-8152 Feldkirchen-Westerham 2
FRG

Joachim Hoehn
Staatliches Amt fuer
Atomsicherheit und Strahlenschutz
Waldowallee 117
Berlin 1157
GDR

Thomas Jobsk
Assistant Member of the Board
KFA Juelich GmbH
P.O. Box 19 13
D-5170 Juelich
FRG

Peter M. S. Jones
Chief Economic Adviser
U.K. Atomic Energy Authority
11 Charles II Street
London SW1
UNITED KINGDOM

Simon M. Koomen
Deputy Head, Nuclear Energy Section
Ministry of Economic Affairs
Bezuidenhoutseweg 6
2500 EC The Hague
THE NETHERLANDS

Ahmad Karbassioun
Division of Nuclear Safety
IAEA
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna
AUSTRIA

Herbert Kouts
Senior Physicist
Brookhaven National Laboratory
Upton, NY 11937
USA

Charles N. Kelber
Senior Technical Advisor
Atomic Safety and Lisencing Board Panel
U.S. Nuclear Regulatory Commission
MS EW/W 439
Washington, DC 20555
USA

Wolfgang Kroeger
Head, Institute for Nuclear
Safety Researchy
Kernforschungsanlage Juelich GmbH
Postfach 1913
5170 Juelich
FRG

Guenther Kessler
Director of the Institute for
Neutron Physics and Reactor Engineering
Kernforschungszentrum Karlsruhe GmbH
Postfach 36 40
D-7500 Karlsruhe 1
FRG

William C.H. Kupferschmidt
Research Scientist
Whiteshell Nuclear Research Establishment
Atomic Energy of Canada Limited
Pinawa, Manitoba ROE 1LO
CANADA

Y. Kishimoto
Director
Technology Development
Coordination Division
Power Reactor and Nuclear Fuel
Development Corporation
Tokai Works
Tokai-mura, Ibaraki-ken 319-11
JAPAN

Kazushige Kuriyama
Senior Engineer
The Institute of Applied Energy
14-2 Nishishinbashi, 1-chome
Minato-ku, Tokyo
JAPAN

Robert Lallement
Director, Nuclear Services
Commissariat a l' Energie Atomique
31 Rue de la Federation
75752 Paris
FRANCE

Jacques LePape
Project Manager
BELGATOM S.A.
75, rue de la Loi
1040 Brussels
BELGIUM

John D. B. Lambert
Manager
Experiment & Component Analysis
Argonne National Laboratory
Building 310
9700 South Cass Avenue
Argonne, IL 60439
USA

Milton Levenson
Executive Engineer
Bechtel Group
50 Beal Street
San Francisco, CA 94105
USA

Robert T. Lancet
Director
Rocketdyne Division
Rockwell International
6633 Canoga Avenue
Canoga Park, CA 91303
USA

Victor M. Libreros Marin
Emergency Planning and Preparedness
Comision Federal de Electricidad
Laguna Verde Nuclear Power Station
Veracruz
MEXICO

Raymond E. Lang
Program Manager
Chicago Operations Office
U.S. Department of Energy
Building 201
9800 South Cass Avenue
Argonne, IL 60439
USA

Michael J. Lineberry
Associate Division Director
Argonne National Laboratory
P.O. Box 2528
Idaho Falls, ID 83404-2528
USA

Wayne K. Lehto
Argonne National Laboratory
P.O. Box 2528
Idaho Falls, ID 83403
USA

Dan Litai
Director
Licensing Division
Israel Atomic Energy Commission
P.O.B. 7061
Tel Aviv 61070
ISRAEL

Walter Loewenstein
President, American Nuclear Society
c/o EPRI
3412 Hillview Avenue
Palo Alto, CA 94303
USA

Jose J. Lopez
Centro de Investigaciones Energeticas,
Medioambientales y Tecnologicas
Avenida Complutense, 22
28040 Madrid
SPAIN

Enzo Lo Prato
Integrated System Analysis Division
ENEA/DISP
Via Vitaliano Brancati, 48
00144 Roma
ITALY

Paul S. Lykoudis
Professor of Nuclear Engineering
School of Nuclear Engineering
Purdue University
West Lafayette, IN 47907
USA

John Madell
President
System Simulation & Analyses
P.O. Box 199
Western Springs, IL 60558
USA

Kiyohiko Maeda
Senior Engineer
PNC
O-Arai
Higashi Ibaraki
Ibaraki 311-13
JAPAN

Hans Maerkl
Executive Director
Systems Engineering and I & C,
Plant Engineering
Siemens AG, KWU Group
Hammerbacherstrasse 12+14
D-8520 Erlangen
FRG

A. Malinauskas
Canadian Climate Centre
4905 Dufferin Street
Downview, Ontario M5H 5T4
CANADA

Bernard Manowitz
Department Chairman
Department of Applied Science
Brookhaven National Laboratory
Building 179A
2 Center Street
Upton, NY 11973
USA

John F. Marchaterre
Director
Reactor Analysis & Safety Division
Argonne National Laboratory
Building 208
9700 south Cass Avenue
Argonne, IL 60439
USA

Gail H. Marcus
Technical Assistant to
Commissioner K. C. Rogers
U.S. Nuclear Regulatory Commission
Washington, DC 20555
USA

Yoshitsugu Mishima
President Atomic Energy Society
of Japan
Professor Emeritus
Tokyo University
3-30-11 Matsunoki,
Suginami-Ku
Tokyo
JAPAN

Stephen J. McAuley
Safety Manager SES-10 Reactor Project
Atomic Energy of Canada Limited
Chalk River Nuclear Laboratories
Chalk River, Ontario KOJ 1JO
CANADA

S. M. Modro
INEL
P.O. Box 1625
Idaho Falls, ID 83415
USA

Miguel Medina
Director General
National Commission for Nuclear Safety
and Safeguards
Insurgentes Sur 1806
01030 Mexico D.F.
MEXICO

Pierre R. Morel
Director, World Climate Research Program
World Meteorological Organization
C.P. 2300
CH - 1211 Geneva 2
SWITZERLAND

Daniel A. Meneley
Professor of Nuclear Engineering
P.O. Box 4400
Fredericton, New Brunswick E3B 5A3
CANADA

Jean M. Morelle
Manager - Fast Reactor Programme
Belgonucleaire
25, rue du Champ de Mars
1050 Brussels
BELGIUM

Michel Mezin
Manager
Nuclear Fuel Cycle Research
Commissariat a l'Energie Atomique
CEN-Saclay
91191 Gif-sur-Yvette
FRANCE

William G. Morison
Vice President, Design and Construction
Ontario Hydro
700 University Avenue
Toronto, Ontarios M5G 1X6
CANADA

Lewis D. Muhlestein
Manager, Safety Support Services
Westinghouse Hanford Company
P.O. Box 1970 (N1-28)
Richland, WA 99352
USA

Arne P. Olson
Nuclear Engineer
Engineering Physics Division
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

Antonio Natalizio
Advanced Concepts
Atomic Energy of Canada Limited
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2
CANADA

Gordon Packman
Safety Assessment Engineer
South of Scotland Electricity Board
Spean Street
Glasgow G44 4BE
UNITED KINGDOM

Keith Nuttall
Director
Whiteshell Nuclear Research Establishment
Atomic Energy of Canada Limited
Pinawa, Manitoba ROE 1LO
CANADA

Jose Palomo
Manager, Safety & Licensing Service
Hidroelectrica Espanola, S.A.
Hermosilla-3
28080 Madrid
SPAIN

Shunsuke Ogiya
Senior Engineer
Nuclear Power Engineering Test Center
4-3-13 Toranomon Minato-ku
Tokyo 105
JAPAN

Jacques Panossian
Sr. Vice President and Technical Advisor
Framatome
92084 Paris/La Defense CEDEX 16
FRANCE

David Okrent
Professor of Nuclear Engineering
UCLA
5532 Boelter Hall
Los Angeles, CA 90024
USA

Dean R. Pedersen
Manager, LMR Program
Reactor Analysis and Safety Division
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

Sergey P. Perminov
Administrative Officer
State Committee for Utilization of
Atomic Energy
Staromonetny per. 26
109180 Moscow
USSR

H. Peter Planchon
Manager
EBR II Support
Argonne National Laboratory
Building 310
9700 South Cass Avenue
Argonne, IL 60439
USA

Jean F. Petit
Deputy Director
Institut de Protection et Surete Nucleaire
Commissariat a l'Energie Atomique
C.E.N./F.A.R.
BP. 6
32265 Fontenay aux Roses-Cedex
FRANCE

Jad R. Popovic
Section Head, Computer Control
Engineering
Atomic Energy of Canada Limited
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2
CANADA

Gianni Petrangeli
Director, R & D Sector
ENEA/DISP
Via Vitaliano Brancati, 48
00144 Roma
ITALY

Don Radcliffe
Commercial Representative
Concord/ABB
Suite 105
Building 1
3000 Sand Hill Road
Menlo Park, CA 94025
USA

Massimo Pezzilli
ENEA/CRE Casaccia
Via Anguillarese 301
00060 S. Maria di Galeria (Roma)
ITALY

Atam S. Rao
Consulting Engineer
GE-Nuclear Energy
Mail Code 754
175 Curtner Avenue
San Jose, CA 95125
USA

Christen W. Pind
Senior Engineer, Secure Projects
ABB Atom AB
S-721 63 Vasteras
SWEDEN

Ami J. Rastas
Head of Development Department
Teollisuuden Voima Oy
27160 Okiluoto Suomi
FINLAND

Cordell Reed
Senior Vice President
Commonwealth Edison Company
P.O. Box 767
Chicago, IL 60690
USA

Morris Rosen
Assistant Deputy Director General and
Director, Division of Nuclear Safety
IAEA
P.O. Box 100
A-1400 Vienna
AUSTRIA

Ignacio M. Rico
Head, Nuclear Safety Technology Group
Instituto de Investigaciones Electricas
Apartado Postal #475
62000 Cuernavaca, Morelos
MEXICO

Sol Rosen
Assistant Deputy Director General and
Director Office of Advanced Reactor
Programs, and Acting Director Division
of International Programs
U. S. Department of Energy
Washington, DC 20545
USA

J. Terence Rogers
Professor of Nuclear Engineering
Carleton University
Colonel by Drive
Ottawa, Ontario K1S 5B6
CANADA

Eva L.J. Rosinger
President Canadian Nuclear Society,
Director Concept Review
Atomic Energy of Canada Limited
Whiteshell Nuclear Research Establishment
Pinawa, Manitoba ROE 1LO
CANADA

Kenneth C. Rogers
Commissioner
U.S. Nuclear Regulatory Commission
Washington, DC 20555
USA

Nils Rydell
Chief Engineer
National Board for Spent Nuclear Fuel
Sehlstedtsgatan 9
S-115 28 Stockholm
SWEDEN

Lester R. Rogers
Consultant
Argonne National Laboratory
Building 223
9700 South Cass Avenue
Argonne, IL 60439
USA

John I. Sackett
EBR - Argonne West 752 1
Argonne National Laboratory
Idaho Falls, ID 83403
USA

Oleg B. Samoilov
Deputy Director
Experimental Machine Contruction
and Design Bureau
Komsomolskoje Shosse
Gorki
USSR

Wolfgang O. Schikarski
Director, Laboratory for
Aerosol Physics and Filter Technology I
Karlsruhe Nuclear Research Center
P.O. Box 3640
D-7500 Karlsruhe 1/Baden Wuerttemberg
FRG

Julian Sanchez
Director, Development and
Research Division
National Institute of Nuclear Research
of Mexico
Sierra Mojada #447
2 Piso
Mexico D.F. 11000
MEXICO

Peter Schmidtlein
Institute for Energy Technology
University of Duisburg
Lotharstrasse 1-21
Postfach 101629
4100 Duisburg 1
FRG

Kazuo Sato
Deputy Director General
Tokai Research Establishment
Japan Atomic Energy Research Institute
Tokai-mura, Naka-gun
Ibaraki-ken 319-11
JAPAN

Alan Schriesheim
Director
Argonne National Laboratory
Building 201
9700 South Cass Avenue
Argonne, IL 60439
USA

Jack C. Scarborough
Technical Assistant to
Commissioner K. C. Rogers
U.S. Nuclear Regulatory Commission
12555 Rockville Pike
Rockville, MD 20852
USA

B. R. Seidel
Deputy Associate Division Director
Argonne National Laboratory
P.O. Box 2528
Idaho Falls, ID 83403-2528
USA

Herbert Schenk
Technical Director
Kernkraftwerk Philippsburg GmbH
D-7522 Philippsburg 1
Rheinschanzinsel
Postfach 11 40
FRG

Victor A. Sidorenko
The First Deputy Chairman
The USSR State Committee for
Supervision of Nuclear Power Safety
Taganskaya, 34
Moscow
USSR

Fred A. Silady
Department Manager
General Atomics
10955 John Jay Hopkins Drive
San Diego, CA 92121
USA

Robert W. Springer
Director
Division of Educational Programs
Argonne National Laboratory
Building 223
9700 South Cass Avenue
Argonne, IL 60439
USA

Victor G. Snell
Local Energy Systems
AECL
Pinawa, Manitoba ROE 1LO
CANADA

Klaus Stadie
Director, Organization for Economic
Cooperation and Development (OECD)
2, rue Andre-Pascal
75775 Pari Cedex 16
FRANCE

Leonard Soffer
Section Leader
U.S. Nuclear Regulatory Commission
Washington, DC 20555
USA

Chauncey Starr
President Emeritus
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303
USA

Alvin A. Solomon
School of Nuclear Engineering
Nuclear Engineering Building
Purdue University
West Lafayette, IN 47907
USA

Wolfgang Stoll
Chief Advisor
Siemens AG
6, Rodenbacher Chaussee
6450 Hanau
FRG

J. E. Speelman
ECN-Netherlands Energy Research Foundation
P.O. Box 1
1755 ZG Petten (N.H.)
THE NETHERLANDS

Stanislav A. Subbotin
Head of Laboratory
Kurchatov Institute of Atomic Energy
Kurchatov Square
Moscow
USSR

Kiyoaki Taketani
Adjunct Professor
Chuo University
Kasugacho Bunkyoku
Tokyo 112
JAPAN

Nicole M. Tellier
Nuclear Installation Inspector
Ministry of Industry/SCSIN
Centre d'Etudes Nucleaires FAR
BP 6
92265 Fontenay aux Roses
FRANCE

James M. Taylor
Acting Executive Director for Operations
Deputy Executive Director for Nuclear
Reactor Regulation, Regional Operation
and Research
U.S. Nuclear Regulatory Commission
OWFN 17 G 21
Washington, DC 20555
USA

Barbara Harrison Thomas
IAEA Programs Officer
U.S. Department of Energy (IE-13)
1000 Independence Avenue, SW
Washington, DC 20585
USA

John J. Taylor
Vice President, Nuclear Power
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303
USA

Charles E. Till
Associate Laboratory Director for
Engineering Research
Argonne National Laboratory
Building 208
9700 South Cass Avenue
Argonne, IL 60439
USA

Harry J. Teague
Deputy Director & Head of
Engineering Technology Division
Safety & Reliability Directorate
United Kingdom Atomic Energy Authority
Wigshaw Lane, Culcheth
Warrington WA3 4NE
Cheshire
UNITED KINGDOM

John C. Tuck
Under Secretary
U.S. Department of Energy
Washington, DC 20545
USA

Kenneth R. Teare
Senior Project Manager
Rolls Royce & Associates, Ltd.
P.O. Box 31
Derby DE2 8BJ
UNITED KINGDOM

Arnaldo Turricchia
Nuclear Safety Manager
Direzione delle Costruzioni
Ente Nazionale per l'Energia Elettrica
Via G. B. Martini,
3 - C. P. 386
00100 Roma
ITALY

Richard A. Valentin
Associate Director
Materials & Components Technology Division
Argonne National Laboratory
Building 308
9700 South Cass Avenue
Argonne, IL 60439
USA

Antti P. U. Vuorinen
Director General
Finnish Centre for Radiation and
Nuclear Safety
Elimaenkatu 25 A
P.O. Box 268
SF-00510 Helsinki
FINLAND

Jan B. van Erp
Nuclear Safety Research Engineer
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439
USA

Walter A. Weinlaender
Member of the Board of Directors
Deutsche Gesellschaft fuer
Wiederaufarbeitung von
Kernbrennstoffen mbH
Hamburger Allee 4
Postfach 1407
D-3000 Hannover 1
FRG

James A. Van Vliet
Deputy Director
Illinois Department of Nuclear Safety
1035 Outer Park Drive
Springfield, IL 62704
USA

Roy R. Wight
Nuclear Safety Administrator II
Illinois Department of Nuclear Safety
1035 Outer Park Drive
Springfield, IL 62704
USA

Carlos Velez
Director General
National Institute of Nuclear Research
of Mexico
Sierra Mojada 447
2 Piso
Mexico, D.F. 11000
MEXICO

Bertram Wolfe
Vice President & General Manager
GE-Nuclear Energy
175 Curtner Avenue
San Jose, CA 95125
USA

Georges Vendryes
Director Emeritus
Commissariat a l'Energie Atomique
7 rue de l'Etang
78150 Rocquencourt
FRANCE

Yunfu Xia
Counsellor
Permanent Mission of China to the IAEA
Steinfeldgasse 3
A-1190 Vienna
AUSTRIA

Werner F. von Lensa
Kernforschungsanlage Juelich GmbH
P.O. Box 1913
D-5170 Juelich
FRG

Professor Genki Yagawa
Professor of Nuclear Engineering
University of Tokyo
7-03-1 Hongo Bunkyo-ku
113 Tokyo
JAPAN

LIST OF PANEL PARTICIPANTS

(in addition to the speakers and chairmen)

Session I	A. Malinauskas	Canada
	J. Jäger	Federal Republic of Germamy
	C. Velez	Mexico
	B.B. Hicks	United States of America
Session II	L. Noviello	Italy
	G. Yagawa	Japan
	T. Calleja	Spain
	P. Jones	United Kingdom
	C. Starr	United States of America
	C.E. Till	United States of America
Session III	J.T. Rogers	Canada
	A.P.U. Vuorinen	Finland
	J. Palomo	Spain
	B. Wolfe	United States of America
Session IV	Z. Domaratzki	Canada
	H. Schenk	Federal Republic of Germany
	K. Sato	Japan
	J. Hannaford	United Kingdom
	V.A. Sidorenko	Union of Soviet Socialist Republics
	J.M. Taylor	United States of America
Session V	C. Reed	United States of America
	M. Levenson	United States of America
Session VI	S. Burstein	United States of America
Session VII	J. Sanchez	Mexico
	J. Panossian	France
Session VIII	J.M. Morelle	Belgium
	W.A. Weinländer	Federal Republic of Germany
Closing Panel	W.G. Morison	Canada
	J. Petit	France
	W. Wäfele	Federal Republic of Germany
	G. Petrangeli	Italy
	K. Sato	Japan
	M. Medina	Mexico
	A. Alonso	Spain
	H.J. Teague	United Kingdom
	A.A. Abagyan	Union of Soviet Socialist Republics

HOW TO ORDER IAEA PUBLICATIONS

An exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, has been appointed in the following country:

UNITED STATES OF AMERICA	UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391

In the following countries IAEA publications may be purchased from the sales agents or booksellers listed or through major local booksellers. Payment can be made in local currency or with UNESCO coupons.

ARGENTINA	Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires
AUSTRALIA	Hunter Publications, 58 A Gipps Street, Collingwood, Victoria 3066
BELGIUM	Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels
CHILE	Comisión Chilena de Energía Nuclear, Venta de Publicaciones, Amunategui 95, Casilla 188-D, Santiago
CHINA	IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing IAEA Publications other than in Chinese: China National Publications Import & Export Corporation, Deutsche Abteilung, P.O. Box 88, Beijing
CZECHOSLOVAKIA	S.N.T.L., Mikulandska 4, CS-116 86 Prague 1 Alfa, Publishers, Hurbanovo námestie 3, CS-815 89 Bratislava
FRANCE	Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
HUNGARY	Kultura, Hungarian Foreign Trading Company, P.O. Box 149, H-1389 Budapest 62
INDIA	Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016 Oxford Book and Stationery Co., Scindia House, New Delhi-110 001
ISRAEL	Heiliger & Co. Ltd. 23 Keren Hayesod Street, Jerusalem 94188
ITALY	Libreria Scientifica, Dott. Lucio de Biasio "aeiou", Via Meravigli 16, I-20123 Milan
JAPAN	Maruzen Company, Ltd, P.O. Box 5050, 100-31 Tokyo International
PAKISTAN	Mirza Book Agency, 65, Shahrah Quaid-e-Azam, P.O. Box 729, Lahore 3
POLAND	Ars Polona-Ruch, Centrala Handlu Zagranicznego, Krakowskie Przedmiescie 7, PL-00-068 Warsaw
ROMANIA	Ilexim, P O. Box 136-137, Bucharest
SOUTH AFRICA	Van Schaik Bookstore (Pty) Ltd, P.O. Box 724, Pretoria 0001
SPAIN	Díaz de Santos, Lagasca 95, E-28006 Madrid Díaz de Santos, Balmes 417, E-08022 Barcelona
SWEDEN	AB Fritzes Kungl. Hovbokhandel, Fredsgatan 2, P.O. Box 16356, S-103 27 Stockholm
UNITED KINGDOM	Her Majesty's Stationery Office, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR
USSR	Mezhdunarodnaya Kniga, Smolenskaya-Sennaya 32-34, Moscow G-200
YUGOSLAVIA	Jugoslovenska Knjiga, Terazije 27, P.O. Box 36, YU-11001 Belgrade

---

Orders from countries where sales agents have not yet been appointed and requests for information should be addressed directly to:

Division of Publications
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria