IAEA-TECDOC-1054

XA9848560 - 92

Technologies for improving the availability and reliability of current and future water cooled nuclear power plants

Proceedings of a Technical Committee meeting held in Argonne, Illinois, United States of America, 8–11 September 1997

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

29-52

The originating Section of this publication in the IAEA was:

Nuclear Power Technology Development Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

TECHNOLOGIES FOR IMPROVING THE AVAILABILITY AND RELIABILITY OF CURRENT AND FUTURE WATER COOLED NUCLEAR POWER PLANTS
IAEA, VIENNA, 1998
IAEA-TECDOC-1054
ISSN 1011-4289

Printed by the IAEA in Austria
November 1998

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

FOREWORD

A successful nuclear power plant is one that performs well. The global nuclear industry has a common interest in improving plant availability and reliability, not only from specific individual plant and country perspectives, but also to assure that it has an image of a well managed, competitive industry.

One of the activities of the IAEA is to provide all Member States with an international source of balanced, objective information on advances in technology for water cooled reactors. This IAEA Technical Committee Meeting on Technologies for Improving the Availability and Reliability of Current and Future Water Cooled Nuclear Power Plants was convened in September 1997 to identify, review and exchange information on international developments in technologies for achieving high availablity and reliability, and to suggest areas where further technical advances could contribute to performance improvement. The TCM was hosted by Argonne National Laboratory (ANL), Argonne, USA, on behalf of the United States Government, organized by the IAEA, and convened within the frame of activities of the IAEA's International Working Groups on Advanced Technologies for Light Water Reactors (IWG-LWR) and the International Working Group on Advanced Technologies for Heavy Water Reactors (IWG-HWR).

The IAEA expresses its appreciation to ANL and to the US Government for hosting the meeting. The IAEA also expresses its appreciation to H. Bliss (ANL), W. Deitrich (ANL), A. Klickman (ANL), J. Herczeg (US Department of Energy), M. Martin-Onraet (Electricité de France), P. Allen (Atomic Energy of Canada, Ltd) and T. Pedersen (ABB Atom) for their contributions to the summary which is presented in this TECDOC.

The IAEA technical officers responsible for this publication were J. Cleveland and R. Lyon of the Division of Nuclear Power.

EDITORIAL NOTE

In preparing this publication for press, staff of the IAEA have made up the pages from the original manuscripts as submitted by the authors. The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.

Throughout the text names of Member States are retained as they were when the text was compiled.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

CONTENTS

SUMMARY 1

OPENING ADDRESS 11
W.D. Magwood

POLICIES, PRACTICES AND PROCEDURES FOR ACHIEVING HIGH RELIABILITY AND AVAILABILITY (Session 1)

Availability analysis of United States BWR IV electrical generation plants 25
D.H. Renick, F. Li, N.E. Todreas
An integrated reliability management system for nuclear power plants 39
T. Kimura, H. Shimokawa, H. Matsushima
Current activities in support of CANDU plant life management:
An industry perspective 47
B.A. Shalaby, E.G. Price, J. Hopkins, P. Charlebois
Improving nuclear utility generation capacity, understanding the sources of forced outage and learning how to prevent them 57
D.L. Brodeur, V.T. Angus, N.E. Todreas
Revitalizing quality assurance 69
F.C. Hawkins
Improved nuclear power plant operations through performance-based safety regulation 73
M.W. Golay
Work management practices that reduce dose and improve efficiency 85
D.W. Miller, M. Hulin

IMPROVING AVAILABILITY AND RELIABILITY THROUGH BETTER USE OF TODAY'S TECHNOLOGIES (Session 2)

Pump system characterization and reliability enhancement 91
R.H. Staunton
Diesel Generator Data Acquisition System (DG-DAQ): A TVA nuclear technology 103
M.D. Bowman
Upgrading elastomer seals for nuclear service 113
K.C. Wittich, R. Wensel, R. LaRose, S. Kuran
Boron injection safety system modification in Atucha I Nuclear Power Plant 123
G. Salom, H. Quiroz
Improvement of lifetime availability through design, inspection, repair and replacement of coolant channels of Indian pressurized heavy water reactors 135
B.B. Rupani, R.K. Sinha
Bohunice V-1 and V-2 approach for achieving high availability, reliability and safety ... 145
M. Lipár, J. Kerak, Š. Rohár

RECENT ADVANCES IN TECHNOLOGIES FOR IMPROVING AVAILABILITY AND RELIABILITY (Session 3)

Prototype equipment status monitor for plant operational configuration management 169
M. DeVerno, S. Groom, D. Trask

Power plant surveillance and fault detection:Applications to a commercial PWR 185
R.M. Singer, K.C. Gross, J.P. Herzog, S. Wegerich, R. Van Alstine, F.K. Bockhorst
Computer-generated direct perception displays for supporting PWR feedwater system start-up and fault management: A proof-of-principle in design 201
D.V.C. Reising, B.G. Jones, N. Moray, S. Shaheen, P.M. Sanderson, J. Rasmussen
IGENPRO knowledge-based digital system for process transient diagnostics and management 213
J.A. Morman, J. Reifman, J.E. Vitela, T.Y.C. Wei, C.A. Applequist, P. Hippely, W. Kuk, L.H. Tsoukalas
The passive autocatalytic recombiner test program at Sandia National Laboratories 225
T.K. Blanchat, A. Malliakos
Use of passive autocatalytic recombiners at Indian Point 2 Nuclear Power Plant 237
D. Shah
Cost-effective instrumentation and control upgrades for commercial nuclear power plants using surety principles developed at Sandia National Laboratories 241
G.E. Rochau, L.J. Dalton
Defense against common-mode failures in protection system design 247
R.H. Wyman, G.L. Johnson

ACHIEVING HIGH AVAILABILITY FOR NEW PLANTS (Session 4)

Development and completion of the first ABWR and further improvement 257
N. Anahara
Advanced plant engineering and construction of Japanese ABWRs 267
N. Gotoh, J. Sumikawa, N. Yoshida, M. Yoshida
Designing for nuclear power plant maintainability and operability 279
T.J. Pedersen
Learning from experience: Feedback to CANDU design 291
P.J. Allen, J.M. Hopwood, G.P. Rousseau
The CIDEM project for integrating availability, operating experience and maintenance in the design of future nuclear power plants 297
C. Degrave, M. Martin-Onraet
EPR design for maintenance 311
U. Krugmann
Availability and its correlation with the cost situation of NPPs and an advanced reactor as a possible future solution 327
M. Fuchs
Plant availability design aspects of Korean next generation reactor 339
Woo Sang Lim, Ha Chung Baek
Advanced digital technology — improving nuclear power plant performance through maintainability 349
J.L. Ford, R.R. Senechal, G.D. Altenhein, R.P. Harvey
The design reliability assurance program for the Westinghouse AP600 reactor 357
M.H. Canton

LIST OF PARTICIPANTS 367

SUMMARY

Introduction

For nuclear power plants, achieving high availability and reliability[1] are essential factors for achieving good economics. Reliability is also extremely important in maintaining a high degree of safety. Achieving high plant availability requires attention to both the nuclear island and the balance of plant.

The average energy availability factor[2] for nuclear power plants in the world has increased from approximately 70 percent in 1989 to 76 percent by the end of 1996, with some utilities achieving significantly higher values. Nuclear plant operators are achieving high availability through integrated programmes including personnel training, quality assurance, improved maintenance planning, as well as technological advances in plant components and systems, and in inspection and maintenance techniques. International cooperation is playing a key role in this success. The various programmes of the World Association of Nuclear Operators (WANO) to exchange information and encourage communication of experience, and the activities of the IAEA including projects in nuclear power plant performance assessment and feedback, and effective quality management, are important examples of international cooperation to improve the performance of current plants.

Future water cooled nuclear power plants are being developed to provide enhanced economics, performance and safety. Advanced plant designs and feedback of experience from operating plants have generated a new set of requirements which influence plant design and layout. In particular, owners of future plants will require plant availability of 87 percent and above. Full advantage should be taken of the opportunity to incorporate the successful experience from operating plants so that the designs can accommodate all factors, organizational and technological, which support the achievement of high availability and reliability.

The Technical Committee Meeting (TCM), which was held in September 1997 at Argonne National Laboratory (ANL), reviewed technologies for improving availability and reliability and examined their implementation into the overall approach taken by operators of current plants which have had success in achieving good performance. Further, designs for future plants were presented in the context of how they can accommodate both the organizational and technical means for reaching even higher levels of performance.

Policies, Practices and Procedures for Achieving High Reliability and Availability

Activities have been and are being implemented at current plants (1) to analyse information from plant operation, at both the system and component level, leading to an improved

---

[1] Availability and reliability are general terms which are used in the nuclear industry. In this publication, the term availability generally refers to the fraction of time that the unit or equipment is capable of operation, and the term reliability refers to design attributes which assure that equipment will operate for a given period of time under stated operating conditions. These usages are considered with, for example, definitions presented in the Advanced Light Water Reactor Utility Requirements Document of the Electric Power Research Institute of the USA.

[2] Based on IAEA Power Reactor Information System (PRIS) data. In PRIS, the energy availability factor is defined as 100 [1-EL/E_m] with E_m being the net electrical energy which would have been produced at maximum capacity under continuous operation during the reference period, and EL is the electrical energy which could have been produced during the reference period by the unavailable capacity. (The numbers reported here are for plants with capacity greater than 100 MW(e) and with more than one year of commercial operation).

understanding of the causes of unavailability, and (2) to improve work practices during maintenance. Improved regulatory processes, improved quality assurance codes and practices, implementation of lessons learned from plant standardization activities focused on advanced plants, and on reduction of occupational exposure also contribute to improved availability and reliability at current plants.

As an example of analyses of operational data to improve the understanding of causes of unavailability, an investigation has been made in the USA of the causes of unavailability at all US BWR-IV units. Effects of early-in-cycle failures, end-of-cycle decreased availability, seasonal availability changes, and extended operating cycles were investigated. Somewhat surprisingly, end of cycle availability remained constant and did not decline as was expected. The initial work presented noted that end of cycle availability increased. A more detailed review of the data and accurate compensation for coast down diminished the magnitude of the end of cycle effects. The cumulative capacity factor, modified for coast down effects, was found to be nearly constant after the first year of operation. Seasonal availability patterns were as expected (planned outages are scheduled to avoid coinciding with heavy demand periods in winter and late summer) and longer operating cycles result in increased availability provided the daily availability during the extended period is greater than the cycle cumulative availability. The initial work presented early in cycle failures as having a significant impact on availability with daily average availability increasing from 60% at the beginning of cycle to about 93% at 100 days into the cycle. A more detailed review of start up effects and data analysis techniques significantly diminished the magnitude of this effect with an initial daily average power of 85% and the average daily power at day 100 of 92%. The reduced impact of the early cycle failures was not significant enough to greatly affect cumulative availability factor. A companion study examined a smaller sample of BWR-IV plants and concluded that balance of plant (BOP) systems initiated most unplanned outages (74%) and accounted for the majority of lost generation (54%). The data show that many systems, both BOP and Nuclear Island, rather than just one or two dominant ones, can fail leading to forced outages. Further, a database developed from only a small number of plants cannot provide a sufficiently broad overview. Thus it is necessary to cooperate in data exchange among several plants of similar design in order to compile enough information from which the most likely causes of unplanned outages can be identified.

Procedures for planning and carrying out maintenance influence reliability and availability. Good planning and organization of work during planned outages can strongly contribute to shortening outage duration and thereby contribute to availability improvements. For example, good face-to-face communication influences the efficiency of the execution of work during an outage, and something as mundane as the office configuration of the people planning outages can influence this communication.

Reactor designers have developed work management systems and component and system reliability data bases for their user groups. For example, Hitachi, Ltd of Japan has developed an integrated reliability management system which includes 4 elements: (a) input, correlation analysis, and retrieval of data on incidents, failures, and minor troubles (domestic and overseas plants), (b) analysis of operating performance indices of domestic operating plants, (c) a design management and design review management system, and (d) a fault tree analysis system specific to Hitachi-designed plants. This reliability management system is used by Hitachi to improve the design, operation and maintenance of its future plants and is also shared with operators of current Hitachi plants. For CANDU plants Atomic Energy of Canada Limited (AECL) has developed the Plant Life Management (PLIM) program to maintain high availability and reliability for the entire design lifetime and hopefully beyond. The PLIM program includes the key elements of identification of aging mechanisms, recommendation and implementation of methods to mitigate

aging effects, adoption of standardized work practices, inspection and rehabilitation/replacement of components, research and development to fill in knowledge gaps, and communication of lessons learned.

The US Nuclear Regulatory Commission's new Risk-Informed Performance-Based regulation policy is expected to contribute to high availability and reliability in that it is a goals-oriented, rather that a means-oriented, system focusing on what licensees must achieve rather than on what they must do. For example, simplification in surveillance and maintenance activities for emergency diesel generators are expected to result from this new policy thereby contributing to increases in availability through goal oriented practices. As another example, the new IAEA Quality Assurance Code 50-C/SG-Q and its fourteen accompanying Safety Guides are performance based; they incorporate contemporary principles and techniques for managing, achieving and assessing quality, emphasizing implementation, effectiveness and results rather than emphasizing programme development and documentation.

Increased standardization of plant design, construction, and operation is one of the hallmarks of future US nuclear plants. Particular attention is being paid to all aspects of plant operation in which it is envisioned that a "family" of plants (5 to 10), each with the same designer, reactor supplier and architect-engineer, will be operated and maintained with identical practices and procedures. A modification or procedure change at one plant is instituted all plants in the family . The results are expected to produce savings through reduced total staffing requirements and higher availability as problems are caught and corrected at most plants in the family before they cause downtime. Commonwealth Edison, in the USA, is in the process of extracting the benefits of this future plant standardization activity and applying them, where practicable, to the development and implementation of common processes, procedures and practices at all six of its sites.

The Information System on Occupational Exposure (ISOE) was established by the Nuclear Energy Agency (NEA) of the OECD in 1992 to facilitate the exchange of dose information on a global basis. An expert working group established by the ISOE Steering Committee showed rather conclusively that, based on European experience (primarily Finnish), there is a correlation between occupational exposure and outage duration. Excellence in work planning and execution leads to lower doses, shorter outages and increased availability. A number of US utilities have adopted work planning processes which have proven to be effective in Europe and have experienced shorter outages with lower occupational exposure.

Improving Availability and Reliability through Better Use of Today's Technologies

The deregulation of the electric power sector in the USA and in Europe is resulting in cost cutting policies in order to achieve or maintain economic competitiveness. At the same time the nuclear industry continues its vigilance in achieving a very high degree of safety. These dual goals of reducing power generation costs and maintaining a very high safety level are both served by better application of today's technologies to increase plant availability and reliability, by components and system upgrades/modifications, and by adoption of new approaches to maintenance and outage planning.

For example, an Oak Ridge National Laboratory (ORNL) study of the pump system (pumps, motors, turbine drives, circuit breakers) has shown that system reliability can be improved through improved circuit breakers, as the number of significant failures of this component exceeds the number of significant failures of the pump itself. The study also showed that testing mandated by regulation (e.g., codes) is focused on the pump only and therefore tends

to overlook the potential failures of other components in the pump system. There are several currently available on-line and off-line diagnostic technologies and monitoring techniques which, together with corrective maintenance, can be applied to make improvements in the reliability of a pump system. Examples are electrical signal and vibration analysis, accoustic and speed regulation monitoring, thermography and lubrication analysis. The challenge for plant designers is to select the best combination of tools, methods, and analysis techniques to provide the necessary diagnostic information.

The Tennessee Valley Authority has implemented a process computer based system providing reliable and accurate surveillance and diagnostics on emergency diesel generators (DG) at all of its nuclear stations. The system input data are DG output voltage and current. The need for shunts, transducers, decade boxes and associated internal wiring required by the previously used strip chart recorder method is avoided. The key new feature is the introduction of an on-line PC to process information. It is a relatively inexpensive device, and commercial software can be used to avoid one-off development. In the monitoring system developed by the TVA, a savings of 400 work hours per outage (representing about 95% of the effort previously required) has been achieved thereby contributing to improved plant availability. The new technique is a significant improvement over the strip chart recorder method and can be easily extended to perform surveillance and diagnostics for other plant systems.

As another example, the concept of on-line maintenance, which is widely used in fossil fueled power plants, is being increasingly applied at nuclear power plants. This technique allows a reduction in the outage work burden, provides a better and more efficient organization of the maintenance staff as well as of the planned outages themselves, and leads to reduced maintenance costs and improved scheduling.

Significant gains in availability and reliability as well as lower maintenance costs are projected, but not yet quantified, from the improvement of elastomer seals in the nuclear industry. This has been achieved through research on properties, development of a database for elastomer compounds for each service application, better quality assurance methods during manufacturing and inspection for defects, and improving elastomer seal storage and installation. The end result is a conscious and systematic selection of the best seal for the item of equipment in its "nuclear" application rather than simply relying on the manufacturer-supplied seal which was most likely based on some "non-nuclear" application of the equipment item.

Another approach to improve availability is to modify the plant configuration making components more accessible for surveillance and maintenance. For example, a modification project at the Atucha-1 plant in Argentina is in progress to move the components of the boron injection system (which takes the reactor subcritical in the case of a failure of the control rods to insert on demand) to a new location outside the reactor room so that maintenance and surveillance can be performed without shutting down the reactor. A mathematical model was developed to verify that the boron injection system actuation time, a key input parameter to the reactor safety analyses, would not be increased beyond the acceptable range by the proposed relocation of the components.

The Bohunice twin-unit V-1 and V-2 nuclear power plants in the Slovak Republic have initiated a comprehensive evaluation of their design and operational safety record and have a safety enhancement programme. Results are preliminary at this point but the plants do report a decrease in availability due to some of the actions implemented under the safety enhancement programme.

Availability and reliability of pressurized heavy water reactors (PHWRs), on which the Indian nuclear power programme is based, are strongly influenced by performance of the pressure tubes. India has developed a comprehensive pressure tube programme with the twin objectives of increasing their lifetime and increasing the efficiency of pressure tube replacement. Under the latter objective a visual inspection system has been developed and implemented, a sliver sample scraping technique to provide samples for estimating hydrogen pickup has been adopted, modifications to reduce inspection downtime have been incorporated, and a semi-automatic and remotely operable pressure tube replacement machine has been introduced which significantly reduces personnel radiation exposure.

In summary, several methods are currently available for improving availability and reliability for current and future plants. These are: reliability analysis, more extensive application of on-line maintenance, improvement accessibility for maintenance, improvement of life management in operation, use of PRA analysis and cost benefit analysis, use of reliability techniques to improve the choice of components, and simplified surveillance and diagnostics by integration of computer based monitoring systems.

Recent Advances in Technologies for Improving Availability and Reliability

Significant progress has been made and is continuing in application of new technologies (those which might not have been used in the nuclear industry but which have been successfully employed elsewhere) for improving availability and reliability. Areas of progress reported at the TCM include:

1. Application of newer developments in information technology for plant configuration management and for reduction of operating staff errors in the control room and field operations.
2. Improved diagnostic systems including novel measurement techniques and data analysis techniques.
3. Use of novel techniques to meet safety requirements, for example, installation of passive autocatalytic recombiners to assure control of hydrogen concentration following a potential accident.
4. Novel application of computers in control and protection systems including development of the required regulatory framework for judging acceptability of design solutions.

The advent of new, object-oriented software tools and smaller, more powerful hand-held computers the size of writing tablets have enabled the development of operational support systems that provide significantly more capability than was available just a few years ago. In Canada, the CANDU utilities and AECL have used these technologies to develop an Equipment status monitor (ESM) system to manage the operational configuration of a plant and to support preparation, execution and tracking of operating instructions. The heart of the system is the ability to record and display the current status of every operational device in the plant. The ESM, which was initially employed at Ontario Hydro's Darlington Station, has resulted in more timely and accurate plant status information and better control of plant changes which, in turn, have led to fewer errors and enhanced availability and reliability.

ANL in the USA has developed and validated an automated, on-line surveillance system for rapid annunciation of the incipience or onset of sensor disturbances, process anomalies, and sensor decalibrations. It was originally used on the EBR-II reactor and has been extended for commercial application. The system, called MSET for "multivariate state estimation technique",

employs a non-linear state estimation technique which is based on pattern recognition methodology integrated with an extremely sensitive fault detection algorithm for early recognition of faults from changes in stochastic characteristic of measured signals. MSET has been installed at Florida Power Corporation's Crystal River 3 plant and so far has detected several faults earlier than would have otherwise been detected; specific faults which have been detected by MSET include: degradation of venturi steam generator feedwater flow meter measurements due to fouling of the venturi surface, sensitivity loss of primary system flow meter, and loss-of-time response failure of a Rosemont pressure transmitter.

Researchers at the University of Illinois have proposed a theoretical approach for rationally designing computer-supported displays of plant configuration at various stages of plant startup. The idea is to present plant data to the operator at the appropriate level of abstraction so that the data perceived matches the cognitive demands of the current task. This approach is expected to enforce the correct sequence of operator behavior and prevent incorrect sequences. It has not reached the stage of actual application at a power plant but a proof-of-principle suite of displays has been developed to support the startup of a PWR feedwater system.

The US Department of Energy is sponsoring a collaborative effort among ANL, Commonwealth Edison Company (ComEd), and Purdue University to perform proof-of-concept studies on the use of Artificial Intelligence based diagnostics for component faults in nuclear power plants. A two level approach is used: at the first level an Expert System uses thermal-hydraulic functions to determine a physical occurrence, such as loss of water, and at the second level an artificial neural network is used to identify the actual source of the transient. The approach has been scaled up for use on the chemical and volume control system (CVCS) of the ComEd's Braidwood NPP Station by blind testing of CVCS faults generated by the Station's full scale simulator. The system correctly diagnosed 95% of faults (transients) with varying precision.

The control of hydrogen concentration within safe levels following a hypothetical loss of coolant accident is a Nuclear Regulatory Commission requirement for US light water reactors. Current plants have met this requirement by installing electrically powered thermal recombiners which have complex support systems, require extensive surveillance testing, and have caused significant maintenance and reliability problems. Recently, through the Electric Power Research Institute's Advanced Light Water Reactor Program, passive autocatalytic hydrogen recombiners (PAR) have emerged as a significant improvement in hydrogen removal technology. They have been successfully tested at Sandia National Laboratory in experiments which measured the ability of PARs to deplete hydrogen in a steam-air environment. Consolidated Edison Company (Con Ed) of New York has sponsored seismic and environmental qualification testing of PARs to shown that they meet the quality assurance requirements of 10 CFR 50 Appendix B. Con Ed is installing PARs at their Indian Point 2 plant in place of the existing thermal recombiners with the expectation of substantially improved availability and reliability of their hydrogen control system including a savings of one day during each refueling outage.

Nuclear plant operators are changing process instrumentation and control systems from analog electronics to digital electronics, incorporating technological advances such as distributed microprocessors and fiber optics. These changes, while greatly enhancing the man-machine interface and improving the ability of operators to control the plant, also bring new regulatory questions. To help address the regulatory questions associated with the conversion to digital technology, Sandia National Laboratory proposes the application of high consequence system surety (HCSS) principles to allow the use of off-the-shelf equipment for the conversion. HCSS has been successfully used to ensure the safety and security of US nuclear weapons. A specific question relates to the possibility of common mode failures due to the presence of identical

software operating in identical redundant systems. The Nuclear Regulatory Commission has developed a position to address this question.

Lawrence Livermore National Laboratory has developed a technique called "defense-in-depth and diversity analysis" to identify common mode failure vulnerabilities and suggests that the vulnerabilities identifed can be greatly reduced through good software engineering practice and a commitment to high software quality.

Achieving High Availability for New Plants

For new plants, the basis of availability and reliability should be incorporated during the design phase. With the increasing emphasis to achieve higher availability and reliability through the life of the plant, design improvements are needed. These design improvements should take into account the operating and maintenance experience of current plants.

Specific factors which can contribute to high availability and reliability if taken into account in the design phase can be categorized as follows:

1. Design considerations at the system and component level
   - Simplification
   - Standardization
   - Diversity and redundancy
   - Fault tolerance
   - Passivity
   - Ease of component replacement and repair
   - Ease of on-line testing and maintenance

2. Technologies
   - Digital instrumentation and control including self-diagnostic systems
   - Control room and man-machine interface improvements
   - Human factors engineering for plant layout
   - Material degradation countermeasures
     - water chemistry
     - material improvements
   - Refueling systems

3. Design for optimum outages, operation, maintenance and inspection (incorporating these aspects at an early state in the design)

4. Increased thermal and hydraulic design margins

In Japan, the development of the Advanced Boiling Water Reactor (ABWR) started in 1978 as an international co-operation between five BWR vendors. The resulting conceptual design was received favourably by Tokyo Electric Power Company (TEPCO) and other Japanese utilities, and as a result, the ABWR was included in the third standardization programme of Japan from 1981. Preliminary design and numerous development and verification tests were carried out by Toshiba, Hitachi and GE together with six Japanese utilities and the Japanese Government. Use of improved technologies to increase plant availability beyond the already successful Japanese experience was a corner stone of ABWR development. Significant examples are the use of internal (to the pressure vessel) reactor recirculation pumps, fine motion control rod drives, advanced (digital and multiplexed fiber optic signal) technologies for instrumentation and

control systems, and a state-of-the-art turbine employing 52-inch last stage buckets. The culmination of the effort was the ordering by TEPCO of two ABWRs, the Kashiwazaki-Kariwa units 6 and 7, which have been successfully taken into commercial operation in November 1996 and July 1997, respectively.

Hitachi has contributed to the success of the ABWR in Japan through the use of two advanced engineering technologies. Modern three dimensional computer aided design (3D-CAD) tools were used during design to assess the plant maintainability and accessibility and during construction to verify proper installations. Further, large-scale modularization and large capacity cranes were used during construction to shorten plant construction time and reduce interest-during-construction costs.

ABB Atom is following their traditional "small-steps" approach in the development of their BWR 90 advanced plant by employing feedback from design, construction, commissioning and operation of previous generations of plants. New features are being introduced only when it can be shown that distinct improvements are gained. Design measures to facilitate maintainance and operation have already been included in ABB Atom's operating plants — improvements demonstrated by operating performance of these plants — and the new BWR 90 design is an evolutionary system based on this experience. Of particular note is the modernization of instrumentation and control systems being applied in several of ABB Atoms operating plants. These upgrades, based on digital technology, will improve maintainability and operability and will be carried over into the BWR 90 design.

AECL has a similar evolutionary approach to feedback of operating plant experience into development of new designs. This allows retention of successful features from current plants while incorporating new features as they are developed and tested. The key to this process is an alliance between AECL (the CANDU designer) and the utilities which operate CANDUs. This alliance provides for the support, operation, development and improvement of CANDU technology. AECL also solicits feedback from equipment suppliers and regulators as well as incorporating market input and pertinent R&D results. Some examples of successful feedback are improved steam generators, updated digital displays and overall human factors enhancements, and better strainer design leading to simpler and improved emergency cooling water system performance.

The CIDEM project of Electricité de France (EdF) is another excellent example of a dedicated effort to incorporate experience with existing plants to optimize the design of future plants. It involves the systematic application of operations experience, outage analyses (planned, forced, and extended), operating and maintenance cost figures, radiation exposure information and research and development needs to minimize the kw/h cost of future plants.

The process, uses concepts known by the acronyms RAM (reliability, availability and maintainability), RCM (reliability centered maintenance), ILS (integrated logistic support).

The project has incorporated requirements on the availability of different systems and components, as well as goals for refuelling outage durations. CIDEM results to date have shown that the availability objective for EdF plants beginning construction around the turn of the century can be increased from 87% to 90%.

In Europe, the nuclear power plant suppliers Siemens and Framatome with their joint subsidiary Nuclear Power International, together with Electricité de France and a group of nuclear German utilities, have worked out the basic design of the European Pressurized Reactor.

This reactor is designed to meet the common set of utility requirements endorsed by the major utilities of European countries as expressed in the European Utilities Requirement document. This includes safety improvements on all levels of defence in depth including the protection of the containment function against severe accident conditions. A key challenge for the project has been the development of an overall maintenance strategy at an early design stage in order to achieve on acceptable plant availability without impairing overall plant safety.

In order to achieve an overall refueling outage duration of less than 18 days, the following measures — beside others — have been taken:

- improved layout of the operating floor to provide adequate space for servicing and equipment laydown,
- redesigned safety systems to permit greater maintenance capability during plant power operation, and
- accessible containment to relax refueling outage from preparatory and cleanup activities.

Utilities are concerned with the escalation of investment costs for new plants and costs for backfitting and modernisation in existing plants due to increasing regulatory requirements which lead to greater redundancy of safety systems but not necessarily diversity to reduce the probability of severe accidents, because it is determined by common mode. As an example to counter this trend, Preussen Elektra advocates consideration of new, innovative ideas to ensure competitivity of nuclear power. The SWR 1000, being developed by Siemens under contract and in close cooperation with German Utilities and with support from various European partners incorporates a number of improvements — such as passive safety features, lower core power density combined with larger coolant inventory, greater water capacity in the passive core cooling systems, and the capability to flood the area around the reactor pressure vessel — that are intended to yield appreciable design simplification and corresponding cost reduction.

The Korean Electric Power Research Institute (KEPRI) is working on the design of the Republic of Korea's next generation, standardized PWR. To increase availability KEPRI is focusing on reducing the number and duration of forced and planned outages. Two major design changes, compared to today's plants, are planned: (1) switching to circulating water pumps in the turbine building open cooling water system, and (2) changing the main feedwater pump drives from steam turbine to adjustable speed motor. KEPRI has concluded that further reductions in the actual refueling time will result since turbine and generator maintenance are on the critical path. They will concentrate future design work in these areas.

ABB Combustion Engineering, in their System 80+ Advanced LWR design, is pursuing greater plant availability by examining the impact of lifetime maintenance. As part of this effort digital technology has been systematically incorporated in the plant's control and protection systems. Application of this technology will allow operation for longer periods of time, compared to today's plants which generally use analog technology, without the need for instrument recalibration or routine maintenance. Portions of ABB CE's improved digital plant protection system, which will first be incorporated in the upcoming Oskershamm 1 upgrade followed by the initial startup of the Ulchin Units 5 and 6 in Korea, have been built at CE's works for verification testing, including seismic qualification.

Westinghouse, for its advanced AP600 plant design, has carried out both a Reliability, Availability and Maintainability Program (RAM) and a Design Reliability Assurance Program (D-RAP). The twin goals of these programmes are a design which meets or exceeds the stringent US NRC safety criteria and which also meets an ambitious availability objective of 90%. These programmes share the same equipment reliability databases but have remained separated

programmatically to ensure that plant safety is not compromised by availability improvement efforts.

In summary, utilities and vendors are, for new plants, placing the main emphasis first on building on accomplishments already achieved; i.e. taking operating experience into consideration, and second, employing new technologies. Formalized processes have been established to ensure information feedback and ways to assess it, e.g., by expert groups or panels. Availability and reliability data have been established for various systems and components in the plant based on analyses of operating experience and evaluation of possibilities for improvements. Some organizations use a more pragmatic and less formalized approach; operating experience is assessed by an expert group consisting of specialists in the different engineering disciplines involved. This group provides recommendations to the designers, after carefully evaluating and scrutinizing proposals for design changes to adapt to operating experience.

The more pragmatic approach centered upon an independent expert group which is capable of evaluating the importance of feedback information, as well as pros and cons of suggested design changes is a very useful method of decision making. Both the more formalized approach as well as the pragmatic approach are quite useful in achieving plant designs that will enable the utilities to operate and maintain their plants in an efficient, economic and reliable manner.

Directions for the Future

In a closing discussion period, the chair persons of the four technical sessions reviewed the key conclusions, and attendees provided comments and suggestions for future direction. The importance of maintaining and increasing focus on the current fleet of operating plants worldwide was emphasized. Good performance at these plants is needed as we go forward into the future. Many utilities have made good progress in reducing the length of refueling outages but there is a need to do better at dealing with forced outages. Current plants can benefit from the development work for advanced reactor designs, and it was suggested that utilities assign engineers to investigate application of advanced technologies, developed for future plants, to solving specific problems of current plants.

A distinction was drawn between technical issues and institutional or regulatory issues. On the technical side, greater use of risk-based inspections would provide a better focus on areas that are more prone to problems. On the institutional or regulatory side, more international co-operation could harmonize codes and standards that currently vary from country to country.

It was noted that the culture of the nuclear industry may have a tendency to stifle innovation. A large investment is required to develop, proof test and license new technologies and there are associated financial risks. On the other hand, without advancements, there is risk of becoming uncompetitive. Long held, deeply entrenched assumptions, should be examined to find more efficient and effective means of achieving performance and safety objectives. Other industries can provide guidance on ways to improve the nuclear industry's practices and to increase availability.

In summary, standardization is the key to future competitiveness. Technologies, such as advanced computing hardware and software, and artificial intelligence, proposed for new plants, should be incorporated where possible in today's plants. In this regard, there is a need for more extensive feedback and information exchange mechanisms. Above all, focus must remain on maintaining the already high level of reliability of current reactors while working to improve their availability.

XA9848561

OPENING ADDRESS

W.D. Magwood
Office of Nuclear Energy, Science and Technology,
United States Department of Energy,
United States of America

Introduction

I am very pleased to meet with you today to kick off what should be a very interesting and important set of discussions. I'd like to thank the IAEA and the Argonne National Laboratory staff for hosting this meeting because I believe that information exchange in conferences like this will help nuclear plant operators to meet the challenges of the future. Those challenges are clear and reflected in many of the discussions you will have over the course of this meeting. While complex to understand and address, the challenges facing nuclear energy are stark and clear at the bottom line. Nuclear power plants that are economic and reliable will be an energy source on which many countries will rely heavily for decades to come. Nuclear power plants that do not prove to be economic and reliable are likely to shut down before the end of their useful lives.

We are at a crucial crossroads in the history of nuclear power. Probably at no point since the advent of nuclear energy some four decades ago has there been so compelling a case for the world to invest in nuclear power technology. At the same time, we face several difficult challenges that must be addressed before we can expect nuclear energy to make a major contribution to the world's energy needs and address its environmental concerns. How the world operates its existing nuclear power plants today will largely determine whether any Nation will build and operate next-generation plants in the future. And increasingly, the technologies once intended for future

nuclear plants can play a vital role in keeping existing plants safe, competitive, and viable today.

At the Department of Energy, we are thinking about the future–more so than at any other time since I joined the agency three and a half years ago. Under the leadership of Secretary Peña, we are looking forward at the strategic energy needs of the Nation. We have asked the questions that everyone in the energy field must ponder as we approach a new millennium: How do we assure that we will have access to reliable supplies of economic energy in the future? How do we respond to environmental challenges such as global climate change? What technologies will we need in a world where the business of generating electricity is more like the soft drink business than the public utility infrastructure we have had for nearly a century? Can we afford to have nuclear power? Can we afford *not* to?

Over the next century, we expect that global energy use will increase significantly. The Energy Information Administration, EIA, predicts that worldwide energy consumption will grow by more than 50 percent over the next 20 years, with much of the growth coming in the developing nations of Asia. While in the past, I know that such projections have been found to overshoot reality by significant margins, today's EIA makes very progressive assumptions about the implementation of energy efficiency measures. Even with this built-in conservatism, EIA's projections indicate that the United States will need to build more than 280 gigawatts of new electric generating capacity by 2015 to meet growing demand and replace retiring power plants.

This will require a massive investment in new power plants. The paramount question for many of us is how many of these plants will be nuclear? The current outlook is not

encouraging. No new nuclear plants have been ordered in the U.S. since 1978 and recently, several utilities have decided to permanently shut down some of their nuclear plants because they are no longer economically viable in today's increasingly competitive electricity market. If this trend continues, it is possible that many of the remaining 108 operating nuclear power plants in the U.S. could be out of business before their current licenses expire.

Were this to occur, it would be to the detriment of our energy supply system. The nuclear power plants currently operating in the U.S. provide about 22 percent of the Nation's electricity and they represent an investment by ratepayers of more than $200 billion. These plants provide reliable baseload electricity in all weather conditions without emitting air pollutants such as those associated with global climate change. Nevertheless, economic and other factors have placed these plants–and the next-generation plants that could replace them–at great risk.

The Global Climate Challenge–Moving Toward Kyoto

One of the most important factors that has emerged over the last few years affecting the future of nuclear power is the arrival of global climate change as a high-priority issue in both the Administration and Congress. In June, the President formalized this new emphasis in national policy. In his address to the United Nations, President Clinton committed this country to reducing the emission of greenhouse gases. The President stated:

> *We will work with our people, and will bring to the Kyoto conference a strong American commitment to realistic and binding limits that will significantly reduce our emission of greenhouse gases.*

This is not simply a shift in U.S. priorities. This December, the nations of the world will gather in Kyoto, Japan for an international conference on global climate change. One of the likely outcomes of this international event is a binding agreement to reduce the annual emissions of greenhouse gases internationally to a specific level by a specific date. While existing international agreements encourage the reduction of each country's emissions to 1990 levels by the year 2010 remains the baseline, we do not yet know what will result from the Kyoto conference. But what we do know is that the targets will be binding.

How will the United States and other Nations respond to the establishment of such a far-reaching international agreement? This is the subject of intensive analyses throughout the Executive Branch, including the White House and especially the Department of Energy. The final shape of the U.S. strategy will most likely emerge over the next year; however, it would not be surprising to see market-based "cap and trade" mechanisms as central to our response–both on an international and national level. This mechanism worked extraordinarily well in implementing the Clean Air Act Amendments and that lesson will not be lost on policy decision-makers.

This sort of device is a macroscopic solution which does not address how we will reduce greenhouse gas emissions on the working level, in the course of everyday society, without hobbling economic growth. Here is where our implementation of a Kyoto treaty is at its most complex and challenging. And this is where the Department of Energy will play a vital role as we move closer and closer to Kyoto.

Efficiency–In the Broad Sense

To reduce greenhouse gas emissions in a relatively short period, that is, by 2010, any realistic strategy will be--by necessity--very conservative. While advanced technologies such as renewable energy, electric vehicles, or advanced light water reactors could have a tremendous impact on reducing carbon dioxide emissions in the longer term, it is very unlikely that any such technologies will play a large role in helping us meet our greenhouse gas reduction goals over the next decade. The measures that will be most important over the next decade can be characterized simply in terms of improvements in efficiency.

In the broadest sense, improving the efficiency of how the energy system converts energy resources to useful work and products is the only economic way to meet the commitments we expect from Kyoto. In this sense, efficiency can be segmented in the following ways:

- increasing the energy efficiency of our homes, businesses, transportation, and industry;
- increasing the efficiency of how energy is delivered to consumers; and
- increasing the efficiency of electricity generation.

The first set of actions is very familiar by now. The Department of Energy has invested billions over the last several years to develop and encourage the market acceptance of

energy efficient technologies such as advanced lighting, high-efficiency transportation systems, and ground-source heat pumps. Many of these technologies are mature enough to be sold on the market and the impact of capped greenhouse gas emissions may make these technologies more economically attractive.

The second set is largely the province of industry and would in any event be driven by the advent of competitive electricity markets. The Electric Power Research Institute, for example is developing the elements of a flexible AC transmission system and the Department is investing in technologies to improve the efficiency of gas transmission. These improvements will become increasingly important in the early part of the next century.

Finally, increasing the efficiency of electricity generation is a set of near-term actions that can be cost-effectively accomplished across many technologies. In the fossil fuel area, the Department has invested significant monies to develop "Clean Coal" technologies. Utilities are beginning to implement high-efficiency power plant technologies such as combined-cycle natural gas plants. They have also implemented efficiency improvements at nuclear power plants. There is a need, however, to do more.

Nuclear Energy is Part of the Solution

In the case of nuclear power plants, the United States has made impressive improvements over the last twenty years. Capacity factors have increased from an average of 57.6% in the U.S. in 1980 to about 80% today. The Department played a

role in some of this improvement–for example, by working with industry to develop high-burn-up fuel technology that allowed fuel cycles to increase from a typical 1970's 12 months to 18 and 24 months today. But much of the recent increase in capacity factors is the result of successful efforts by U.S. nuclear utilities to increase reliability and plant availability while at the same time reducing costs. Our industry friends are correct to be proud of their accomplishments–which were, as many of you know, not completed without considerable pain–but this is not the time to rest.

These past increases in plant reliability and availability have merely kept nuclear power in the race. They have not yet assured survival. Newly-competitive electricity markets linked with uncertainty associated with plant license renewal conspire to make life very difficult for all but the most efficient and best-run nuclear power plants.

If our nuclear plants can meet the challenge, they will prove to be a vital factor in meeting our international obligations. Every one percent fleet average plant capacity factor increase in U.S. nuclear plants equates to bringing a new 1000 MWe plant on-line. This helps address the energy need challenges I mentioned earlier and has obvious direct economic benefit to the owners of the plant. But the fact that has gained the attention of many of my colleagues in Washington is the fact that each one percent improvement in the average capacity factor for U.S. plants corresponds to an additional two million metric tons of CO_2 emissions that will be avoided each year. Importantly, key members of Congress such as Senate Energy and Natural Resources Chairman Frank Murkowski are now on the record as recognizing the importance of nuclear energy in our global climate change strategy. In a recent letter to the Department of

State in which he urged a more visible role for nuclear energy in plans to manage greenhouse gas emissions, Chairman Murkowski wrote:

> *Nuclear energy . . . is responsible for 89% of all CO2 emissions avoided by U.S. electric utilities between 1973 and 1995. Over 1.9 billion metric tons of carbon emissions have been avoided in the U.S. alone through the use of nuclear energy.*

As a result, the Department is interested in working with utilities to find ways to increase the efficiency of nuclear power plants. While for many plants, management issues and interactions with the Nuclear Regulatory Commission must be dealt with first, there are some important technology issues that must be addressed. For example, application of advanced instrumentation and control systems, in-service inspection, and other technological innovations can help us maximize the use of our existing plants to the benefit of the Nation and the global environment.

We believe that by the year 2010, the United States fleet average capacity factor should be no less than 85 percent. In accomplishing this, we will see a more competitive and viable nuclear power industry, set the stage for implementation of next-generation nuclear power plants in the next century, and have a dramatic impact on carbon emissions.

Whereas existing nuclear plants have a large impact on carbon emissions in the years leading to 2010, they become invaluable in the years following 2010. If just the existing U.S. plants continue to operate to the end of their initial license periods (the last of

which would expire in 2035), the U.S. will avoid emissions of more than 3 billion metric tons of carbon compared to what would occur if coal-fired plants were used instead. The impact is magnified if many of these plants receive renewed licenses. In addition, next-generation plants could be a singular factor in controlling carbon emissions in the longer term, particularly if energy efficiency gains flatten and become less economic over time and gas supplies become more expensive.

Issues Affecting the Future

There are important issues that will come into play as we consider not simply maintaining, but *expanding* the world's use of nuclear energy. Many of them are very well known. Foremost, we must deal effectively with the high-level and low-level waste issues. These are complicated as technical issues but even more complex as political issues. Unless they are dealt with, the construction of new nuclear plants and perhaps the long-term operation of existing plants will become increasingly problematic.

While I am not here today to debate about the Department's high-level waste program, I will say that a part of the solution may be to make less waste. The Department has been working with Electric Power Research Institute and others in the industry to develop a joint Spent Fuel Minimization program. This technology activity would pick up where our high-burn-up nuclear fuel program left off in the early 1980's. We have proposed the development of advanced nuclear fuel technologies which could see burn-ups increase to 100,000 megawatt days per metric ton. This is an ambitious target, but we believe it is possible and in reach of a cooperative venture.

We will continue to work to open new markets to U.S. nuclear technology companies, especially in the growing markets of Asia. Many countries in the region expect to turn to nuclear power as a key component of their future energy mix. They have many reasons for this, including energy independence and the desire to establish advanced technology infrastructures. But as we consider nuclear trade with developing countries, we must also deal with concerns over the proliferation of nuclear technology and nuclear materials as more developing countries build and operate nuclear power plants. Improved nuclear safeguards and monitoring, and proliferation resistant technologies will be necessary to reduce risks throughout the world as developing nations build nuclear plants. IAEA Director General Hans Blix has echoed these concerns in several of his speeches over the past few years. For the longer term, the Department is interested in investigating advanced proliferation-resistant nuclear power and fuel technologies that could significantly reduce proliferation risks.

We also remain committed to addressing issues such as the vital, strategic need we all have to assure high levels of nuclear safety in all countries. One of our most important programs over the last several years has been our effort to increase the safety of nuclear plants in the former Soviet Union and Central and Eastern Europe. Another "Chornobyl" in one of these countries would not only be a major political and humanitarian disaster, but it would be a disaster for the nuclear utilities and technology companies throughout the world. Some progress has been made by the international community to address this challenge, but a great deal remains to be done.

Finally, the Department is concerned over the state of the U.S. nuclear technology infrastructure. Experienced personnel and valuable facilities in both the government

sector and industry are aging with limited prospect of replacement. This is not just a problem in the U.S.; it is an international problem. We have been trying to address part of the problem at DOE by investing more in university nuclear engineering programs and encouraging new missions for our irreplaceable research and test reactors and hot cells. In today's budget environment, however, this has been exceedingly difficult.

Conclusion

To close, I believe that these challenges--significant as they are--are certainly within our ability to overcome if we work together. Government, industry, and universities all have much at stake in assuring a viable nuclear energy option in the future. The United States must work with other nations to address issues of trade, proliferation, and nuclear safety while fostering an invigorated environment for international technology collaboration. As this conference proceeds, I encourage you to look for ways of enhancing cooperation across all sectors of society and across all oceans of the world.

The work starts here--and at each individual nuclear power plant. There will be a limited future for nuclear power unless existing plants prove that the technology is economically competitive. We know it can be done because many of you are doing it and helping to point the way to a healthier global environment in the process. If we are successful in first maintaining the nuclear energy option, then--having dealt with the issues I have mentioned today--expanding our use of it in the future, the potential of nuclear energy will be fully realized to the benefit of all the world's peoples.

NEXT PAGE(S)
left BLANK

POLICIES, PRACTICES AND PROCEDURES FOR ACHIEVING HIGH RELIABILITY AND AVAILABILITY

(Session 1)

Chairman

J. HERCZEG
United States of America

NEXT PAGE(S) left BLANK

XA9848562

AVAILABILITY ANALYSIS OF UNITED STATES BWR IV ELECTRICAL GENERATION PLANTS*

D.H. RENICK, F. LI, N.E. TODREAS
Department of Nuclear Engineering,
Massachusetts Institute of Technology,
Cambridge, Massachusetts,
United States of America

Abstract

Availability, as quantified by power output levels, from all active U.S. BWR IV plants were analyzed over a seven and a half year period to determine the operational characteristics of these plants throughout an operating cycle. The operational data were examined for infant mortality, end of cycle decreased availability, and seasonal availability variations. Scheduled outages were also examined to determine the industry's current approach to planning maintenance outages. The results of this study show that nuclear power plants do suffer significant infant mortality following a refueling outage. And while they do not suffer an end of cycle decrease in availability, a mid-cycle period of decreased availability is evident. This period of decreased availability is due to a combination of increased forced unavailability and seasonally scheduled maintenance and refueling outages. These findings form the start of a rational approach to increasing plant availability.

1. INTRODUCTION

This study was conducted as part of an ongoing study at the Massachusetts Institute of Technology to examine the forced unavailability of nuclear power generation facilities. This research has been performed under the funding and sponsorship of INEEL.

2. DATA ANALYSIS TECHNIQUE

2.1. Capacity Factor

The purpose of this study was to examine plants operational availability during a refueling cycle and how the availability relates to the capacity factor. In general, the capacity factor, defined as the ratio of the actual electrical energy produced to the theoretical electrical energy which could have been produced over a given time period, is defined by the following equation:

$$\textbf{Capacity Factor} = \frac{\textbf{MWe output}}{\textbf{MWe theoretical}} \qquad (1)$$

The time period used for this study is an operating cycle which is defined as:

$$\textbf{Operating Cycle Length} = \textbf{Refueling Outage Length} + \textbf{Refueling cycle Length} \qquad (2)$$

The capacity factor during an operating cycle then is given by:

$$\textbf{Capacity Factor} = \frac{(\textbf{Refueling Cycle Length}) \times (\textbf{Refueling Cycle Availability})}{(\textbf{Refueling Cycle Length}) + (\textbf{Refueling Outage Length})} \qquad (3)$$

*This project has been funded by the INEEL University Research Consortium. The INEEL is managed by Lockheed Martin Idaho Technologies Company for the US Department of Energy, Idaho Operations Office, under contract No. DE-AC07-94ID13223.

where

$$\textbf{Refueling Cycle Availability} = \frac{\textbf{MWoutput}}{\textbf{MWrated}} \text{ or}$$

$$= \textbf{percentage of maximum power output}$$

The operating cycle capacity factor depends on three factors: refueling cycle availability, refueling outage length, and refueling cycle length. The independent effect of these three variables on capacity factor is shown in Fig. 1 for assumed changes in refueling cycle availability from 89% to 97%, refueling outage from 78 days to 30 days, and refueling cycle length from 18 months to 24 months. The zero point reference capacity factor in Fig. 1 of 77.25% is an average of U.S. BWR IV plants from 1990 through May, 1997. Notice that the operating cycle capacity factor goes from 77.25% to 84.65% when availability increases, to 83.80% when the refueling outage is reduced and to 80.10% when the refueling cycle is extended.

Increasing the availability during the refueling cycle gives the greatest gains. However U.S. refueling cycle availability performance has been historically low. Although decreasing the length of the refueling outage gives nearly the same gain in capacity factor, there are intensive industry efforts to reduce it already underway. Hence, refueling cycle availability and refueling cycle length are investigated further. First, the method of analysis is presented.

2.2. Plant Availability Data

Operating data from all U.S. BWR IV plants were examined from January, 1990 through May, 1997. All U.S. BWR IV plants were included in the study with the exception of Shoreham, which was decommissioned in 1987, and Brown's Ferry 1 and 2 which were shutdown for the majority of the time period. Of the remaining 17 plants, the time period which encompassed the long NRC-imposed shutdowns for Brunswick 1, Brunswick 2, and Cooper Station were ignored.

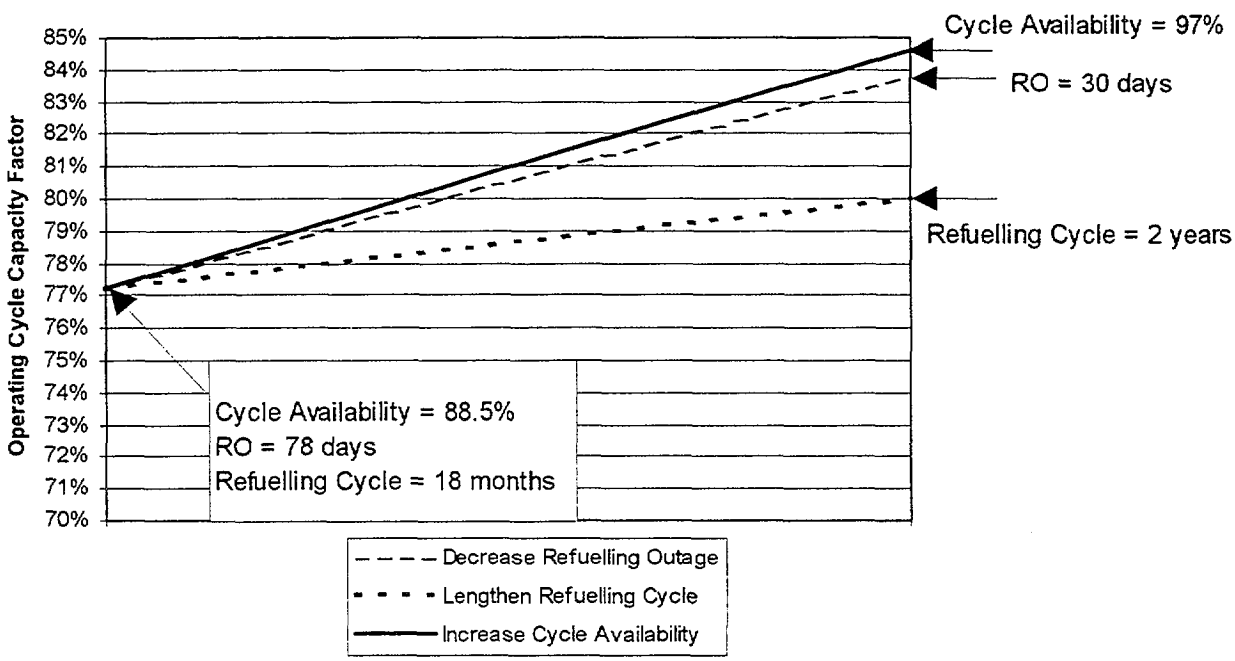


FIG. 1. How the Operating Cycle Capacity Factor changes by independently varying refueling cycle length, refueling cycle availability, and refueling outage length.

The daily refueling cycle availability was derived from NRC monthly "gray book" data [1]. The gray book data lists, for each plant, the daily average power output by the plant for the 24 hour period. The daily average power outputs were transformed into a daily percentage of maximum power output, or daily availability. Then the plant data were split into refueling cycles, rather than months. It was then necessary to re-align the refueling cycles such that all plant data were examined for beginning of cycle and end of cycle performance.

2.3. Refueling Cycle Availability Analysis

All refueling cycle starts were aligned by calling the first day of the refueling cycle for each plant day "1". As shown in Fig. 2, the refueling cycles were "left- justified" by aligning the first day of each refueling cycle. A vertical average at any given day during the refueling cycle gives the average availability for all plants on that day of the refueling cycle. This method accurately accounts for the performance of each plant during the beginning of a

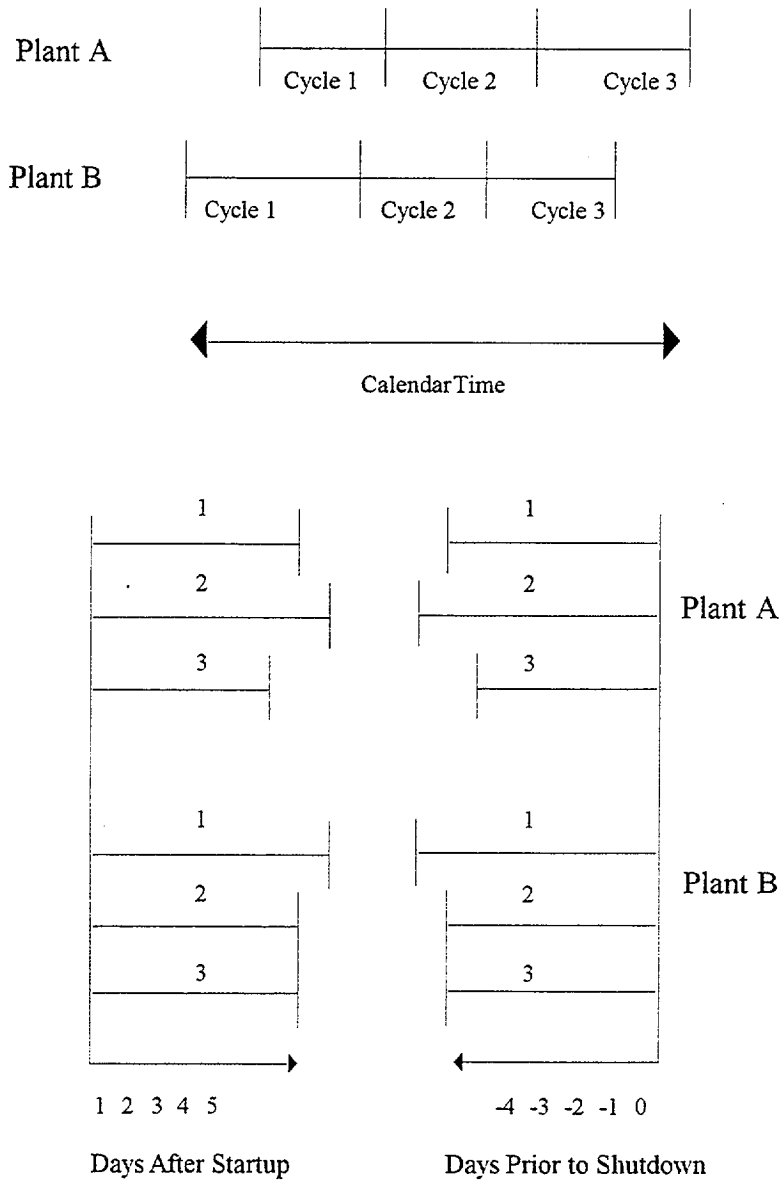


FIG. 2. Sample data which shows how refueling cycle data was transformed from calendar time to a time scale based upon the number of days after the start of the refueling cycle and the number of days before the plant shutdown for the following refueling outage.

refueling cycle. In a second analysis, the refueling cycles were "right- justified" such that the refueling cycles end on the same day. This method is used to show the availability of every plant during the end of the refueling cycle.

3. US BWR IV PLANT START OF REFUELING CYCLE AVAILABILITY

3.1. Availability at the Start of a Refueling Cycle

Fig. 3 presents the daily and cumulative availability for "left-justified" data. In Fig. 3, day 1 along the x-axis represents the average availability of all U.S. BWR IV plants on the first day of the refueling cycle. Notice that daily availability is significantly depressed during the beginning of the refueling cycle. This effect can be directly attributed to infant mortality, which is defined as early failures in a system where the failure rate decreases with time [2]. While infant mortality is usually only applied to single component failures, in an assembly of many components the entire assembly, in this case the plant, exhibits infant mortality as the collective effects of individual components performance. The depression in daily availability corresponding to an increase in forced unavailability which occurs mid-cycle between days 210 and 390 will be examined in detail later.

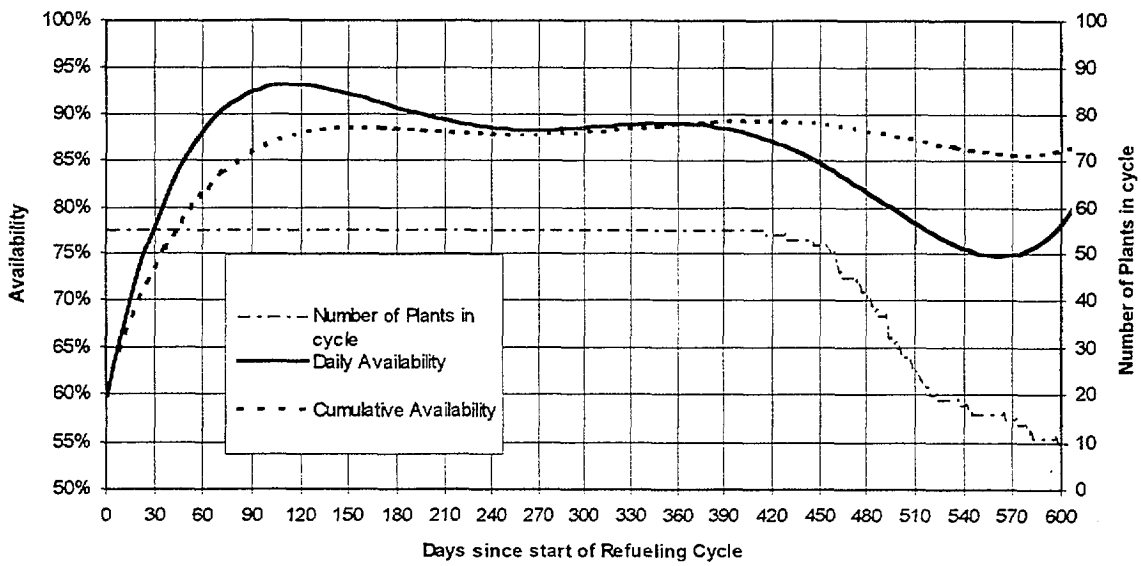


FIG. 3. The average of all BWR IV plant's daily and cumulative availability during a refueling cycle. The bottom line shows the number of plants not in a refueling outage -- as plants shutdown for a refueling outage this line drops accordingly.

The bottom line of Fig. 3 shows the number of plants still in-cycle. When a plant enters a refueling outage the number of plants in cycle represented by the bottom line drops, and the that plant is no longer considered in the industry average. Thus the daily availability near the end of the refueling cycle on the right hand side of Fig. 3 is not indicative of all plants near the end of the refueling cycle since there are fewer plants remaining in-cycle. Also, this segment of data may be skewed downwards as most plants experience some degree of end of cycle coastdown. When a plant starts the next refueling cycle, its availability is restarted at day 1.

The cumulative availability at any day contains the history of all of the daily availabilities preceding that day. The equation for cumulative availability is given by

$$\text{Cumulative Average at time T} = \frac{1}{T}\int_0^T [\text{DailyAvailability}(t)]dt \quad (4)$$

When equation (4) is discretized, it becomes:

$$\text{Cumulative Average at time T} = \frac{1}{T}\sum_{i=1}^{T} (\text{Daily Availability})_i \quad (5)$$

3.2. Effect of Eliminating Infant Mortality

A plant that eliminates infant mortality will see a significant increase in refueling cycle availability, and hence an increase in capacity factor. To show this, the first 120 days of daily availability data shown in Fig. 3 were parametrically increased to constant values between 87% and 100% . The BWR IV average refueling cycle length of 540 days was used for the rest of the calculation. Fig. 4 shows how this artificial boost in performance increased the operating cycle capacity factor by increasing the refueling cycle availability.

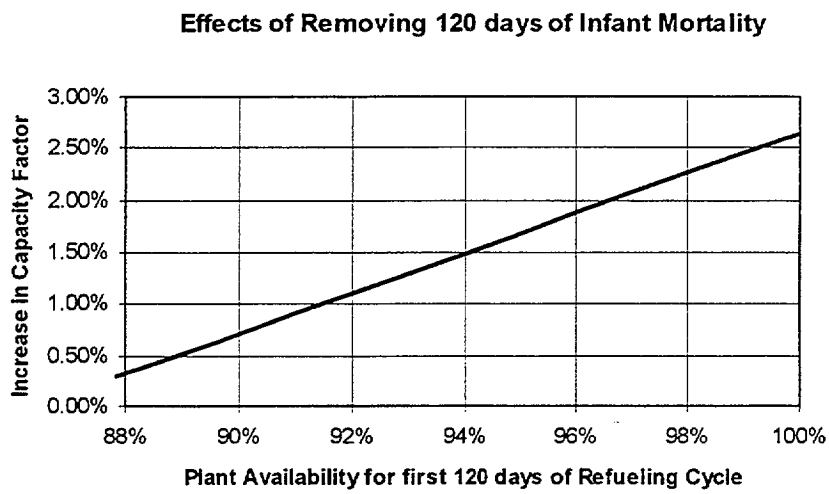


FIG. 4. By artificially setting the daily availability to different values over the first 120 days of the refueling cycle, the refueling cycle availability increases, which equates to increased operating cycle capacity factor.

4. US BWR IV END OF REFUELING CYCLE AVAILABILITY

4.1. Availability at the End of a Refueling Cycle

As previously stated, the data in Fig. 3 are invalid near the end of the refueling cycle. Therefore, the so-called "right- justified" analysis was used to accurately portray how each plant operates at the end of the refueling cycle. The coastdown effect was removed from the data by matching the maximum power output level reported in the NRC database to the daily power output level. All outages and major power reductions were left in the data. In this manner, plant availability was not unduly decreased due to core life, but was decreased due to operating casualties and outages. Fig. 5 shows the resulting daily availability.

Fig. 6 amplifies a portion of Fig. 5 and shows the daily availability data of every BWR IV plant over the last 180 days of each plant's refueling cycle. The cumulative availability curve shown in Fig. 6 was derived by subtracting 180 days from the average refueling cycle length of 532 days, and finding the cumulative availability at the 352nd day of the refueling cycle from the "left-justified" data in Fig. 3. The cumulative availability for the first 352 days of operation is 88.72%, and the cumulative availability during the final 180 days is found using equation 4 by combining the first 352 days of operation from Fig. 3 and the last 180 days of operation from Fig. 6. Using this method, the cumulative availability for the last 180 days of

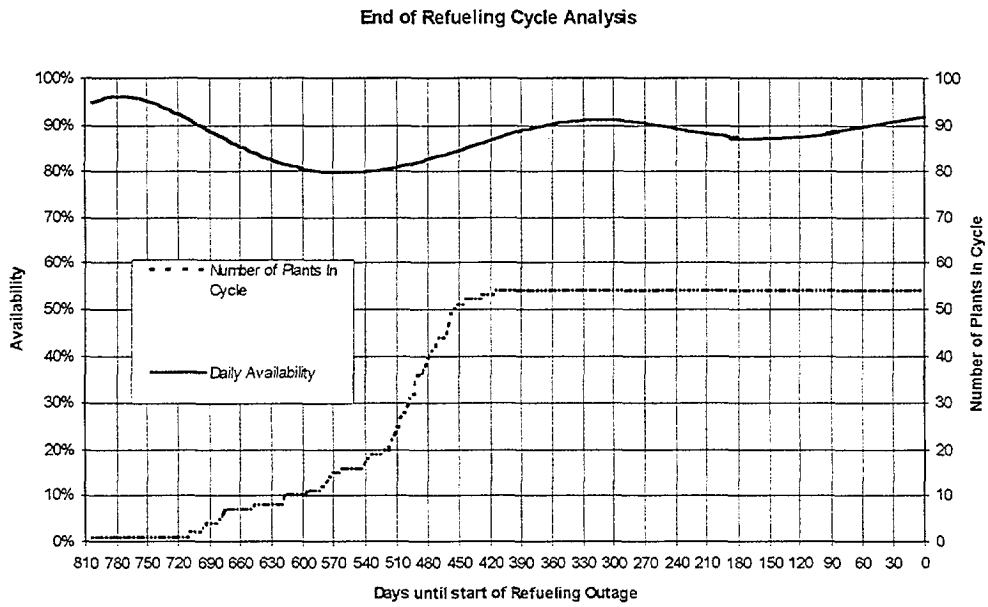


FIG. 5. The average of all BWR IV plant's daily availability using a "right-justified" alignment whereby all plants finish the refueling cycle on the same day, day 0.

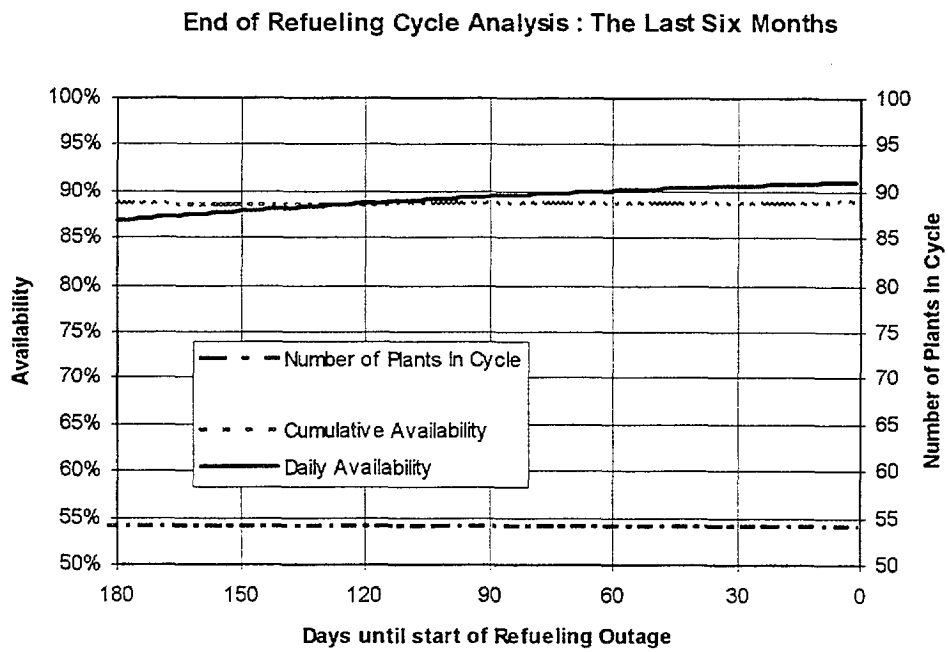


FIG. 6. Daily and Cumulative availability for all plants during the last 180 days of the refueling cycle. Note how the daily availability curve is higher than the cumulative availability curve.

operation contains the beginning of cycle history. It is significant to note that over the last four months of operations, the daily availability curve is greater than the cumulative availability. This means that the plants are operating better at the end of the refueling cycle than previously. This increase in performance may result from the mid-cycle availability decrease. That is, equipment breakdowns occur in the middle of the refueling cycle and not at the end of the refueling cycle. Significantly, for the cycle lengths examined, the mid-refueling cycle breakdown period is not followed by a subsequent breakdown or wear out period prior to the plants shutting down. A plant with an extended core could sustain the higher level of performance seen in the end of cycle period and increase availability and capacity factor.

Extending the refueling cycle length will increase the refueling cycle availability if it is assumed that the daily availability remains higher than the cumulative availability. This is a reasonable assumption based on a case study conducted at M.I.T. with a BWR IV plant [Brodeur, 1997] which showed that less than 20% of component failures are age related. Another M.I.T. study [Moore, 1996], showed that specific components, such as the main feedwater pump, are not age limited. Furthermore, this assumption is supported by the recent decision to operate British Advanced Gas Reactors which refuel on-line on three year operating cycles. If the refueling cycle is artificially extended 180 days to 2 years, and the daily availability during the extended 180 day period is maintained at 90.7% (the availability on the last day of actual refueling cycle operations), the cumulative and daily availability can be plotted as shown in Fig. 7.

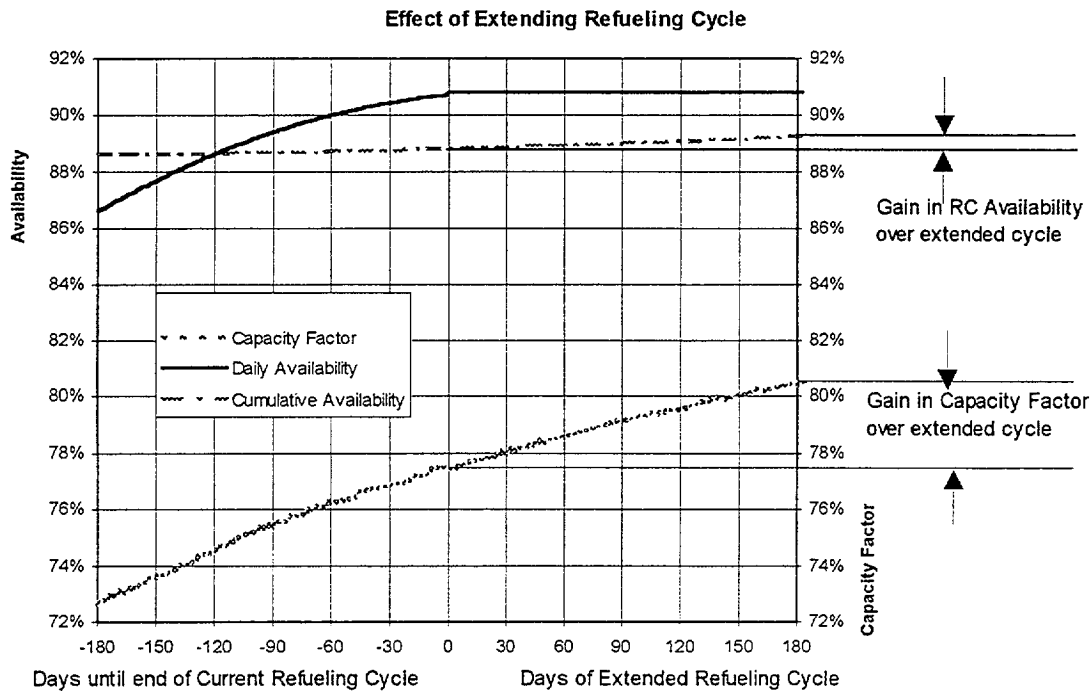


FIG. 7. The refueling cycle here is artificially extended 180 days, and the daily availability is set to 90.7%. Notice that the cumulative availability increases since the daily availability is always higher. The increase in cumulative availability corresponds to an increase in refueling cycle availability, which leads to the increase in operating cycle capacity factor.

Here the cumulative availability includes the first 352 days of operations from the "left-justified" data, the final 180 days of availability from the "right-justified" data, and the artificial availability from the extended data.

Fig. 7 shows that the refueling cycle availability increases 0.75% due to the high daily availability achieved in the extended operational period. Since capacity factor depends upon both refueling cycle availability and refueling cycle length, there is a non-linear increase in capacity factor with an extended refueling cycle. The capacity factor increases 2.80% with extended refueling cycle. This non-linear relationship is the basis for an economic advantage to extending the current 18 month refueling cycle.

The preceding paragraphs have shown that eliminating infant mortality and extending the length of the refueling cycle can increase the operating cycle capacity factor. The large dip in daily availability in the middle of the refueling cycle shown in Fig. 3 must be explained to complete the discussion of refueling cycle availability.

5. US BWR IV PLANT MID-CYCLE REDUCED AVAILABILITY

5.1. Mid-cycle Daily Availability Dip

The mid-cycle dip in daily availability is due to a mix of seasonally scheduled maintenance and an increase in forced unavailability. The seasonal effects are shown by re-examining the daily availability using the original calendar time scale. Instead of finding the daily availability as a function of the number of days since the start of the refueling cycle, this analysis yields the daily availability as a function of calendar day.

5.2. Seasonal Effects upon Daily Availability

Fig. 8 shows the monthly availability for U.S. BWR IV plants. While the data deviate greatly, there are relative peaks during the heavy demand, late summer and winter periods and reduced availability during the lesser demand spring and fall months. This pattern suggests that perhaps plants are taking a scheduled maintenance outage prior to and following the summer months. This hypothesis is confirmed by plotting in Fig. 9 the percentage of plants in a scheduled outage status. There are a significant number of scheduled outage days in March,

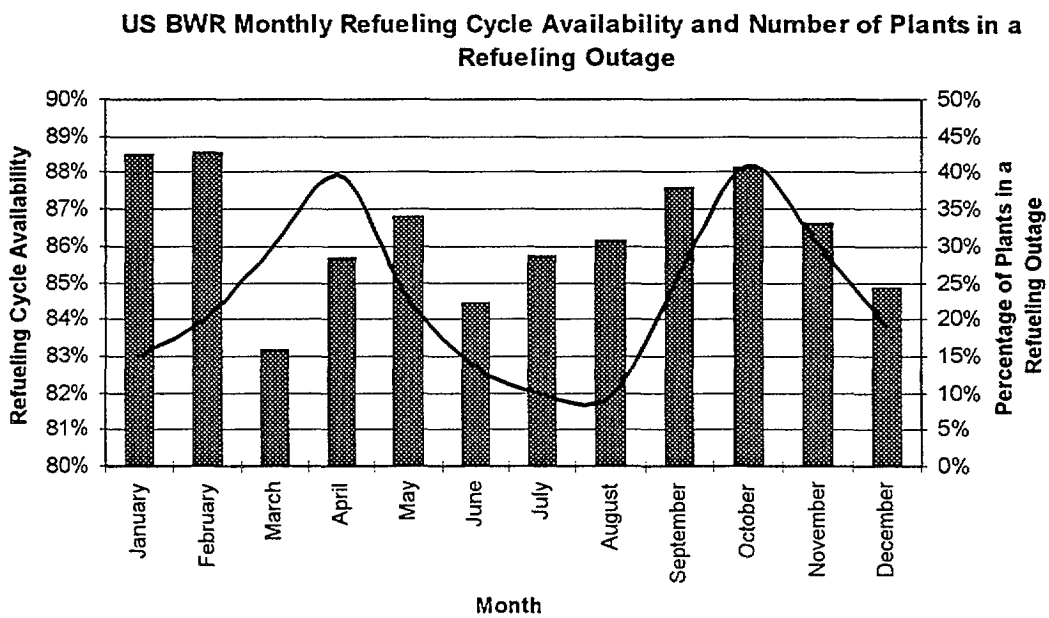


FIG. 8. The bars show the monthly variation in availability for U.S. BWR IV plants. Notice the high peak during the late summer, early fall months and winter months. The line corresponds to the percentage of plants in a refueling outage. Notice that it takes 4 to 6 months for availability to peak after plants come out of the refueling outage.

April, November, and December, and very few scheduled outage days from May through September. The availability dip in June can not be explained as being due to scheduled outages: even when full power days lost to scheduled outages occurring in June are added to the monthly availability of Fig. 8, the resulting availability is significantly below May. Rather than scheduled outages, the low availability in June is due to infant mortality. As the line which shows the percentage of plants in a refueling outage status decreases in Fig. 8, plants are exiting the refueling outage and starting a refueling cycle. Notice the high number of plant starts in April and May, which drive the availability low in June, and low in July and August relative to the higher performance of September and October. The same is true for the high number of plant starts in October and November, which drive availability low in November and December.

5.3. Increased Forced Unavailability in the middle of the refueling cycle

Not all of the decrease in mid-refueling cycle availability is due to seasonally planned maintenance outages and infant mortality. Some of this decrease is due to an increase in forced unavailability during the middle of the refueling cycle. This effect is shown by removing all scheduled outages from the refueling cycle data, and examining the data along a refueling cycle axis, similar to Fig. 3.

The results, shown in Fig. 10, still show the dip in daily availability in the mid-cycle time period. This suggests that plants are suffering a period of increased forced unavailability, and are forced to shutdown to fix problems. Fig. 10 also shows that scheduled outages are evenly distributed throughout the refueling cycle, and are not being heavily utilized to overcome the mid cycle increase in forced unavailability.

5.4. Implications of Seasonal Maintenance on Capacity Factor

Seasonally-adjusted planned maintenance can be used to offset the effects of mid-cycle increased forced unavailability. The first benefit of planned maintenance is that plants undergo less traumatic infant mortality following a planned maintenance outage. Fig. 11 compares the daily availability following a scheduled outage compared to the daily availability following a

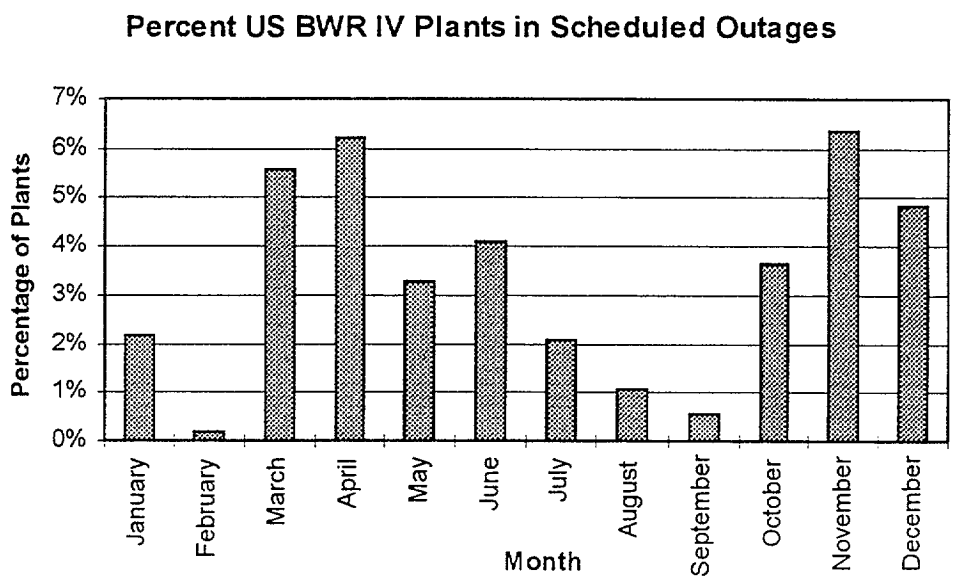


FIG. 9. Monthly variation in the percentage of plants in a scheduled outage status. Notice the large peaks in spring and late fall. The large increase in June is unexplainable.

refueling outage. Notice that the infant mortality period following a scheduled outage is not as prolonged or pronounce as that following a refueling outage. Second, planned, conditional maintenance could reduce the incidence of forced outages during the middle of the refueling cycle. Third, as a plant reduces the forced unavailability, and plans for outage periods, fuel usage can be optimized to match the economic benefits of operating during peak demand periods, and the coastdown period can be optimized. And finally, a plant that plans outages is in control of the outage, and not being controlled by the outage.

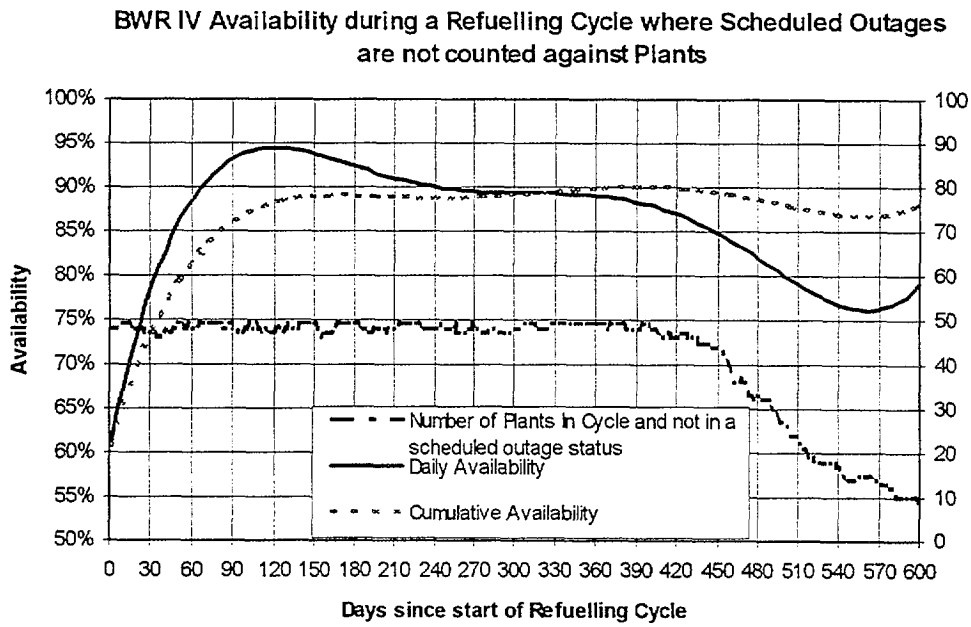


FIG. 10. Daily availability during the refueling cycle with schedule outages removed. If the mid-cycle dip in daily availability had been due purely to seasonal scheduled outages, the daily availability would have remained flat. The fact that the dip persists suggests that plants suffer a mid-cycle increase in forced unavailability.

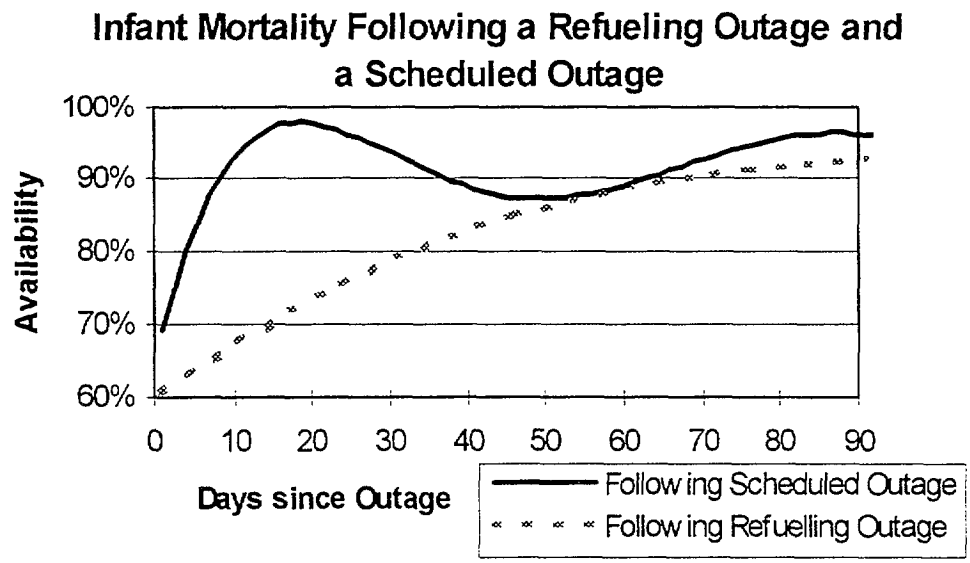


FIG. 11. Daily Availability following a scheduled outage and following a refueling outage. Notice that the infant mortality following a scheduled outage is much less severe (in magnitude and length of time) than the infant mortality following a refueling outage.

6. CONCLUSIONS

6.1. Conclusions and Recommendations for Improved Availability

This paper showed how the operating cycle capacity factor is affected by refueling outage length, refueling cycle length, and refueling cycle availability. Refueling cycle availability is affected by infant mortality, seasonally-adjusted scheduled maintenance outages, and forced outages. Increasing refueling cycle availability to 97% can increase operating cycle capacity factor over 7%. This goal can be realized:

(1) Reducing the forced unavailability following a refueling outage. Elimination of infant mortality leads to a 2.5% gain in operating cycle capacity factor as shown in FIG. 4.

(2) Implementing conditional, seasonally-planned maintenance. While scheduled outages occur seasonally as shown in Fig. 9, they do not occur at strategic times within the refueling cycle to prevent increases in forced unavailability, as seen from Fig. 10. A rational maintenance outage can reduce forced unavailability by fixing equipment before it breaks, and at a time that is economically convenient for the plant. Scheduling outage time also allows for better core life planning.

(3) Seeking extended refueling cycles through new, longer core designs. Operational data show that the balance of plant will not reduce availability if core life is extended. Rather, high availabilities would be maintained which would non-linearly increase capacity factor. Fig. 7 shows this beneficial, non-linear increase.

REFERENCES

[1] United States Nuclear Regulatory Commission Monthly Operating Report for United States Nuclear Facilities, 1989-1997

[2] RAMAKUMAR,R., *Engineering Reliability: Fundamentals and Applications*. Prentice Hall, New Jersey (1993) 482 pp.

Addendum to "Availability Analysis of United States BWR IV Electrical Generation Plants" by D. H. Renick, F. Li and N. E. Todreas

by, D. L. Brodeur, Department of Nuclear Engineering, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139

This addendum is attached to modify the findings of the attached paper. These new insights are the results of continued research in the area of BWR/IV US nuclear power plant reliability. Detailed findings are presented in MIT report to INEEL, "A Study of US Nuclear Power Boiling Water Reactor, Class IV, Operating Performance, 1992-1997" by David L. Brodeur and Virginia T. Angus. Reporting inconsistencies in the daily average power data used for the original paper were noted and overcome by establishing the maximum generation for any plant within an operating cycle as 100% capacity. Additionally the time frame of the study was restricted to five and a half years, January 1992 to June 1997, to reflect more current operating trends.

Figure 3A portrays the same information as Figure 3 of the paper using the refined data. The daily mean capacity data has been shown in addition to the fitted curves. It is noted that the mean daily capacity for the first seven days is discontinuous with that of the remainder of the operating cycle. For the first seven days the mean daily capacity increases linearly from zero to eighty five percent. After day seven the mean capacity is much more random exhibiting the impact of individual plant failures. The linear response during the first seven days can be attributed to the lengthy process of power accession and testing following the refueling outage. The thin 21 day moving average line has been added to observe the changes in daily mean capacity. It is a connection of the daily mean capacities for the first seven days and an expanding 21 day average after day seven. The average expands such that day nine is a three day average, day 10 a five day average up to day 18 and greater when the average is held at 21 days. The heavy solid line is then a sixth

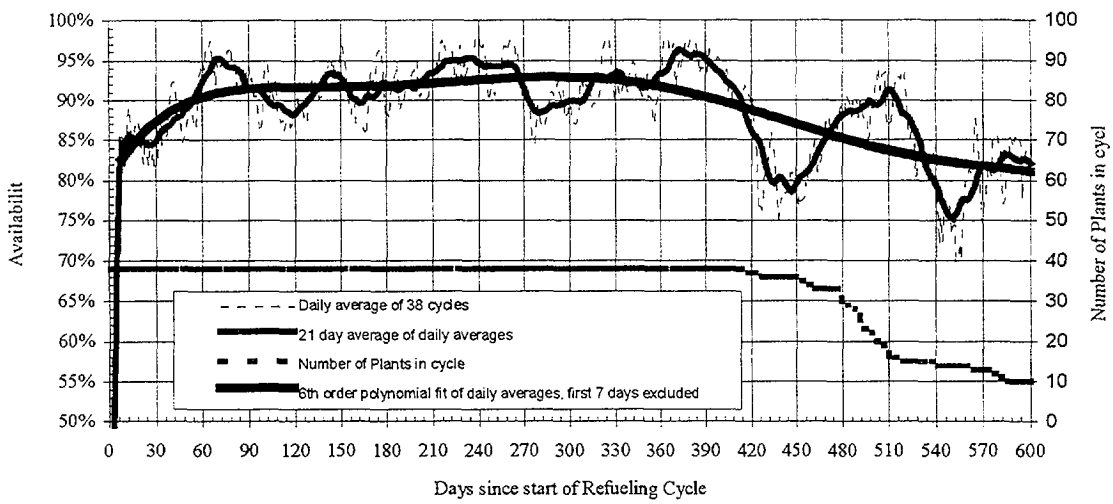


Figure 3A. The average of all BWR/4 plant's daily and cumulative availability during a refueling cycle. The bottom line shows the number of plant operating cycles averaged – as plants shutdown for a refueling outage this line drops accordingly.

order best fit of the 21 day average data. It is observed that this line is a good fit to the daily mean capacity data. This line replaces the solid line of figure 3 in the original paper and is representative of the daily capacity.

There are four regions noted of daily mean capacity performance. As discussed earlier during the first seven days capacity is linearly increasing from 0 to 85%. This is attributed to the start up process and not plant reliability failures. From day eight to day 90 the mean daily capacity is observed to increase from 85% to 92%. This is attributed to early cycle plant failures, the infant mortality reported in the original paper. Note that this is an observable but small effect. From day 90 until day 330 mean daily capacity is noted to be relatively constant at 92%. This period marks the optimum mid-cycle operating period. After day 330 the mean daily capacity is observed to steadily decline.

Of significance, the large period of decreased early cycle capacity, reported earlier as infant mortality, has been much diminished. The cumulative cycle performance is observed to slowly climb to greater than 90% during the mid-cycle period of steady performance. The end of cycle declining daily capacity is observed to drag the cumulative capacity down to below 80% by day 600. The lesser impact of the early cycle decreased performance is noted by the proximity of the cumulative capacity to the mean daily capacity by the end of the mid-cycle plateau (92 versus 90%). In comparison, the entire cycle cumulative capacity falls by greater than 10% as a result of the constantly declining end of cycle performance. As noted in the original paper, it is unclear whether this declining performance is the result of the end of cycle fuel coast down or declining plant reliability.

To examine the end of cycle performance the mean operating cycle data is again examined in a right justified manner, similar to the original paper. The daily capacity reported by plants has been carefully modified to reflect the percentage of power that could be generated as limited by fuel coast down. The heavy line of figure 5A is a third order best fit curve of the mean daily coast down modified capacity. The other points and

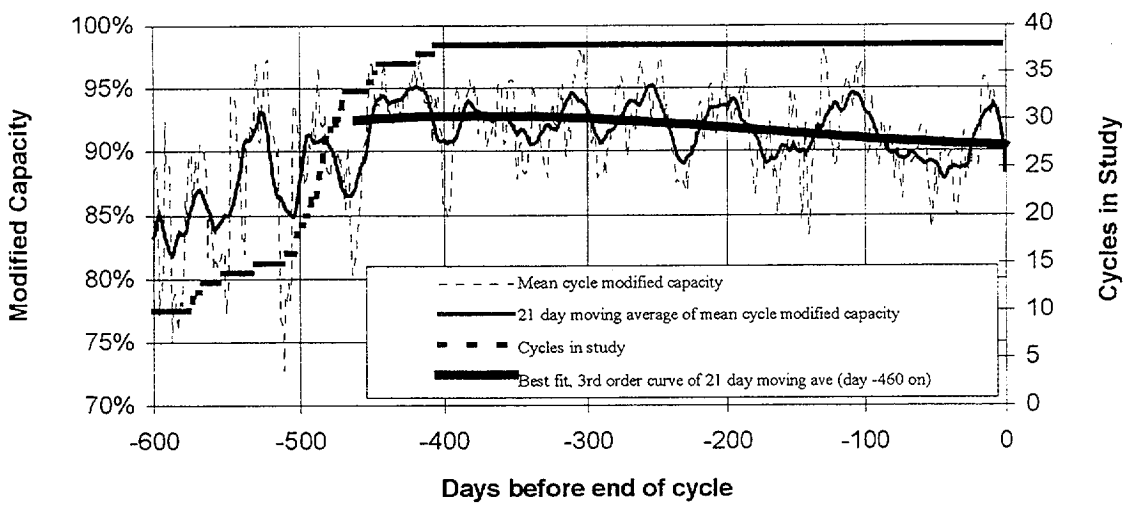


Figure 5A. The average of all BWR/4 plant's daily modified capacity using a "right justified" alignment whereby all plants finish the operating cycle on the same day, day 0.

curves are similar to those of figure 3A. It is noted that the capacity, modified to remove the effects of coast down, slowly declines in performance from 92.5% 460 days before the common end of cycle point to 90% by the end of cycle. This degradation is not as significant as the fuel coast down effects but does reflect an increasing difficulty of plant reliability with increasing cycle length. This finding is contrary to that of the attached paper.

The observations noted in this paper resulted from a detailed examination of each cycle's data and from a requirement that raw data be plotted along with fitted curves. For this reason the above figures contain the raw data, averaged data and then fitted curves. A lesson has been learned to cautiously view fitted curves for which the raw data is no longer visible.

XA9848563

AN INTEGRATED RELIABILITY MANAGEMENT SYSTEM FOR NUCLEAR POWER PLANTS

T. KIMURA, H. SHIMOKAWA, H. MATSUSHIMA
Nuclear Power Plant Reliability Program Department,
Hitachi Ltd,
Ibaraki, Japan

Abstract

The responsibility in the nuclear field of the Government, utilities and manufactures has increased in the past years due to the need of stable operation and great reliability of nuclear power plants. The need to improve the reliability is not only for the new plants but also for those now running. So, several measures have been taken to improve reliability. In particular, the plant manufactures have developed a reliability management system for each phase (planning, construction, maintenance and operation) and these have been integrated as a unified system. This integrated reliability management system for nuclear power plants contains information about plant performance, failures and incidents which have occurred in the plants.

1. Introduction

The first light-water nuclear power plant in Japan began commercial operation in 1970. Thereafter, the number of units has increased gradually and, as of Aug. 1997, 51 units were in operation with a power generating capacity of 45 million kW, representing approximately 20% of the total generating capacity in Japan. Their average capacity factor has stabilized above 70%, and it was above 80% in fiscal 1995 and 1996 , representing approximately 33% of the total Japanese electric power supply. Electric power supply from nuclear power will continue to increase in the future.

Against this background and with a move toward more stable operation and greater reliability of nuclear power plants, the responsibility of plant manufacturers has increased. As a nuclear power plant manufacturer, Hitachi has continually broadened its development of plant reliability through the entire lifetime of a plant, including the planning, design, fabrication, operation and maintenance stages. We strive to improve the reliability not only of new plants but also of those now running. This is done by performing analysis and design review (DR) in the planning and design stages on the one hand, and trouble recurrence prevention and reflection of actual trouble in the operating plants (called horizontal application) on the other.

This paper outlines our integrated reliability system and its associated applications for nuclear power plants developed by Hitachi.

2. Flow of ensuring the reliability of a nuclear power plant

2.1 Outline of quality assurance activities in Japan

As the number of nuclear power plants increases, both the importance of the role of nuclear power in the total power generation and the national demand for safety are rising. To satisfy these needs, the government, utilities and manufacturers are working on enhancing reliability. As a result, in Japan, the plant capacity factor has risen as shown in Figure 1 and unscheduled forced outages has decreased. Since

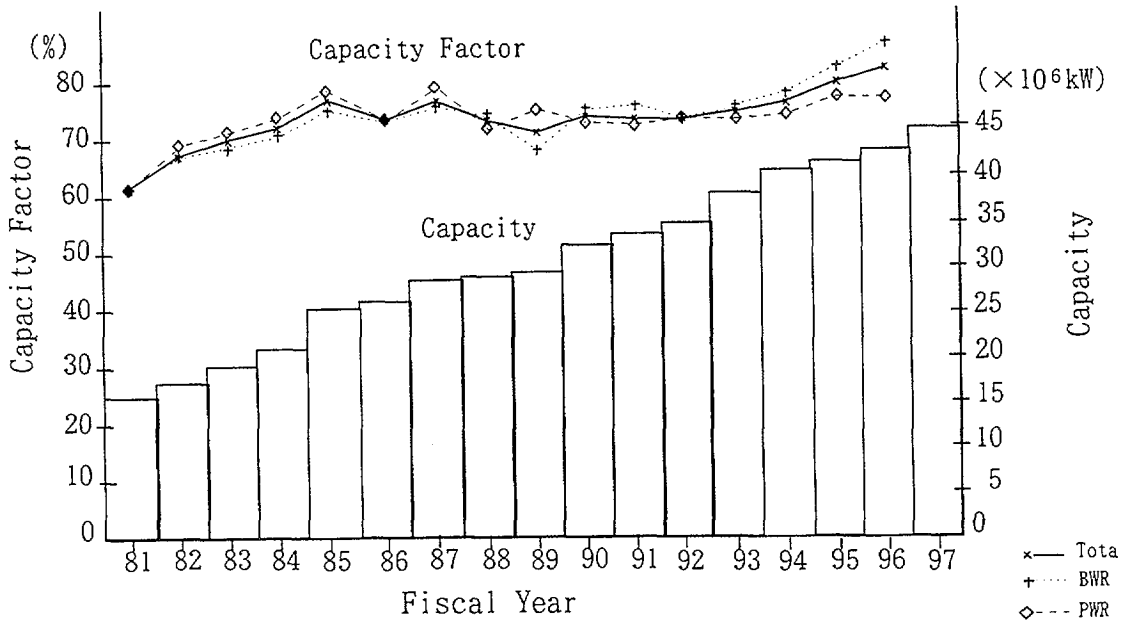


FIG. 1. Capacity factor of LWRs in Japan (Ref. Annual Report of NPP Operating Management).

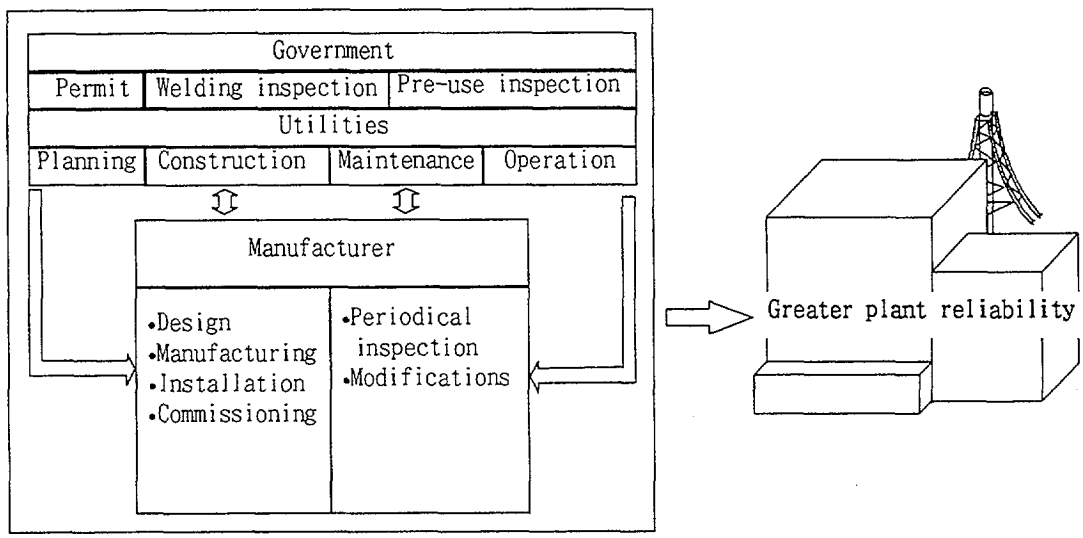


FIG. 2. Plant reliability improvement activities in Japan.

introduction, the operational experiences of plants have been analyzed and assessed to obtain an accurate understanding, and measures against anticipated underlying causes have been taken. Quality assurance criteria have been established, and national standardization and development programs by related organizations have been carried out. Figure 2 shows flow of the activity for reliability assurance. At present, such quality assurance activities are again being extended by way of Japanese QA techniques.

2.2 Necessity of reliability management support tools

As stated above, we have taken several measures to improve reliability. When promoting such integrated activities throughout the life of a plant, it is important to create a mechanism capable of dependably following up such jobs in addition to information management. The reasons why various reliability information must be controlled as a data base and how the system must be organized are as follows.

(1) There are many reliability management items, with a broad content and a wide scope.
(2) The quantity of data is huge and many sections in charge of products are involved.
(3) Managing jobs must be rationalized in size and made efficient.

3. Outline of an integrated reliability management system for nuclear power plants

To make reliability management efficient throughout the life of nuclear power plants, we have developed a reliability management system to suit the purpose of each phase and have integrated them as a unified system.

Figure 3 outlines the integrated reliability management system for nuclear power plants. The system manages past trouble information, prevents trouble recurrence

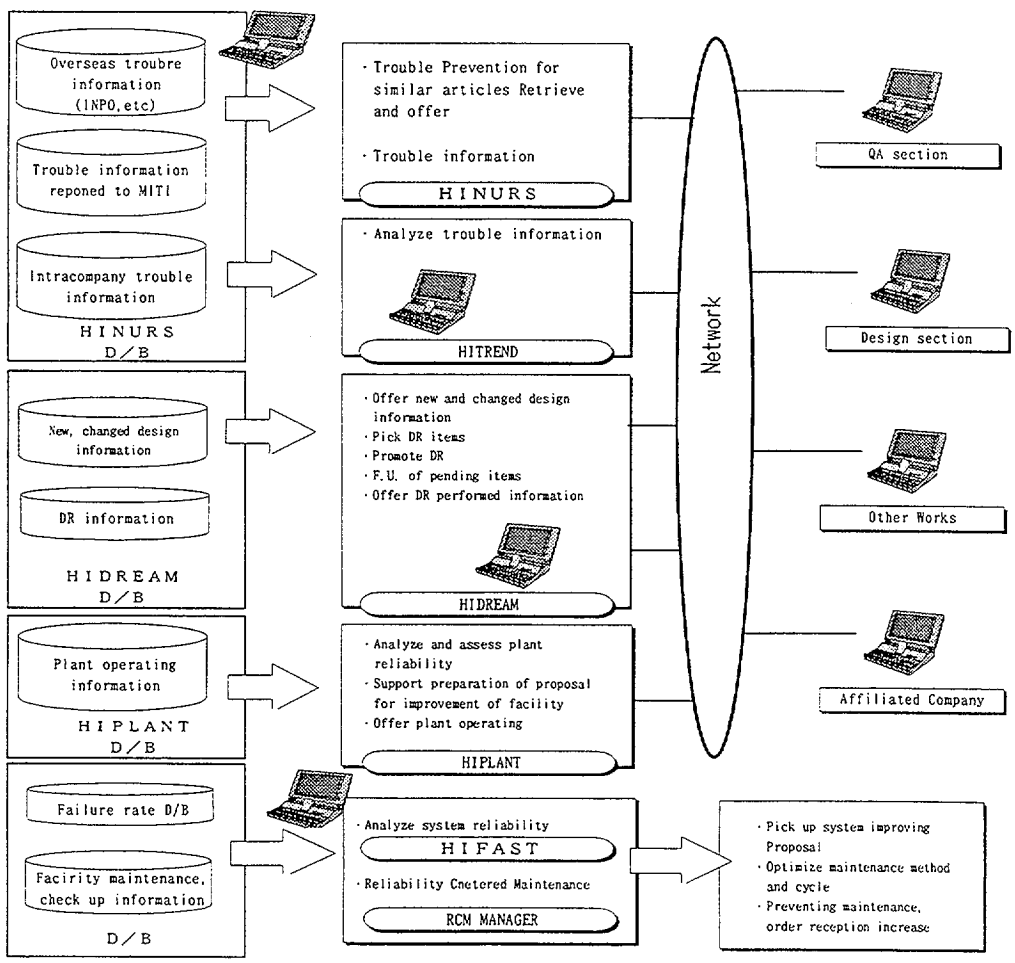


FIG. 3. Configuration of an integrated reliability management system for nuclear power plants.

on all issues that have been or may be affected, analyzes new designs in the design stage and executes the design review (DR), manages plant operation result information, manages plant facilities information and analyzes reliability in the design stage. We try to actively utilize the system as an effective means for reliability management. The following management items are introduced below.

(1) Nuclear power plant reliability information retrieval system
(2) New and modified design management and review management system
(3) Plant operation information management system
(4) Reliability analysis and assessment system

3.1 Nuclear power plant reliability information retrieval system (HINURS/HITREND)

(1) Purpose

The nuclear power plant reliability information retrieval system creates a data base by acquiring a wide range of intracompany, domestic and overseas information on incidents, failures and relatively minor troubles of plant power generation. The system also outputs the results of analyses on causes and phenomena, etc. based on data for study when the design is reviewed.

HINURS

(a) Acquire information and prepare a data base
(b) Provide information for design review
(c) Contribute to information retrieval

HITREND

(a) Probabilistic or correlation analysis with HINURS data

(2) System configuration

This system is configured as an interactive system in order to allow distributed processing and the data base is created on a work station. The system features:

(a) The data base includes key data down to information on relatively minor incidents and failures. There are approximately 3000 registered instances of intracompany troubles, incidents and failures notified to the Ministry of International Trade and Industry (MITI).
(b) Provides information to relevant sections on existing conditions for taking countermeasures to prevent troubles from recurring and horizontal applications.
(c) Retrieval of keywords for systems, equipment, causes, etc. to facilitate the analysis of failure trends.
(d) Offers timely information on trouble instances for design review, periodical inspection of no-trouble tasks, overall design checks and review and various other reliability activities.
(e) Builds an information network encompassing related works to utilize the data base and keep the information consistent.

(3) System operation

We use this system to provide trouble information and the results of analysis on the cause of previous troubles at design review meetings. We also obtain information on the status of trouble recurrence activities and their reflection to other plants. The status of counter measures taken in plants is reported in the trouble recurrence prevention meetings every month.

Recently, the data base is being expanded through data acquisition by on-line information retrieval from the U.S. Institute of Nuclear Power Operation (INPO). We have created an entire corporate network and control the reliability information in those sections involved.

3.2 New and modified design management and design review management system (HIDREAM)

(1) Purpose

Newly designed equipment and modified points are important items to review. The choice of which new or modified design to focus on affects the reliability.

The new and modified design review and management system controls the following items to locate and correct the weak points of design.

(a) Selecting newly designed and modified points and managing their information.
(b) Strictly pursuing design reviews
(c) Strictly enforcing items determined by DR
(d) Promoting the settlement of pending or selected DR items
(e) Consistently managing DR information

(2) System configuration

The system is constructed on work stations and personal computers to store the data base and transmit information. Data is registered and updated for new or modified designs, objects to be reviewed, distinctions between system-based DR and device-based DR, schedules, basic information on responsibilities, coordinators, etc., how far execution has advanced, results, etc. The design section in charge of entering the basic information and the QA section that manages the received information are interconnected by a communication line, creating a network which maintains data integrity.

(3) System operation

The design section in charge of products specifies newly designed and modified points and registers them in the date base. The date base contains 19 items of information, such as management number, item name, reasons for design change, and verification methods. When a verifying method requires a DR, the relevant design section prepares a DR execution schedule, and registers the basic information of the design review in the system at the beginning of the fiscal term. Based on the DR information planned and entered by the design section, the QA section participates in DR, provides information on troubles, etc., issues monthly DR reports and ensures that sections that follow DR apply decided matters to actual plants and settle pending matters.

3.3 Plant operation information management system (HIPLANT)

(1) Purpose

This system is used to analyze the operating performance indices of domestic commercial nuclear power plants according to the data base of plant operating information such as the capacity factor, length of annual planned outage and volume of radioactive waste, etc.

(2) System configuration

This system and the data base reside on personal computers. The system can evaluate the cumulative operating performance and probabilistic analyses and can draw curves of analytical results. The following data are prepared;

Basic Plant Information

Name of plant, Utilities, Reactor type, Plant capacity, Main contractor and Maintenance responsibility

Plant Performance Information

Generated electrical power, Operating and outage time, Amount of radioactive waste, Rate of exposure and trouble information

(3) System operation

Currently, information from 51 domestic plants is gathered on a network of personal computers. By analyzing this system, plant performance characteristics and trends can be evaluated. Especially by assessing the plant capability factor and load factor we may obtain the strategy of the reliability program of the next stage and facility improvement proposal.

3.4 Reliability analysis and assessment system (HIFAST)

(1) Purpose

In system reliability analyses and assessments, fault tree analysis (FTA), and failure mode effect analysis (FMEA), are often used. Through fault tree analysis among other methods, a system failure or other specific event (top event) is selected, and equipment failures, human errors or other basic events that are the direct cause are obtained. The results are then expressed as a logical graph (FT diagram), the system failure causes are qualitatively estimated and, simultaneously, the system failure occurrence probability and basic event importance are quantitatively estimated from the failure rate, recovery time, etc. of the basic event. This is effective for analyzing the safety and reliability of nuclear power plants or other huge systems. The Hitachi fault tree analysis tool (HIFAST), which supports the reliability analysis at the personal computer level, is designed to support the following reliability management jobs in a series of such analyses.

(a) Control the target system reliability value
(b) Support reliability analysis and assessment jobs
(c) Acquire equipment failure rate data and prepare a data base

(2) System configuration

This system and data base are run on a personal computer, and the major features are as follows:

(a) Operation under MS-Windows V3.0 or V3.1, for general-purpose use.

(b) Editing of FT diagrams in Japanese on screen.

(c) Estimating functions by FTA:

- Calculating of minimal cut set
- Calculation of system unreliability (point estimation)
- Analysis of uncertainty of system unreliability
- Estimation of importance of basic event

(d) Indicates graph of probability density function and cumulative probability distribution function resulting from uncertainty analysis.

(3) System operation

The system functions such as the fault tree drafting function, minimal cut set calculation, unreliability calculation and uncertainty analysis functions are run on a personal computer. The reliability of the system is then analyzed and assessed for the design review, etc. Data bases of the fault trees of all operating systems prepared for each plant facilitate estimation of system unreliability, and in case a decision on the system configuration or system modification is made, whether plant standby facilities or duplicated instruments should be provided or not.

4. Conclusion

The authors collected information related to the reliability of nuclear power plants and refined tools for the reliability assessment. A network was established for an overall reliability management system for nuclear power plants. The system enables centralized management of communication and instructions between departments, such as the design and QA, thus rationalizing the reliability management.

Efforts were focused on enhancing the use of QA systems. Efforts by users to improve the reliability of nuclear power plants have raised the reliability of plants by reducing unscheduled outages of the plant and preventing faults and accidents, thus improving the availability of the plant.

The availability of plants must be increased by reducing the duration of regular inspections and by rationalizing inspections and maintenance work as plants grow older. Reliability management will therefore need to enhance the use of QA systems.

REFERENCES

[1]Shimokawa, et al: Development of reliability target setting technique for large plant system by the Japan Federation of Science and Engineering May. 1984

[2]Hitachi Review: Development of light water reactor technology to meet social needs Oct. 1992

[3]Shimokawa, et al: The Japan Society for Reliability Research The Hitachi Nuclear Reliability Management System May. 1994

[4]Matsushima, et al: Japan Nuclear Society Application of system reliability analysis to nuclear power plants Sep. 1994

[5]Matsushima, et al: Japan Nuclear Society Activities for nuclear power plant facility improvement Sep. 1994

NEXT PAGE(S) left BLANK

XA9848564

CURRENT ACTIVITIES IN SUPPORT OF CANDU PLANT LIFE MANAGEMENT: AN INDUSTRY PERSPECTIVE

B.A. SHALABY, E.G. PRICE, J. HOPKINS, P. CHARLEBOIS
Atomic Energy of Canada Limited,
Mississauga, Ontario,
Canada

Abstract

The current focus of the CANDU industry is to position the nuclear option as a cost competitive, safe and reliable means of electricity production. To achieve its goal the CANDU industry as a whole is undertaking steps to improve further its performance and safety of its nuclear power plants. A number of programs have been planned and implemented particularly for plants in the mid-life range. Some of these programs include life assessment studies of critical systems, Structures and Components (SSCS), refurbishment and upgrading programs and monitoring and periodic inspection programs. Some elements of the programs have been in place from station start up and some are being instituted as part of the aging management and performance improvement program.

The industry recognizes that the key to sustaining high performance over the life of the plant is the implementation of an integrated aging management program that encompasses all elements of plant operation and maintenance. A systematically implemented program on optimized maintenance and inspection strategy, standardized work processes, component rehabilitation programs, and applying lessons learned are some of the elements of a sustainable high performance and an effective plant life assurance program.

The paper will describe the elements of an integrated program, the multiphase approach defined for CANDU PLIM and some of the activities undertaken by the industry to further improve and sustain plant safety reliability and performance

1. INTRODUCTION

This decade marks the maturity of the CANDU program with many plants approaching mid-life (20-30 years) particularly in Canada. Table 1 shows the age distribution of CANDU NPPs worldwide (in operation or under construction). Therefore Plant Life Management (PLIM) for CANDU plants became the focus of CANDU owning utilities in the last few years to ensure the long term safe operation of the units coupled with reliable operation to achieve economic performance.

The aging process affects all nuclear power plants presently in operation. The Aging processes that occur in nuclear power plant structures, systems and components (SSC) need to be identified and understood if age-related degradation is to be properly managed. This Plant Life Management (PLIM) program intends to examine in depth the technical limitations of the plant systems, structures and components (SSCs), define degradation parameters and attempt to project the useful life remaining for the identified SSC's. Once defined, an integrated aging management program will be defined to encompass all elements of PLIM. These will include optimized Inspection/ Maintenance programs, and design measures for mitigation and R&D efforts to address gaps in knowledge. With a successful PLIM program, the information provided will assist the stations in maintaining the capacity factors required while achieving assurances of how the plants can continue safe, reliable and cost-effective operation for their whole design life and beyond.

The overall mission for the PLIM program is as follows:

To perform the technical assessments, inspection and maintenance programs required to effectively manage the effects of Aging degradation to ensure continuing safe, reliable and cost effective operation of existing CANDU 6 stations.

TABLE 1. CANDU REACTORS IN OPERATION OR UNDER CONSTRUCTION

Name	*Location*	*Capacity Mwe (net)*	*In-Service date*	*Age(years)*
Pickering 1	Canada	515	1971	26
Pickering 2	Canada	515	1971	26
Pickering 3	Canada	515	1972	25
Pickering 4	Canada	515	1973	24
Bruce 1	Canada	848*	1977	20
Bruce 2	Canada	848*	1977	20
Bruce 3	Canada	848*	1978	19
Bruce 4	Canada	848*	1979	18
Point Lepreau	Canada	633	1983	14
Gentilly-2	Canada	638	1983	14
Wolsong 1	Korea	638	1983	14
Embalse	Argentina	600	1984	13
Pickering 5	Canada	516	1983	14
Pickering 6	Canada	516	1984	13
Pickering 7	Canada	516	1984	13
Pickering 8	Canada	516	1986	11
Bruce 5	Canada	860	1985	12
Bruce 6	Canada	860	1984	13
Bruce 7	Canada	860	1984	13
Bruce 8	Canada	860	1987	10
Darlington 1	Canada	881	1990	7
Darlington 2	Canada	881	1989	8
Darlington 3	Canada	881	1991	6
Darlington 4	Canada	881	1992	5
Cernavoda 1-3	Romania	665 x 3	1996/2003**	-
Wolsong 2,3&4	Korea	668 x 3	1997/1999	-
Qinshan Phase 3	China	700 x 2	2003	-

* Electrical equivalent (electricity plus process steam)

** Forecast date for Unit #3

The program's main objectives are:

a) To maintain the long-term reliability and safety of Gentilly-2 and Point Lepreau during the nominal design life of 30 years (life assurance);

b) To maintain the long-term availability and capacity factors of Gentilly-2 and Point Lepreau with controlled and reasonable generating costs during the nominal design life of 30 years (life assurance);

c) To preserve the option of extending the life of Gentilly-2 and Point Lepreau with good safety and availability at reasonable costs, beyond the nominal design life of 30 years, up to 50 years or more (life extension);

d) Identify potential aging issues, ahead and provide means for monitoring and mitigation to ensure reliable component performance.

1.1 Overall Approach

An NPP has a large variety of systems, structures and components (SSCs), many of which are essential for overall plant safety and reliability. To enable components to be selected for Aging assessments an overall approach and a systematic methodology is required.

For CANDU Nuclear power plant components have been classified into one of the following classifications:

1) Critical Non Replaceable (Critical systems structures and components (SSCs) that are not replaceable).

2) Critical Replaceable (Critical SSCs that are replaceable)

3) Non Critical, SSCs

A) Critical components are those, if failed, will have a major impact on plant safety, reliability. In some extreme cases their failure could limit the life of the plant. A component is classified "critical" if it meets one or more of the following criteria:

1) Cost:

The cost of refurbishment or replacement is significantly high (-<$50M)

2) Plant Availability:

Its failure leads to a long forced outage leading to a long term impact on plant reliability.

3) Safety and Environmental Protection:

Its failure results in the inability to meet jurisdictional requirements in terms of public safety, worker safety or environmental regulations.

A) Non Critical SSCs

Non Critical SSCs are plant systems, structures or components that do not directly impact safety or plant reliability and hence can be replaced or maintained during the plant regular outages and maintenance call ups.

2. KEY PROGRAM ELEMENTS

The key elements that formed the bases of the PLIM programs were:

- Identification of critical systems, structures and components (SSCs), assessment of Aging mechanisms for each SSC and its impact of its safety and performance requirements.
- Aging Assessment of critical SSCs of plausible degradation mechanisms given in reactor environment and design bases. Ensuring recommendations of methods of mitigation and monitoring of the plausible degradation mechanisms.
- Effective inspection, plant monitoring and overall maintenance strategies to monitor and mitigate Aging by changes in operating conditions of such components.
- Rehabilitation through upgrading, refurbishing and/or replacement for some plant components.
- A variety of programs including R&D aimed at addressing gaps in knowledge, improving plant monitoring, maintenance, and inspection of critical components and understanding the influence of various factors on service life.
- Incorporation of successes, lessons learned and technological advances from both Canadian and international programs into existing and new designs.

Beyond these distinct elements a second tier of programs are formulated based on various inputs;

1) from the utilities operating practices,

2) results/recommendations of Phase 1 assessment studies,

3) knowledge from the R&D programs,

4) results/recommendations from Phase 2 life attainment studies and preparation for mid-life rehabilitation,

5) emerging product issues and means of mitigating the impact of such issues on continued safe and economic operation of the plant,

6) the action plan and recommendation ensuring from the Capacity Factor Improvement program with the utilities, and

7) Figure 3 depicts such inputs as the "Technology Watch" plan aimed at "avoiding surprises" that might impact on the plant's long term safety and reliability.

3. PHASED APPROACH

CANDU PLIM program can be divided into three phases.

- **Phase 1**: Detailed Aging Assessment Studies of critical SSCs:

A screening and prioritised methodology is defined to identify critical systems, structures and components (SSCs). The screening methodology is outlined in Figure 1 and is driven by safety and economic considerations.

Further screening can also be applied based on the plant Probabilistic Safety Assessments (PSA), Final Safety Analysis Reports (FSARs), Operating Principles and Procedures (OP&P) and collected data from condition based monitoring, etc.

Detailed Aging Assessment Studies are currently being performed to identify all applicable aging degradation mechanisms and their plausibility, given the years of service and in reactor conditions. Ensuing conclusions and recommendations are then formulated and implemented under an overall aging management program. Figure 2 describes Phase 1.

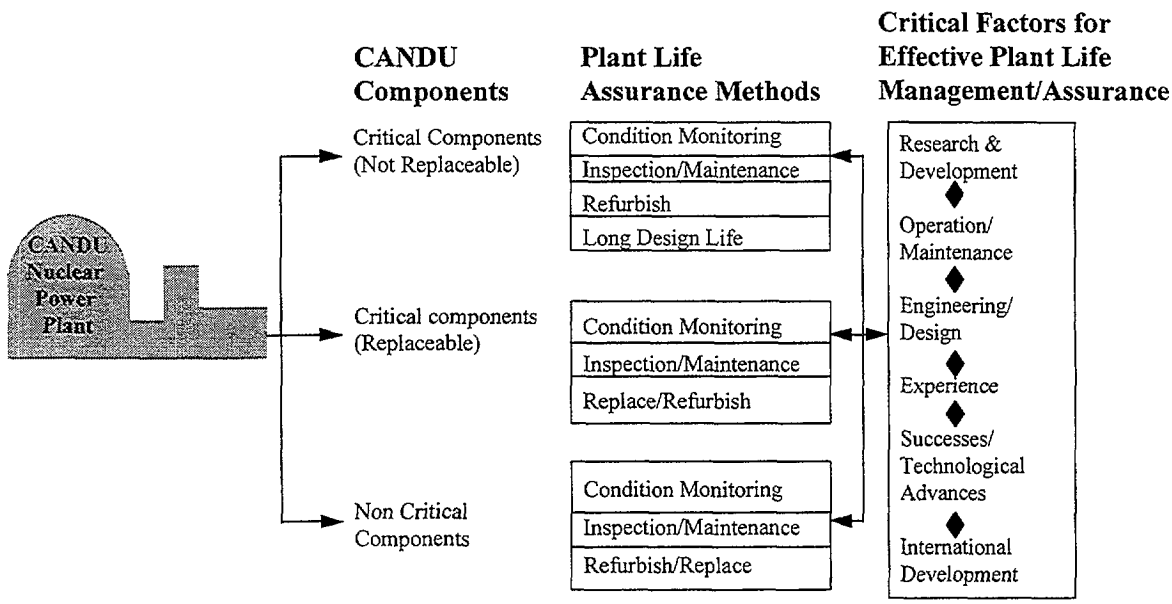


FIG. 1. The Screening/Prioritization Approach in CANDU NPP PLIM

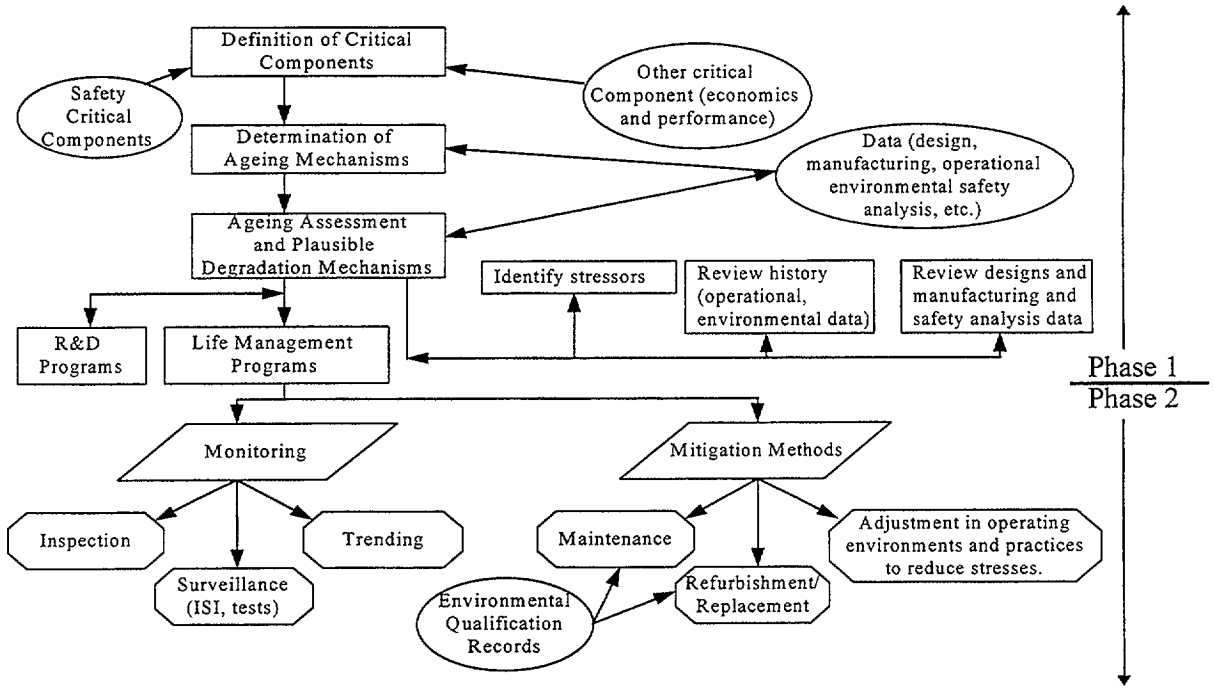


FIG. 2. Elements of CANDU Plant Life Management : Technical

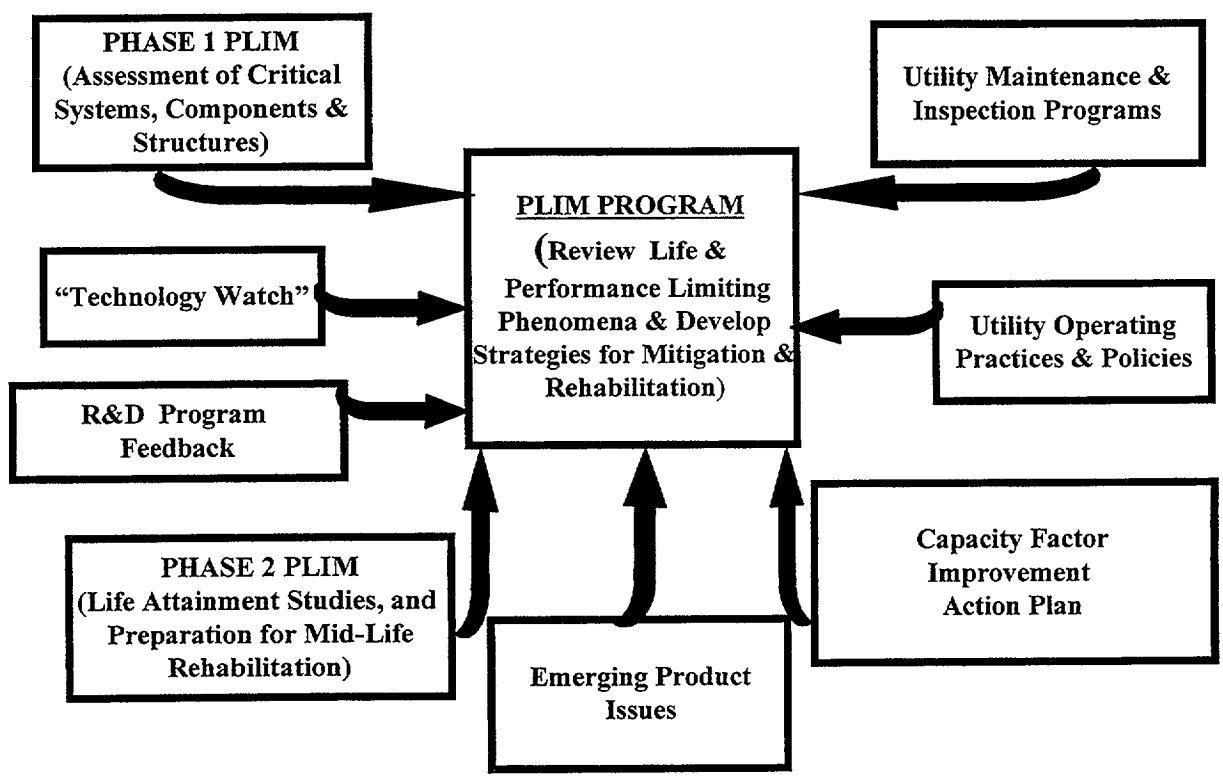


FIG. 3. Program Elements of Plant Life Management (PLIM)

TABLE 2. THE CANDU PLIM MULTIPHASE APPROACH

Phase	*Period*	*Scope*
Phase 1	1994-1998	Scoping Study • Identification of critical SSCs. • Ageing assessment studies of critical components • Scoping of regulatory and safety related design modifications • Supporting R&D • Advanced Technology Development • Phase 2 Planning
Phase 2	1998-2008	Detail Planning Evaluations and Engineering • Formulation and planning of the detailed PLIM program • CANDU 6 detailed inspection and specific residual life assessment of key components • Implementation of some life management programs, plant monitoring, surveillance, etc.. • Documentation for submission to the regulatory authorities • Continue advanced technology development
Phase 3	2008-2012	Refurbish, Replacement and Rehabilitation • Implementation • Rehabilitation Programs

- **Phase 2**: Formulation and planning of the detailed aging management program:

  During this phase some programs will be implemented and some programs will be scheduled for implementation during an extended planned outage.

  During Phase 2, detailed planning, inspection, evaluations, engineering assessments and developments are undertaken for input into the utility's economic evaluation and planning programs. In parallel with such activities, engineering developments and supporting R&D programs will continue to support safety and regulatory requirements, mitigation of plant aging, and assure the plant's design life to enable its extension to the optimum life.

- **Phase 3**: Refurbish, Replacement and Maintenance:

  This phase will be influenced by the regulatory and economic environments. This implementation phase, Phase 3, will be formulated by the results of Phase 2; mainly knowledge from inspections using advanced technologies resulting from R&D and other programs e.g. Environmental Qualification, Condition Based Monitoring, etc..

The overall description of the PLIM plan and its relevance to the current CANDU 6 plants is shown in Figure 3 and Table 2. This long term plan may be modified in accordance with the results of Phase 1 studies.

4. TECHNICAL ASPECTS

Phase 1 started with defining the most critical components of a CANDU NPP. These are:

1) Fuel Channels
2) Steam Generators (including internals)
3) Reactor Assembly/Calandria Supports
4) Reactor Headers, Reactor Coolant Piping, Pressurizer and General Nuclear Piping
5) Cables

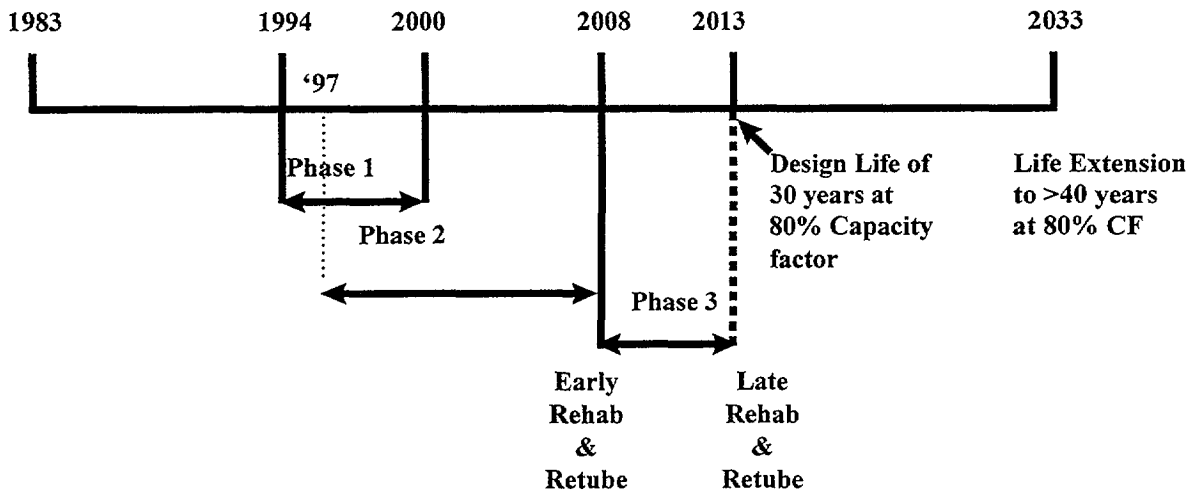


FIG. 4. PLIM Schedule of CANDU 6 NPPs (with 1983 In-service Date)

6) Conventional Piping
7) Containment Structures
8) Airlocks
9) Instrumentation and Control
10) Turbine
11) Turbine Generator
12) Cooling Water Intake
13) Other Civil Structures

These critical components or structures were selected from the criterion that their failure will have the most impact on plant life and hence they include replaceable and non-replaceable components. Ontario Hydro has undertaken for Pickering A (25 years of operation), detailed life assessment studies of most of these components under its NPLA program. Detailed ageing assessment studies were undertaken for some of the critical components for the CANDU 6 designs with specific emphasis on Pt. Lepreau and G-2. Conclusions and recommendations reached todate are:

- 13 critical SSCs (or categories of SSCs) have been identified.
- All other equipment (non-critical) repair or replacement will be planned through normal maintenance programs and undertaken in a cost effective manner to maintain reliability and safety.
- All ensuing recommendations from the in-depth studies done for Pickering A have or are being addressed either generically by R&D or by inspection and maintenance programs.
- All critical components are subject to periodic, or in-service inspections to assess and incorporate recent data collection into plant ageing management strategies.

The most sensitive of those equipment are discussed below:

4.1 Fuel Channels

Todate, pressure tube ageing degradation mechanisms have been fully characterized through extensive R&D and inspection of current reactors. These resulted in the development and application of fitness for service guidelines and methods for mitigating ageing in current plants. A summary of key PT ageing mechanisms and life management programs applied is in Table 3. For CANDU units currently under construction or planned, the fuel channel design and material property improvements that have been developed are expected to result in less degradation and significantly reduced inspection and maintenance requirements to achieve the design lifetime of the tubes

4.2 Steam Generators

Steam generators in CANDU plants have performed relatively well compared to PWR plants. However they have contributed to the incapability of operating plants particularly in Bruce A and Pickering. Experience todate with Incoloy 800 tubing on Darlington and CANDU 6 Steam generators has been relatively good. Strict control of operating conditions (e.g. chemistry) and aggressive remedial actions and careful proactive maintenance activities, backed by significant R&D have led to a decrease in S/G related unavailability of CANDU plants. Canadian CANDU utilities have developed programs for remedial actions to combat degradation of performance (Gentilly 2)

TABLE 3. SUMMARY OF KEY AGEING MECHANISMS OF CANDU P/T LIFE MANAGEMENT ACTIONS

Mechanism	**Units Affected**	**Life Management Actions**
Irradiation Enhanced Deformation	Pickering (1-4) Bruce (1&2)	Large Scale Fuel Channel Replacement (LSFCR)
	All other units	• Monitor deformation of operating tubes (increased design allowances are available) • Testing at fast flux facilities for end of life properties
DHC due to a hydride blister (from PT/CT contact)	Pickering (1-4) Bruce (1-2)	LSFCR LSFCR
	Units with 4 potentially displaced spacers	Spacer Location and Relocation (SLAR)
	All other units	No special maintenance needed
DHC due to stress concentration (tube flaw)	Early units	P/T with flaws removed
	Later units	Sources of serious tube flaws eliminated. Reference to FFSG. Generally no action needed

Pt.Lepreau, Bruce A/B, Pickering A/B) and strategic plans to ensure good future operation. CANDU specific fitness for service guidelines (FFSG) are currently being prepared capturing R&D results, corrosion and mechanical degradation of tube bundles and internals, chemistry, thermal hydraulics, fouling, inspection, etc.. Apart from the FFSGs, other ageing mitigation programs are being implemented as needed including S/G tube primary and secondary side cleaning and regular water lancing of sludge piles. The combined effects of all proactive measures/ improvements in operating practices and chemistry modifications will ensure S/G design life above the required capacity factor.

4.3 CANDU Reactor Assembly

CANDU reactor assemblies are designed to be maintenance free for the design life of the plant. Thus manufacture, assembly and installation procedures were carefully considered with respect to degradation mechanisms before parts were created. Numerous material and fabrication specifications are written to produce a degradation tolerant design. This may have required that the applicable design codes, and standards were supplemented in cases where the codes and standards are considered to give an inadequate margins to the design in terms of potential degradation mechanisms. Detailed

assessments for Pickering A, G-2, Pt. Lepreau plants show that there is little concern with postulated degradation mechanisms at this time. Mitigation of any detected potential would be addressed with a R&D program.

4.4 Cables

Extensive R&D has been done in support of Environmental Qualification of control and power cables for CANDU NPPs. The thrusts of these programs were ageing characterization and applicability of various diagnostics to assess the state of cabling materials in higher than room temperature, high radiation environments. Todate, Cable insulation was found to be the most sensitive of the cable components in providing early indication of ageing related degradation. Work continues for a variety of insulation materials and temperature-radiation conditions. Results today have been used in new plants in the selection of cabling materials for different in-reactor environments.

5. CONCLUSION

The Canadian Nuclear Industry and the Regulatory Body (Atomic Energy Control Board) have strived to maintain the CANDU NPP as a safe and reliable means of electricity production in recognition of its role in today's global economy. To achieve this standard, the industry has focused on an effective strategy for plant life management and potential life extension.

The CANDU design life was initially set at thirty years. Based on Pickering A experience todate and the replacements and/or refurbishments done to it, a minimum of 40 year operating life can be achieved. In new designs of CANDU units a 60 year life is predicted.

NEXT PAGE(S) left BLANK

IMPROVING NUCLEAR UTILITY GENERATION CAPACITY, UNDERSTANDING THE SOURCES OF FORCED OUTAGE AND LEARNING HOW TO PREVENT THEM

XA9848565

D.L. BRODEUR*, V.T. ANGUS**, N.E. TODREAS*

*Massachusetts Institute of Technology,
Cambridge, Massachusetts

**PECO Energy Co.,
Sanatoga, Pennsylvania

United States of America

Abstract

MIT and PECO Energy have completed a detailed examination of the sources of forced outages at the Limerick Generating Station (LGS) Boiling Water Reactor Class IV (BWR IV) site over a five year period and contrasted that information to similar BWR IV utilities in the United States over the same period. Each forced outage was attributed to one system and assigned causal codes of equipment versus human factors and failure attributes such as weak design, poor craftsmanship, and worn parts. It was found that fifty four percent of the lost power at LGS was the result of Balance of Plant failures. Industry wide data identified fifty nine percent of the lost power as attributed to Balance of Plant failures. Balance of Plant systems are those systems not included in the primary and safety related system category. Considering failure causal factors, forty six percent of the lost power at the utility under study was the result of equipment factors such as weak design or worn parts. Significantly, the study showed a high variance between those systems which caused significant forced outage at the two sister LGS units. This demonstrated the infrequent nature of plant forced outages within a given system. This was supported by the observation that dominant systems attributing to forced outage at LGS were not equally represented in industry data. It is suggested that for individual utilities to dramatically improve unit capability factors with regard to Balance of Plant systems, they must learn from industry wide experiences and develop cooperative means of exchanging lessons learned among similarly designed plants and systems. With the broad knowledge base of system failures, current designs must be frequently assessed and altered until each system poses an acceptable level of risk to generation capacity.

1. Background

This paper seeks to understand the nature of nuclear utility lost generation capacity, determine the current vulnerabilities of utilities and explore processes that can be used to improve utility generation capability. This research has been performed in a cooperative arrangement between MIT under the funding and sponsorship of INEEL and the Limerick Generating Station under the sponsorship of their parent utility PECO Energy.

2. Hypothesis

It is postulated that Balance of Plant systems pose the greatest risk to the high capacity performance of nuclear utilities. Primary plant and safety related systems receive greater

attention in their design, fabrication, testing and operation. These systems are redundant in nature, have excellent engineering oversight and are operated and maintained with much more care. The Balance of Plant systems which include the power generation equipment, secondary steam systems and supporting equipment are often designed without redundancy, have less engineering oversight and receive less attention when maintained and operated. It is also postulated that the failures experienced by individual utilities are infrequent in nature but have a significant impact on forced outage rate. This would imply that individual utilities could greatly improve their reliability by examining a broader base of failures at similar utilities where other infrequent failures may have been experienced. To improve the operational capacity of utilities it is necessary to fully understand the nature of forced outages and losses of generation capacity at the utility of interest and at similar utilities.

3. Methods

To understand the nature of lost generation capacity, specific utility data from Limerick Generation Station's two BWR type IV power plants was analyzed for a five year period from 1992 to 1996. This analysis was very detailed as the data was collected by engineering personnel at the utility and reviewed by the utility management. Forced outage data representative of all BWR type IVs using an NRC monthly report data base maintained by INEEL data was also collected. This data was much less detailed but provided greater breadth to characterize the losses experienced by the industry. Periods of lost generation capacity were analyzed to determine the system whose failure caused the outage and the nature of the failure.

Teams have been organized within PECO Energy to review each Balance of Plant system's reliability. With the knowledge of the past failures at Limerick and within the BWR class IV industry, each system will be examined to isolate weaknesses and proposed alterations that will enhance system reliability.

4. Research results

4.1 Specific Utility Data, Limerick Generating Station

Limerick Generation Station has two BWR type IV plants. Each unit is rated to produce 1160 MW electric. Unit one went into operation in 1986. Unit two went into operation in 1990. There is one engineering and maintenance staff that oversees both plants. Operators are rotated between the plants. All reductions in generation at Limerick's two units of greater than 100 MW for a five year period were examined. Losses in availability were characterized by the outage length, MW hours of electric generation lost, the system initiating the outage, and the nature of the outage. Scheduled outages to repair failed equipment were included in this data. Only refueling outages and scheduled outages to support planned preventative maintenance were excluded. If the plant was shut down to repair several systems only the system primarily responsible for the shut down was included. This focused the results on those system failures that actually affected generation capacity.

4.2 Analysis by System

4.2.1 Overall Lost Capability and Occurrences of Failure

Each period of lost generation capability at the two Limerick generating stations was characterized by the total lost generation potential from the start of the reduction in full

power until the resumption of full power and by the system in which the failure caused the reduction. Figure 1 depicts the percentage of the total lost generation capacity attributed to each system and the relative frequency with which each system caused periods of reduced generation capability. For each system there are two bars. The left colored bar represents the percentage of the total five year lost generation capacity at both plants attributed to that system. The light gray bar on the right represents the percentage of lost generation occurrences attributed to that system. Balance of plant systems have been grouped together and are shown in red (moderately dark in black and white). Primary and safety related systems are shown in blue (dark black). Losses in generation resulting from forces external to the utility, such as lightening or grid instabilities, are shown in yellow (white). This figure represents more than just forced outage data as periods of reduced generation are included in which the generator remained on line. This figure does not represent failures of systems which did not impact generation capability.

Balance of Plant systems account for 54 percent of the lost generation capacity. The EHC (Electro-Hydraulic Control) grouping was dominated by piping failures and control system instabilities. The large generation loss of the Main Steam grouping was the result of three Main Steam Relief Valve based shutdowns. This well understood weak component obviously poses a high risk to efficient operation. The Recirc (Recirculation) system grouping failures were characterized by control system instabilities, age related failures and maintenance failures.

The relationship between a system's contribution to total lost capability and to total failure occurrences portrays the risk posed by individual failures. Main steam (steam relief valves) and Reactor (fuel failures) are noted to fail infrequently but consume large losses in generation capability for each failure. Feedwater, Condensate, and Feedwater heating are noted to fail frequently but consume little generation capability loss for each failure. Many of these failures constitute only a load drop making restoration of power much more rapid. The overall tendency of the Balance of Plant systems to fail more frequently, but with less impact, is noted by fact that 74% of the frequency of reductions in generation capacity were the result of Balance of Plant system failures yet only 54% of the total generation capability

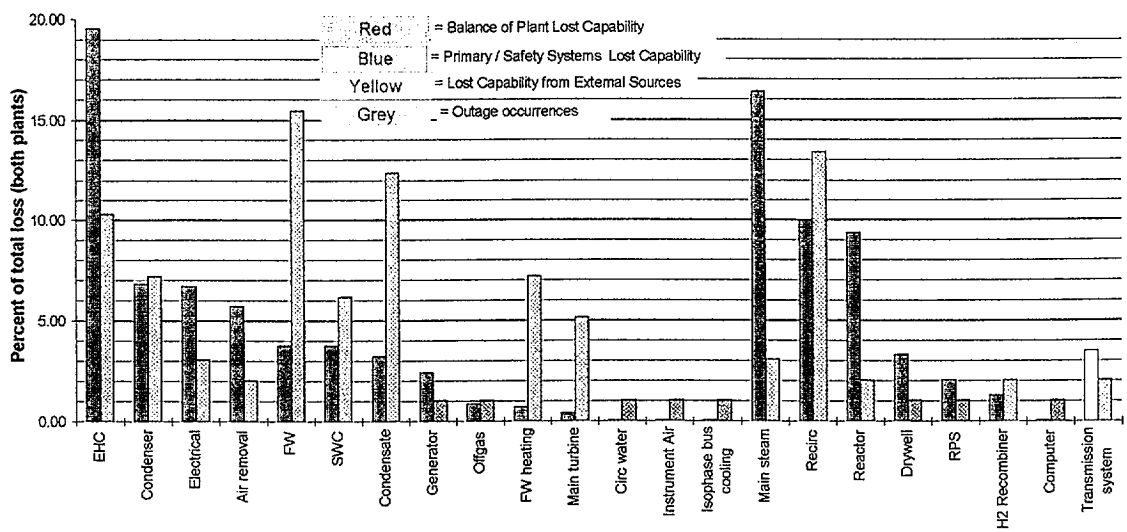


FIG. 1. Lost Generation Capacity by System and Occurrence, Limerick Units 1 and 2

was lost to these failures. Improvements to those systems that fail infrequently but carry a severe penalty can have a dramatic improvement on overall plant capacity. Improvements to systems that fail often but carry little penalty can minimize the transients to which the plant is subject and possibly prevent a large subsequent outage due to related equipment failures or plant control difficulties.

4.2.2 Comparison of Limerick Units

Figure 2 contrasts the lost generation attributed to each system at the two sister Limerick plants. The plants have the same engineering and maintenance staffs, similar designs, were constructed within six years of each other and are operated in the same manner. It can be seen that there is great variance in the lost generation capacity attributed to each system between the two plants. This could be the result of the infrequent nature of the failures, the result of inherent differences between the two plants or the result of the learning that occurs at both plants when one experiences a failure. If a failure occurs at one plant, both plants are modified since they are overseen by the same staff. Preliminary research has only supported the infrequent nature of failures approach.

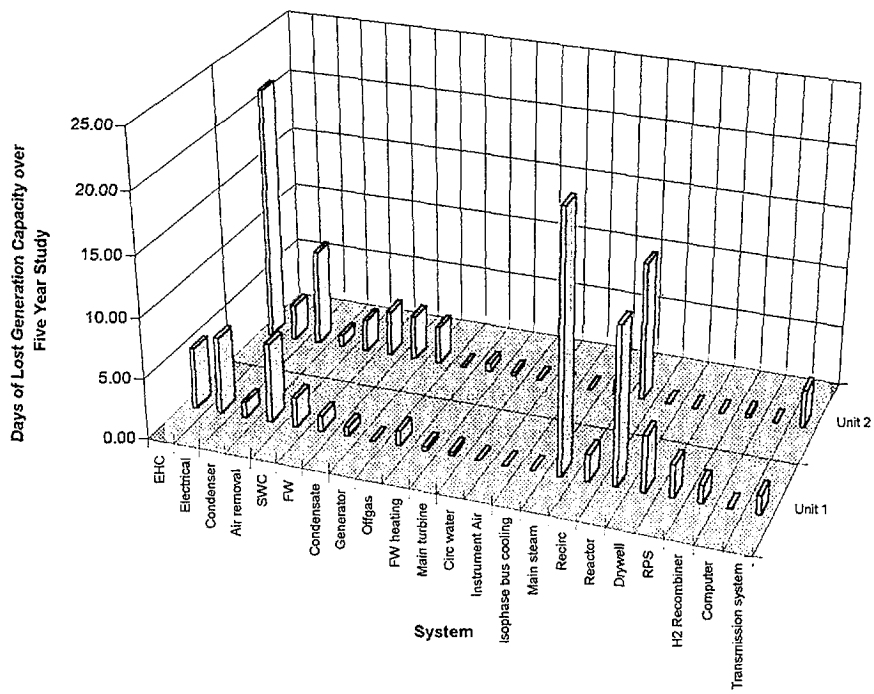


FIG. 2. Comparison between Limerick Plants, Lost Generation Capability by System

4.2.3 Comparison of Limerick to other BWR IV Plants

A BWR IV class wide data base was developed to compare Limerick's areas of lost generation capacity with other similar plants. The data base was built from the monthly reports submitted by utilities to the United States Nuclear Regulatory Commission (NRC). The data was received from Mr. Gary Roberts of INEEL who maintains the reports in a common electronic data base which minimizes the differences in reporting formats. Any event removing the main generator from service was reported by the hours off line or the hours of forced outage. Greatest analysis weight was put on the event narrative section.

Scheduled outages that were taken to repair a failed component were included as forced outages. Refueling outages and scheduled outages taken just to conduct routine preventative maintenance were excluded. Note that this data base is much less detailed than the specific utility data obtained from Limerick.

Forced outage data from the 19 BWR IV utilities was collected for the same five year period that the Limerick analysis was conducted, 1992 - 1996. Failures were again attributed to a single system causing the outage, figure 3. A category of operations was created for NRC and Utility mandated safety shut downs. Several utilities had extremely long forced outages during this period. Browns Ferry Unit 1 was in an NRC shut down for the entire five years of the study. Browns Ferry Unit 2 was in an NRC shut down for over three and a half years. Brunswick units 1 and 2 were shutdown for approximately one year each during the study as the result of diesel technical specification problems. Cooper Station was also shutdown for nearly nine months during the study as the result of diesel requirements. If these forced outages were included in the entire BWR IV forced outage data base they would dominate all other concerns and make it difficult to understand the significance of other causes of forced outage. All forced outages were therefore limited in length to one month with respect to the data base. This had the desired effect of keeping these large outages in the analysis data, keeping them significant, yet allowing other weak systems to become apparent, figure 4.

Specific Utility data was gathered in a manner similar to Limerick from the Peach Bottom Atom Atomic Power Station. Peach Bottom is a BWR class IV, also operated by PECO Energy, that has joined in the same cooperative research with Limerick and MIT. Data from both Limerick and Peach Bottom was truncated for this comparison to keep them comparable to the NRC industry wide data base. All periods of load reduction were excluded as they did not constitute a period of forced outage.

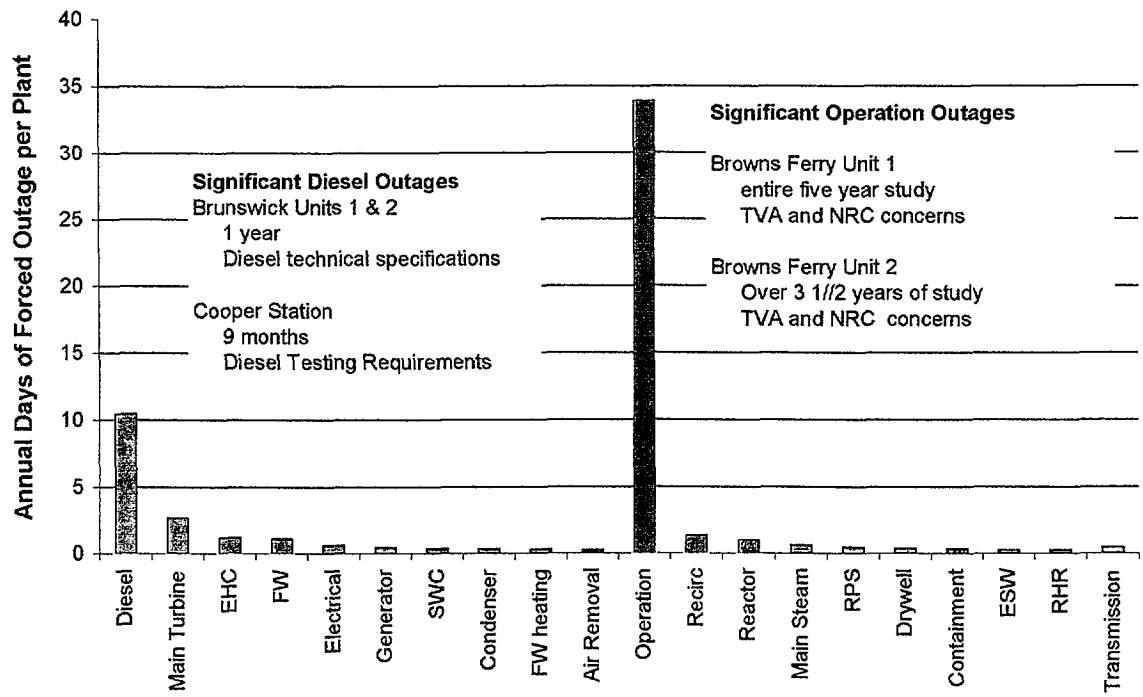


FIG. 3. BWR IV Average Annual Forced Outage Days by System

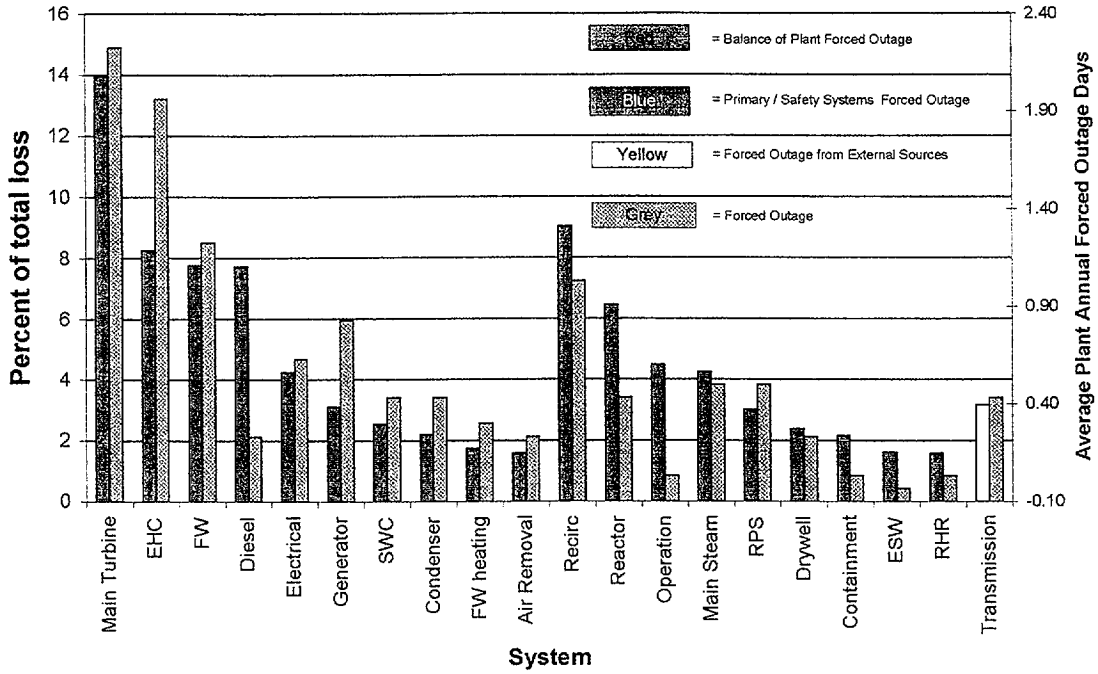


FIG. 4. Comparison – BWR IV Forced Outage Days and Failure Frequency by System.

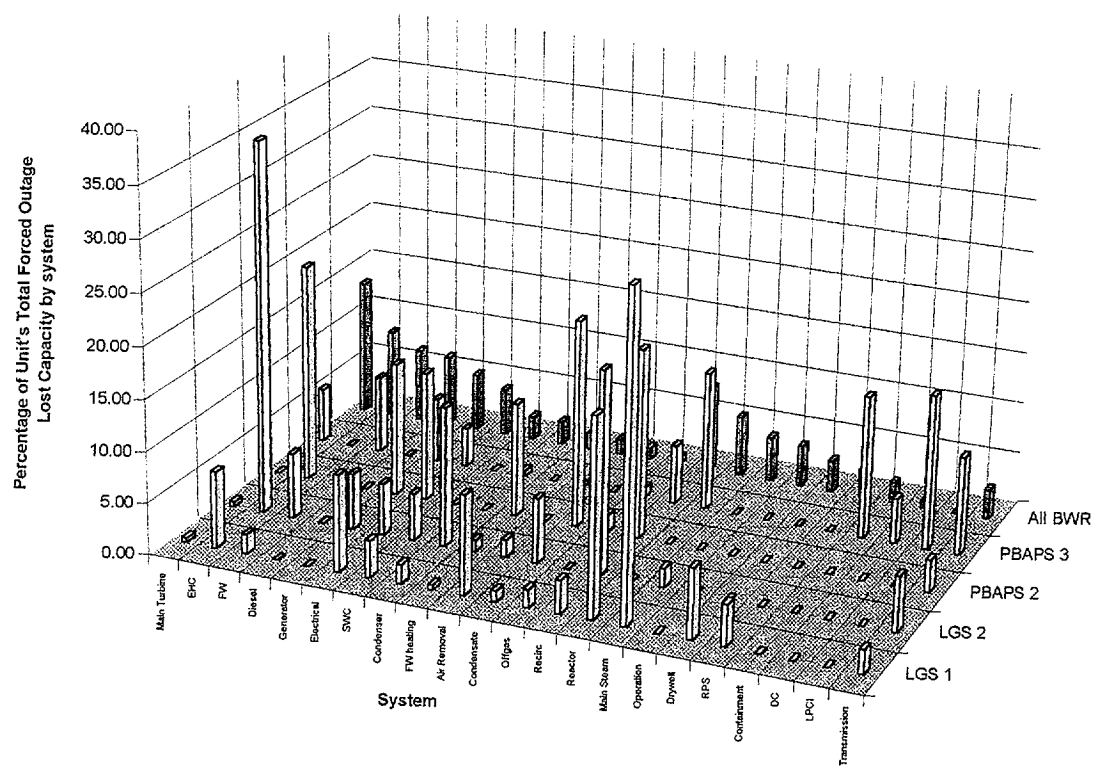


FIG. 5. Comparison, Fraction of 5 year forced outage hours attributed to each system, Limerick Units 1 and 2, Peach Bottom Units 2 and 3 and average BWR IV industry data

To further understand the variant nature of utility system failures, Limerick forced outage data was plotted against Peach Bottom and against the entire BWR IV class. Figure 5 contrasts the relative days of forced outage between the two Limerick units, the two Peach Bottom units, and the BWR IV utility average. The specific plant data appears spiked in comparison to the slowly varying BWR IV data. This spiked appearance demonstrates that individual plants experienced only a small portion of the problems experienced by the broader industry during the five year study. As the plant systems improve in reliability, there will be fewer failures, and the individual failures will appear even more spiked. If one plant only experienced four significant outages in five years, they would have four large spikes As fewer failures happen at an individual plant they must use broader sources of failure data to understand plant vulnerabilities to determine whether they are immune from the failures experienced by others or whether they could experience the same failure and should modify their system. In example, neither utility experienced any diesel related outages, yet that system has a significant portion of the industry data. Limerick is unique from most of the industry with this system as they have eight independent diesels. Peach Bottom is not unique with only four diesels. As a further example, it is noted that there are significant forced outages attributed to the Main Turbine in the industry data but that this system caused few outages at Limerick and Peach Bottom. There were 34 industry wide forced outages attributed to the Main Turbine. The failures were predominately mechanical failures and vibration problems. It is possible that there are enough differences between the turbines to explain the inconsistency. It is possible that time in life is vastly different and that Limericks turbines have not experienced wear out yet. It is also possible that the failures are infrequent enough that Limerick just has not yet experienced them during this analysis window. In either case it would be beneficial to investigate the failures observed at other utilities and attempt to prevent their occurrence at Limerick. While a utility is well aware of their past failures and weaknesses, this plot implies that they must use larger data bases to understand the potential future weaknesses of their systems.

4.3 Failure Causal Analysis

Attempts were made to determine the cause of failures such that the effects of different operating strategies and the effectiveness of improvement strategies could be judged. In the first analysis each loss of generation capacity was attributed to one of the following categories;

- age (failure of parts at the expected end of their useful life),
- design (failure of a poorly designed system, prematurely under normal plant operations),
- fabrication (failure the result of a flaw resident at initial fabrication),
- installation (failure the result of inadequate installation of a good component),
- maintenance (failure attributed to past maintenance actions),
- operation (failure as a result of operator actions).

While these classifications are arbitrary, the cumulative results provide meaningful qualitative assessments. It is seen in figure 6 that only 17% of all losses in generation capacity were the result of age effects. This would give promise to the ability of the plant to support extended operating cycles. Design and maintenance failures, which account for 40% of the lost capacity, can be directly affected by engineering and procedural changes. The installation and fabrication failures are difficult for a utility to affect as the failures occur outside their area of

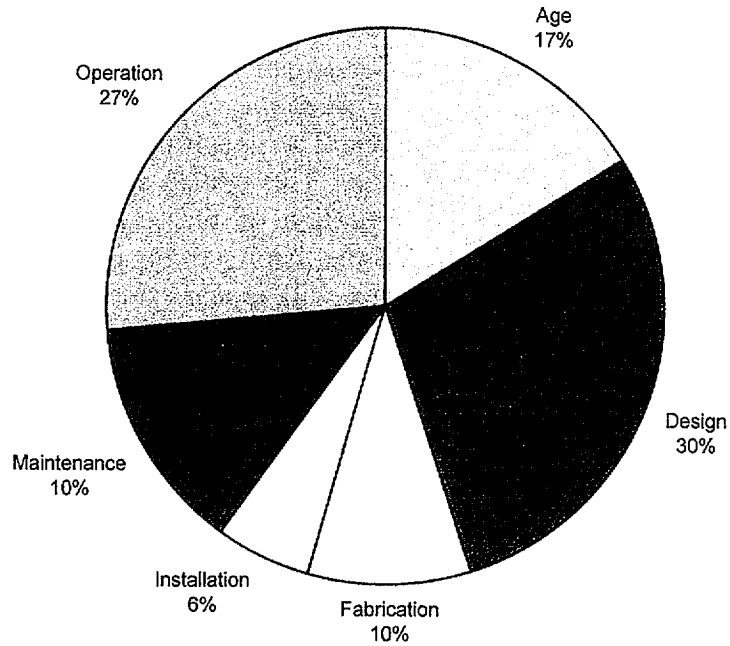


FIG. 6. Lost Generation Capability by System Failure Mode

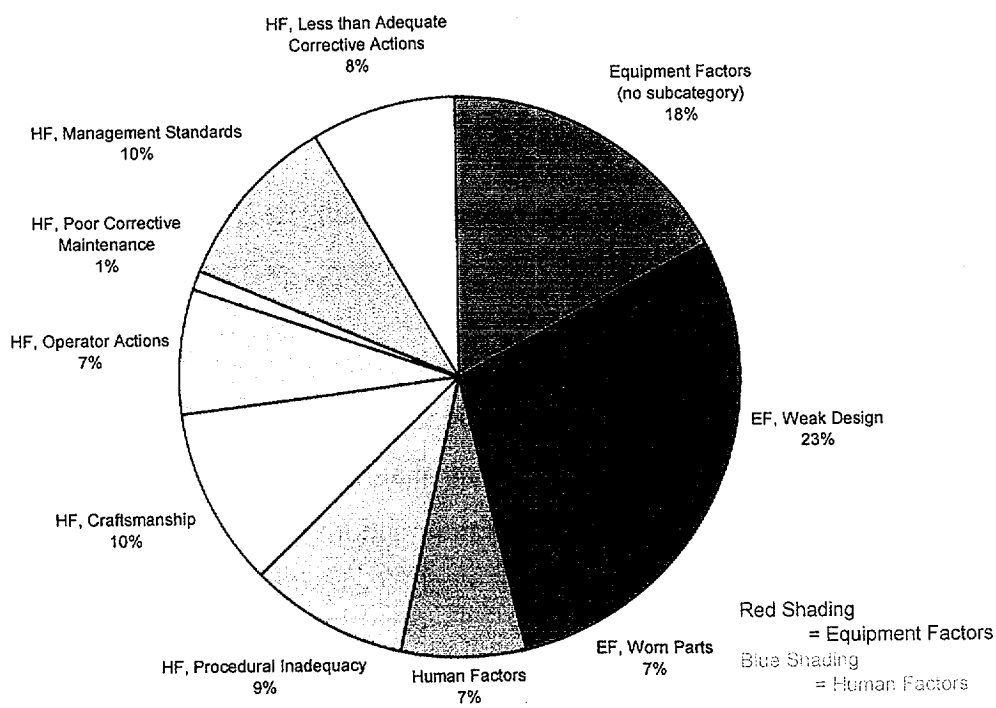


FIG. 7. Lost Generation Capability by Causal Factors

control. Similarly operation related failures are difficult to effect permanent change with as they are significantly tied to personnel actions.

Another study of failure causes was conducted in which failures were classified as the result of either primarily human factors or equipment factors. These categories were then further divided where common failure causes were noted. The equipment factors were subdivided into subcategories of failures due to equipment weak design and worn parts. The human factors related generation losses were subdivided into the following categories:

- procedural inadequacy,
- craftsmanship,
- operator actions,
- poor corrective maintenance (recurring failures attributed to inadequate corrective maintenance),
- management standards (failures related to an intentional decision to operate with components in a reduced state of performance),
- less than adequate corrective actions (recurring failures attributed to the failure to identify and correct the original cause of failure).

Figure 7 shows the lost generation capacity attributed to these causal subcategories. Note that all equipment related losses are shown in red shades and all human related losses are shown in blue shades. When this analysis was first done, equipment related failures which now represent 48% of all losses, were 81% of the total. As each period of lost generation was researched in greater depth, there was a trend toward human related factors. It was also easier to assess a particular human related factor than a specific equipment factor. Engineering improvements to the systems should reduce the equipment factor related losses. Improvements in the human factors subcategories of procedural inadequacy, craftsmanship, and poor corrective maintenance, and less than adequate corrective actions are well understood. Improvements to the subcategories of operator actions and management standards are less easily understood or preventable as each failure is a unique event.

5. Focus on Improvement Team Process

To improve overall reliability at Limerick, cross-disciplined Focus on Improvement Team (FIT) reviews are being performed on the systems identified above to be the primary sources for load reductions and transients. The FIT reviews focus on the design, maintenance, and operation of the systems. FIT system reviews are being conducted to identify weak or potentially weak areas within a system and to develop methods to strengthen these areas in order to improve the overall system reliability. These comprehensive reviews target opportunities to improve system performance. The resultant opportunities include modifications to upgrade components or add redundancy to the system design, changes to operating, testing, and maintenance procedures, changes to maintenance practices or maintenance frequencies, or any other change which could improve the system reliability.

The systems undergoing FIT review have been chosen based on their direct impact on plant reliability. These systems either have caused or have the ability to cause a significant loss in megawatts through plant load drops or shutdowns. The FIT review includes an in-depth review of the system design, historical corrective maintenance on system components, and the preventive maintenance activities currently in place for the system.

The FIT teams for each system include the current Limerick (LGS) and Peach Bottom Atomic Power Station (PBAPS) system manager, the previous system managers at each site, and representatives from Design Engineering, Component Engineering, Operations, Maintenance, Instrumentation & Controls (I&C), and Health Physics.

To date, four FIT reviews have been conducted. The reviews resulted in a significant number of recommendations for improvements to these systems. Many of these ideas can be implemented simply; therefore, evaluations are being created and assigned to the appropriate individuals for implementation of each of these items. These items include, but are not limited to, procedure changes, preventative maintenance (PM) activity changes, PM frequency changes, addition of new PM's, and items requiring further investigation. For the more involved recommendations (i.e. modifications), these ideas are prioritized based on their respective impact on reliability and associated cost. These will be presented to Management for sponsorship.

The results of the FIT reviews completed thus far indicate some commonality of issues between systems. Component specific chronic problems such as air operated valves, limit switches, and recorders were identified across several systems. Maintenance while the plant is at power is extremely difficult, if not, impossible for some of the balance of plant systems since these systems typically operate all of the time. For some systems, the addition of various isolation valves will make it possible to perform on-line maintenance instead of having to shut the plant down to perform the work. The FIT reviews also identified the generic need for additional computer points for monitoring and trending system performance.

Due to the nonredundent design of most Balance of Plant systems, spurious actuation of system components often were observed resulting in power plant transients. A simple fix being pursued for this type of failure is to include a time delay in the logic, such that a valid signal will provide the actuation; however, a spurious signal will not. Issues were brought up concerning obsolete parts and entire control systems such as the Electro-Hydraulic Control (EHC) system for the Main Turbine. In the near future, the vendor will no longer be supplying replacement parts for this system. Either another supplier must be found to build the replacement parts, or the system must be modified to use available technology and parts. Where systems or components are obsolete, recommendations were made to upgrade to newer and more reliable designs. For EHC, strong recommendations were made to upgrade to digital controls and indications for improved reliability.

The results of each FIT review are evaluated for their benefit towards improved system and plant reliability and the associated cost for implementation. The ultimate goal is to implement the most worthwhile recommendations to increase reliability of the equipment in the balance of plant systems; thereby, increasing the reliability of the plant.

6. Conclusions

This study has reviewed the causes of losses in generation capacity over five years at the Limerick Generating Station and the relationship of these losses to industry data. The following conclusions can be made:

- Balance of Plant system failures initiate the vast majority of utility losses in generation and can be attributed to the majority of lost generation power.
    - Seventy Four percent of the periods of reduced generation ability were initiated by Balance of Plant system failures.

- These Balance of Plant failure periods accounted for fifty four percent of the total lost generation power.
- Balance of Plant failures are more frequent but of a shorter duration than primary or safety related systems.
- Failures of individual systems are infrequent events. There is little correlation between system failures at individual plants. It is therefore necessary to use the largest possible data base to draw meaningful conclusions.
- As system performance improves, there is even less correlation of failures between individual plants, strengthening the need to gather knowledge from the widest possible source.
- Analysis of the causes of system failures that can be directly attributed to periods of lost generation imply that equipment will support extended operating cycle lengths and give promise to the ability of engineering staffs to improve system performance.
  - Only 17% of the lost generation capacity was attributed to age related failures.
  - Fifty seven percent of the lost generation capability can be attributed to failures as the result of aged, poorly designed or poorly maintained equipment.
- Forty eight percent of lost generation capacity can be attributed to equipment factors such as weak design and worn parts, while 52% of lost capacity is attributed to human factors such as craftsmanship and operator actions.
- Knowledge of potential system weaknesses can be gained from industry level data and applied to individual utilities through disciplined teams of personnel focused on improving system reliability.

It is understandable why capability lost to Balance of Plant Failures is more frequent than to safety related systems. Nevertheless, Balance of Plant initiated failures frequently challenge the plant and operators, resulting in significant lost generation capability. Weaknesses in these systems must be explored at other utilities due to their infrequent nature of occurrence at an individual utility. With knowledge of industry wide problems, a reliability focused review can determine methods for improvement.

Future work in this area should be done to make the industry data more accessible and develop open communication networks between utility engineering staffs. Additionally further research could improve the detail of the industry wide data base available and increase the types of reactor plant design included in the study.

Acknowledgements

This project has been funded by the Idaho National Energy and Environmental Laboratory (INEEL) University Research Consortium. The INEEL is managed by Lockheed Martin Idaho Technologies Company for the U.S. Department of Energy, Idaho Operations Office, under Contract No. DE-AC07-94ID13223.

The principle author of this report is an active duty naval officer, studying at MIT under the 520 curriculum. As such this work belongs to the United States Government and is not subject to copyright.

NEXT PAGE(S) left BLANK

REVITALIZING QUALITY ASSURANCE

XA9848566

F.C. HAWKINS
Office of International Health Programs,
US Department of Energy,
Germantown, Maryland,
United States of America

Abstract

The image of someone inspecting or auditing often comes to mind when people hear the term quality assurance. Although partially correct, this image is not the complete picture. The person doing the inspecting or auditing is probably part of a traditional quality assurance organization, but that organization is only one aspect of a properly conceived and effectively implemented quality assurance system whose goal is improved facility safety and reliability.

This paper introduces the underlying philosophies and basic concepts of the International Atomic Energy Agency's new quality assurance initiative that began in 1991 as part of a broad Agency-wide program to enhance nuclear safety. The first product of that initiative was publication in 1996 of a new Quality Assurance Code 50-C/SG-Q and fourteen related Safety Guides. This new suite of documents provide the technical and philosophical foundation upon which Member States can base their quality assurance programs.

Just What is Quality Assurance?

When people hear the term "quality assurance," the image of an inspector or auditor often comes to mind. Although partially correct, the image evoked is incomplete. The inspector or auditor is probably part of a traditional, inspection-driven quality assurance organization, but that organization represents only one part of a properly conceived and effectively implemented quality assurance program.

In the broadest sense, quality is the degree of excellence that a product or service possesses. The degree of excellence required for any given product or service is determined by the customer's needs and is achieved by consistently anticipating and meeting his/her expectations. Quality assurance comprises all the actions, from product inception to application, that ensure the customer's needs and expectations are met.

A Short History

Quality assurance began with the first article made by man. Before there were factories, craftsmen depended on individual skill and knowledge to produce goods that served their intended functions. Skill and knowledge were passed from parent to child or from master to apprentice. The skills of some craftsmen were much better than those of others, and the quality of their work varied accordingly. Craftsmen prospered mainly on the basis of their reputations: the most skillful and creative could charge the highest prices for their products.

With the advent of mass production, the responsibility for quality shifted from the craftsman himself to the assembly-line foreman, who oversaw several workers as well as the production process. Under this system, the worker no longer controlled the product, its quality, or the process involved. Mass production thus marked a departure from the traditional value placed on individual achievement: based on acceptance of an average level of quality, the final product was better than that supplied by poor craftsmen but could not compare with that provided by the best. Moreover, the foreman was responsible for production quotas and shipping dates as well as quality. When deadlines drew near, choices often had to be made between business objectives and product quality. Given such choices, the quality of the final product was almost always compromised.

The "foreman-as-inspector" era lasted until World War II, when U.S. industry, of necessity, had to manufacture some of the largest and most sophisticated devices ever produced. The massive U.S. shipbuilding program provides but one illustration of how the system was inadequate. Quality-related problems became apparent when the production of ships for the U.S. Navy fell behind schedule. To speed up the process, the industry offered incentives to workers. Welders, for instance, were paid on the basis of how many feet of weld they completed or how many pounds of weld rod they consumed. As a result, production increased and the shipbuilding effort was soon back on schedule. However, during their first winter in the North Atlantic, tragedy struck when several new ships broke up and sank in relatively calm seas. A subsequent investigation determined that weld defects, resulting from material shortcomings and inadequate welding procedures, were the principal cause.

As a result of this investigation, one of the first modern programs to control quality was developed and implemented. The program identified the need to establish a formal quality assurance program, develop procedures, provide controls for materials, conduct inspections, perform tests, and take corrective actions throughout the construction process. This quality program was written into a basic quality control document and was later revised as U.S. Military Specification (MilSpec) Q-9858, which was issued in 1959. MilSpec Q-9858 probably represents the first systematic effort to ensure product quality in the post-World War II era. The premise behind this and other early programs was their reliance on an acceptable level of quality for any given component. Depending on the component, the probability that it would not be defective might range from 96 to 99 percent. This meant that a 1-4 percent failure rate could be tolerated. But when products became more complex, the 1-4 percent failure rate meant that the success of any given mission depended on luck. For example, if the product required 200 parts, 2-8 could be expected to fail. Success thus rested on the hope that the parts that failed were not critical to the mission.

During the late 1950's, when the U.S. space program was suffering its early setbacks, it became obvious that an improved system to control quality was necessary. The new system was based on the goal of mission success, not on individual component reliability. To achieve this goal, the National Aeronautics and Space Administration (NASA) responded with a program to identify critical components--and the new program used a performance-based approach. By definition, the failure of these critical components would endanger the mission. These critical components must demonstrate extremely high reliability, perhaps 99.99 percent or more, or would require backup in case of failure. To meet this extremely demanding reliability requirement, every step in the production process for each component would have to be verified.

As for the nuclear industry, in July 1967 the U.S. Atomic Energy Commission (AEC) published Appendix A ("General Design Criteria for Nuclear Power Plants") to Title 10, Part 50, of the Code of Federal Regulations (10 CFR 50). The first General Design Criteria in Appendix A contained only one sentence on quality assurance. It states simply that "a quality assurance program shall be established and implemented in order to provide adequate assurance that structures, systems, and components will satisfactorily perform their safety functions" as they relate to radiological safety.

During the licensing hearings for the Commonwealth Edison Company's Zion Plant in 1968, the AEC's Atomic Safety and Licensing Board criticized the industry's lack of standardized requirements for its quality assurance programs. The Board ruled that a document must be drafted to address these missing requirements. As a result, Appendix B ("Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants") of 10 CFR 50 was issued for comment in April 1969. In June 1970, Appendix B was approved and became part of the Code of Federal Regulations. The 18 criteria listed in Appendix B provided the basic requirements considered necessary for an acceptable quality assurance program and stressed the need for objective, documented evidence to prove that the quality of a facility was sufficient to justify the granting of an operating license. Appendix B refined several existing quality assurance programs, including MilSpec Q-9858 and the NASA program, and evolved them to a higher level. Its specific application was for commercial nuclear plant design, construction, and operation, but the program was applicable to modern industry in general.

What's Needed Now?

In many countries, including the United States, the nuclear industry has struggled for years to reestablish public confidence in its operations. Quality assurance is a tool that will help the industry meet this goal--not the traditional inspection-driven quality assurance, which has become the mainstay of the nuclear industry, but a more practical, holistic quality assurance system encompassing the work of every employee.

Quality assurance as it applies to the nuclear industry in particular is often misunderstood and misapplied. Over the years, many people representing diverse interests have written countless reports and papers supporting this conclusion. Quality assurance and the frustrations associated with it are the topics of conferences, meetings, and endless professional discussions. Real-life horror stories are shared about rogue auditors, belligerent plant managers, and the bureaucratic imposition of improperly or inadequately defined requirements. Serious action to change the status quo criticized by so many has now is now taking shape.

In 1996, as part of a broad, systematic program designed to enhance nuclear safety, the International Atomic Energy Agency (IAEA) issued a revised Quality Assurance Code 50-C/SG-Q and fourteen Safety Guides designed to improve the safety, reliability, and performance of Member States' nuclear facilities. The new Code and Safety Guides incorporate contemporary principles and techniques for managing, achieving, and assessing quality; they reflect modern principles and practices; and they make use of commonly accepted and understood concepts and terminology.

As a result, the nuclear industry has recognized that to be successful it must reach beyond traditional quality assurance methods. What this means is that management, workers, and those who assess the quality of work all contribute to plant safety, reliability, and performance. [1] Even though their respective roles differ, every employee (not just the quality assurance professional) implements the quality assurance program, ensuring that risks are minimized and that safety, reliability, and performance are maximized.

More and more, industry is looking to instill a "quality culture" where the customer's needs and expectations are met. The International Atomic Energy Agency's revised Quality Assurance Code 50-C/SG-Q and accompanying fourteen Safety Guides provide a platform from which to build such a culture, demanding an integrated team approach in which every employee works toward the shared goals of safety, reliability, and performance. No longer is the quality assurance professional alone on the front line trying to "inspect" quality into activities and processes over which someone else has control. In this new role, the quality professional focuses his/her attention on matters of substance rather than form.

The quality culture endorsed by the International Atomic Energy Agency recognizes that it is *management's* responsibility to establish and cultivate the principles that integrate quality into the daily work routine. For this integration to be successful, the people actually performing the work must receive appropriate information, tools, support, and encouragement. It is incumbent on management to define requirements clearly; properly train, motivate, and empower personnel; provide appropriate resources; and assess performance. Management should demonstrate commitment and leadership through active involvement in the implementation of an organization's quality assurance program. The individual employee's role is thus to meet established requirements and to recommend concurrent improvements in item and process quality.

As previously suggested, the concept of work (defined as any productive activity) is fundamental to a successful quality assurance program. From a task analysis point of view, all work can be broken down into fundamental building blocks. At the top of this hierarchy are performance objectives: these represent the reasons an organization exists; they define the goals to which the organization aspires. For the sake of clarity, performance objectives may be divided into intermediate objectives, which in turn are divided into subordinate objectives. The intermediate objectives describe the immediate steps or processes required to achieve the performance objectives, and the subordinate objectives provide the fine-grained details for how the

---

[1] IAEA Quality Assurance Code 50-C/SG-Q defines the three functional areas of work responsibility as management, performance, and assessment.

intermediate objectives are to be accomplished. For the whole organization to work successfully, this hierarchy must be clearly defined by management and implemented by the line organization.

Performance objectives are achieved by means of implementing processes that are defined by the intermediate and subordinate objectives. When properly defined and controlled, these processes provide assurance that performance objectives will be met. The inherent interrelationship between performance objectives and processes defines an organization's level of success. When the balance between performance objectives and processes is skewed, when the organization's focus on the latter increases while the former is ignored, this crucial relationship is destroyed. The organization is no longer in a state of equilibrium. Internal controls fail. The ability of the organization to achieve its performance objectives--its reason for being--is lost. The organization itself ultimately fails.

The nuclear community often severs performance objectives from their processes. Many nuclear organizations become so engrossed in the "trees" of the processes (intermediate and subordinate objectives) that the "forest" of performance objectives is eclipsed from view. Traditional quality assurance programs focus on the fine-grained details of processes, not performance. Because organizations fail to identify and articulate their performance objectives, the credibility of the industry is called into question by a public that does not understand, and often fears, its objectives.

For example, a traditional quality assurance program for maintenance elevates the calibration of measuring and test equipment to the level of a performance objective rather than viewing it as one of a number of intermediate objectives.[2] Although the content of a traditional quality assurance program and a performance-based program are virtually the same, in the latter the intermediate objectives of calibration, control of items, work control, as well as subordinate objectives involving the use of instructions and procedures, are all recognized as supportive of the performance objective.

As illustrated by this example, a pragmatic performance-based quality assurance program strikes the appropriate balance between performance objectives and processes. In other words, it focuses on performance objectives without abandoning the processes needed to achieve them. The performance objectives of many organizations are buried two, three, or even four layers deep in the quality assurance program. Consequently, these programs lend themselves more readily to a process-dominated approach to quality assurance. A successful program is performance-based at the highest level. This biases the program toward achieving the whole organization's performance objectives, which should be carefully defined and limited in number.

Conclusion

The inherent limitations of traditional quality assurance have, in part, resulted in mediocre performance and have sometimes compromised plant safety, reliability, and performance. Many organizations have already begun implementing the principles described in the International Atomic Energy Agency's new Code and Safety Guides. Their successes attest to the common sense of implementing a more practical approach to quality assurance, one that emphasizes implementation, effectiveness, and results rather than program development and documentation.

Revitalizing quality assurance through the application of these principles requires constant willingness to reexamine and reevaluate the status quo. This in turn requires a willingness to accept and implement change. It is for the sake of improving plant safety and reliability that performance-based quality assurance programs using Code 50-C/SG-Q and the accompanying Safety Guides should be encouraged.

---

[2] The criteria listed in Quality Assurance Code 50-C/SG-Q combine performance, intermediate, and subordinate objectives into a comprehensive package of basic requirements. One of these criteria, "work processes," is the generic representation of such performance objectives as research and development, maintenance, software development and use, operations, and data collection.

XA9848567

IMPROVED NUCLEAR POWER PLANT OPERATIONS THROUGH PERFORMANCE-BASED SAFETY REGULATION

M.W. GOLAY
Massachusetts Institute of Technology,
Cambridge, Massachusetts,
United States of America

Abstract

The US Nuclear Regulatory Commission (NRC) has recently instituted use of Risk-Informed, Performance-Based Regulation (RIPBR) for protecting public safety in the use of nuclear power. This was done most importantly during June 1997 in issuance of revised Regulatory Guides and Standard Review Plan (SRP) guidance to licensees and the NRC staff. The porpoise of RIPBR is to replace the previously-used system of prescriptive regulation, which focuses upon what licensees must do, to a system which focuses upon what they must achieve. RIPBR is goals-oriented and the previous system is means-oriented.

This regulatory change is potentially revolutionary, and offers many opportunities for improving the efficiency of improving both nuclear power operations and safety. However, it must be nurtured carefully if is to be successful. The work reported in this paper is concerned with showing how RIPBR can be implemented successfully, with benefits in both areas being attained,. It is also concerned with how several of the practical barriers to establishing a workable new regulatory system can be overcome.

This work, sponsored by the US Dept. Of Energy, is being performed in collaboration with Northeast Utilities Services Corp. and the Idaho National Engineering Laboratory. In our work we have examined a practical safety-related example at the Millstone 3 nuclear power station for implementation of RIPBR. In this examination we have formulated a set of modifications to the plant's technical specifications, and are in the process of investigating their bases and refining the modifications.

INTRODUCTION TO PERFORMANCE-BASED REGULATION

The Nature and Status of Performance-Based Nuclear Safety Regulation

Performance-based nuclear safety regulation is a method of obtaining a high level of nuclear safety by focusing regulations upon the desired safety results rather than upon the means by which they may be obtained. The latter approach, termed prescriptive regulation, has been the traditional treatment in the United States from the start of the nuclear power era until today. It has been criticized for being inconsistent, arbitrary and needlessly burdensome. Performance-based regulation has come into use on a limited trial basis as a response to the weaknesses of the current system.

The arbitrariness of the current prescriptive regulatory structure was illustrated in the example of the Department of Energy's new production reactor (NPR), a project terminated in 1993. The Secretary of Energy, James Watkins, decreed that the NPR should be as safe as the civilian power reactors. Unfortunately for his staff they found that they could not state what that meant, as the roughly 110 civilian reactors differ greatly in terms of the various measures of safety by which they are evaluated. Ultimately this puzzle was left unsolved, as the NPR project was canceled in its early stages.

Under performance-based regulation the safety regulator [the Nuclear Regulatory Commission (NRC)] negotiates an agreement with a nuclear power plant license holder regarding what performance goals will be required, how complacence will be measured and

what corrective actions would be required should compliance not be achieved. The primary means of demonstrating compliance is through performance tests of systems and personnel. To-date, performance-based regulation has been employed in small-scale regulatory experiments concerned with reducing regulations which are burdensome and providing only small safety benefits (e.g., containment leak rate testing, and quality assurance (QA) requirements). Under performance-based regulation ultimately the documented pedigree required of "safety grade" plant components required to show that they have been manufactured using NRC-approved facilities and processes would be replaced by test data indicating the expected reliability of the components. This replacement has not yet occurred, but the number of components requiring full documentation is being reduced.

A more substantial use of performance-based regulation came into effect in July 1996 in the form of the "Maintenance Rule." The requirements of the "Maintenance Rule" utilize probabilistic risk assessment (PRA) as a method for prioritizing the devotion of maintenance-related resources among the various plant SSCs (Systems, Structures and Components). This prioritization is intended to ensure that the SSCs which are most important for maintaining current levels of safety receive their proportionate share of available resources. A similar prioritization can be used subsequently to ensure that any additional resources are devoted to improving the SSCs which would be most valuable in increasing safety performance.

The primary vehicles of RIPBR advancement are the Maintenance Rule implementation and a set of "Pilot Projects" investigating various regulatory examples. These include:

- o In-service testing and in-service inspections
- o Graded quality assurance
- o Technical specifications modifications
- o Allowed outage times.

The NRC has indicated that some licensee benefits are likely to be allowed in the near future in theses regulatory experiments. If this is done the impetus for widespread utilization of RIPBR could be substantial.

Currently probabilistic risk assessment techniques (i.e., models, modeling assumptions and data bases) are not sufficiently accurate and reproducible that such analyses can be employed without review and refinement by experienced engineers. Thus, it has become common in use of probabilistic risk assessment under the Maintenance Rule to require use of subjective judgment by an expert panel of its results before they can be used as a decision-making basis.

Should the need for plant modifications also be indicated, the expected performance of the modified systems, structures and components would first be analyzed using the sorts of deterministic methods which have always been at the heart of nuclear safety analysis. Then the priority for assignment of safety-related maintenance resources would be determined through probabilistic risk assessment followed by expert evaluation. Regulatory compliance tests and potential corrective remedies would be negotiated as the basis of that system, structure, or component's future maintenance plan.

In order to stimulate this examination each power plant licensee has been required to submit a plant-specific version of a PRA under the Individual Plant Examination (IPE) and the Individual Plant Examination - External Events (IPEEE) programs; these PRAs identify individual plant risk vulnerabilities and provide a measure of the variation of risk measures among the set of US nuclear power plants. These reports have been partially evaluated by the NRC staff, with AN interim Evaluation Report and to be issued shortly.

Finally, in more recent action the NRC Chairman, Dr. S. A. Jackson, in 1996 gave a priority to moving the NRC to using what she terms "risk-informed performance based regulation." In order to speed this transition she has directed the NRC staff to reformulate its Standard Review Plan and to issue corresponding Regulatory Guides for the use of

licensees, to incorporate use of PBR with PRA by the end of 1996. This has been done and these documents have now been released for public review.

Each of these documents follow a standard, high level, structure for proposal and evaluation of license-requirement changes under RIPBR as follows:

1. Describe the change and its rationale.
2. Perform an engineering evaluation of the change
   - 2.1 A traditional deterministic evaluation showing that current regulations are satisfied, and that the requirements for conservatism and defense in-depth are satisfied.
   - 2.2 A (newly required) probabilistic risk evaluation, showing that the risk implications of the change are small, and hopefully beneficial.
3. Formulate a plan for monitoring the implementation of the change, ensuring that the associated performance goals will be met.
4. Document the change proposal.

The NRC has undertaken expanding the set of staff knowledgeable about and able to use PRAs in their work, and has begun guiding standardized treatments of PRA modeling and data bases; this work will require some years to complete, but is important for having been started. The treatment of uncertainty is one of the most important outstanding areas of work.

The Decision-Making Bases of Performance-Based Regulation

The previous paragraph illustrates the interplay of the major decision-making bases of performance-based regulation. They are listed in Table 1 in order of importance, with examples of where in the overall nuclear safety problem each basis is particularly valuable.

The primary basis of performance-based regulation is Tests of performance. This is the case because such tests, where appropriate, are the most accurate and least ambiguous of the performance-based regulation decision making bases.

Supporting Tests as the primary decision basis are both probabilistic risk assessment and deterministic analyses. Each class of analysis has particular areas of strength within the overall safety evaluation problem, as illustrated by the examples of Table 1. Deterministic analyses are most valuable in prediction of nominal SSC performance and for incorporation of conservative bias.

Probabilistic risk assessments are most valuable for sensitivity analyses of expected system performance, and for identifying the relative importance of the different systems, structures and components within a system. From this discussion it is seen that risk assessments provide one of the important bases of performance-based regulation, but are far from providing the entire overall evaluation of safety. In discussions of how performance-based regulation should be structured this point is often confused because excessive attention is sometimes paid to the role of probabilistic risk assessment in restructuring nuclear safety decision-making. This is because probabilistic risk assessment is still in an early stage of development, because a plan for how it should be used in a comprehensive regulatory system is still evolving, and because its initiation will be a major undertaking. This paper is intended to contribute to the evolution of that plan.

Regardless of how probabilistic risk assessment is used ultimately its implementation as a routine regulatory tool will be slow and expensive, both in terms of people and funds. This is because the decision-making tools currently utilized within the nuclear power industry will have to be augmented by those of probabilistic risk

Table 1

Foundation of Performance-Based Regulation

BASIS ELEMENT	AREAS OF BEST APPLICATION
Tests and Inspections	Actual system or component reliability or capability Personnel capabilities
Deterministic Analyses (sometimes with conservative bias)	Plant and system design
PRA (basis of Risk-Based Regulation)	System reliability analysis System vulnerability analysis System improvement analysis
Subjective Judgment	Very complex or poorly understood phenomena • Severe accidents • Personnel behavior

assessment. Doing this will require creation of convenient NRC-approved models, modeling treatment and data bases (which will require continual refinement as new data are generated). The precedent of the 1970s emergency core cooling system (ECCS) analysis treatment by the NRC is relevant. In this case the agency identified computer codes, modeling assumptions and data, and the agency stated that it would accept analyses resulting from their use.

An additional objection to use of probabilistic risk assessment which is sometimes raised is that it is too uncertain to be used in regulation. It is important to note that the uncertainty of our knowledge of the safety of a nuclear power plant is only reduced, not raised, through use of probabilistic risk assessment. Thus, the existence of uncertainty in probabilistic risk assessments provides no reason for not using them. This uncertainty is inherent in the design and phenomena of the plant. Use of probabilistic risk assessment can illuminate the existence of areas of uncertainty, but it does not create them. Rather, in the absence of probabilistic risk assessment, the social bargains embedded in the current regulatory process may accommodate or even disguise the existing uncertainties, but they do not eliminate them.

Subjective (i.e., expert) judgments play a natural role in portions of the safety problem where the previous three methods are insufficiently accurate to provide a reliable decision basis. A role for informed subjective judgment has been encouraged in plans for implementation of the Maintenance Rule. However, more generally the United States nuclear regulatory system has underutilized this decision-making basis—mainly because it is ill-suited to quantification. This policy is inconsistent with most of human experience, where the most important decisions, from the choice of a spouse to the election of acceptable risks, are based upon informal subjective evaluations. One of the great opportunities within performance-based regulation for improving safety decisions is in providing for more widespread explicit use of subjective judgment processes in the many areas of decision-making where it can serve best.

Notably, the NRC has long used subjective judgment in the regulatory process, but to a too-limited extent. Relevant examples include the work of the NRC commissioners themselves, of the Atomic Safety and Licensing Boards, and of the Advisory Committee on Reactor Safeguards.

RESEARCH PROJECT ON PERFORMANCE-BASED REGULATION

The main objective behind employing performance based regulation in nuclear power plants is to enhance the performance of the plants such that operational safety is not only maintained but improved. We illustrate the benefits and requirements of RIPBR in the project on Integrated Models, Data Bases And Practices needed for Performance-Based Safety Regulation. It is sponsored by the US Dept. Of Energy, is being performed in collaboration with Northeast Utilities Services Corp. and the Idaho National Engineering Laboratory. The purpose of the project is to investigate and demonstrate the potential benefits of performance-based safety regulation (PBR), or as it has become know more recently risk-informed, performance-based regulation (RIPBR). These goals are explained further in the abstract from the project proposal, as follows:

"It is proposed to develop tools, methods and practices to support both the US Nuclear Regulatory Commission (NRC) and nuclear power industry in structuring a practical approach to performance-based safety regulation. Success in this work will improve the safety of operating nuclear power plants and permit much more efficient use of nuclear power plant resources. The project's results can improve the capabilities of the INEL and enable the NRC to build the foundations and framework for performance-based regulation. The tools and practices developed in this work will demonstrate that the framework is realistic, and that the goals are achievable. At all stages of the project emphasis will be given to insights gained from industry experience. This is likely to produce results having a high acceptance level with not only the NRC but also with the nuclear industry."

We have focused our project's work upon the surveillances and maintenance activities associated with the emergency diesel generators (EDG) of the Millstone 3 (MP-3) PWR nuclear power plant. The reasons for this choice are that:

1. The EDGs are very important for safety, having the highest value of the Fusell-Vesely risk importance measure for core damage frequency (CDF) at that plant—meaning that failure of the EDGs would contribute more to core damage risks than would failure of any other system in the plant.
2. The EDGs require frequent surveillance testing and mandatory maintenance, as required by the technical specifications, with the objective basis of these requirements never having been established.
3. Potentially improvements in terms of both safety and economics can be achieved by basing future requirements in these areas upon risk-based arguments.
4. The EDG system has a reliability goal that is set by the Station Blackout (SBO) rule.[1]

In addition to the EDG requirements at MP-3 we have also investigated the practices and bases of the NRC treatments of EDGs for nuclear power plant licensees, and for similar activities in other industries (i.e., the U.S. Navy, the Federal Aviation Administration and civilian hospitals).

Emergency Diesel Generator System Description

A central concept upon which nuclear power plants are built is that of redundancy in safety system and their components. Redundancy is employed in order to safeguard against failures of single component systems. One of the backup systems incorporated in nuclear power plants is an onsite emergency power supply system. Most power plants utilize diesel generators for that purpose. Typically, a plant has at least two independent emergency power supply trains and each is connected to an emergency diesel generator EDG. In the case of MP-3 each of the two generators is a 4.6 kV, 3 phase, 60 Hz diesel engine-driven generator.[2,3] The capacity of each generator is 4,986 kW continuously, or 5,335 kW for 2,000 hr. Each EDG has independent support systems to minimize common cause failures. An EDG's system components and related support systems are shown

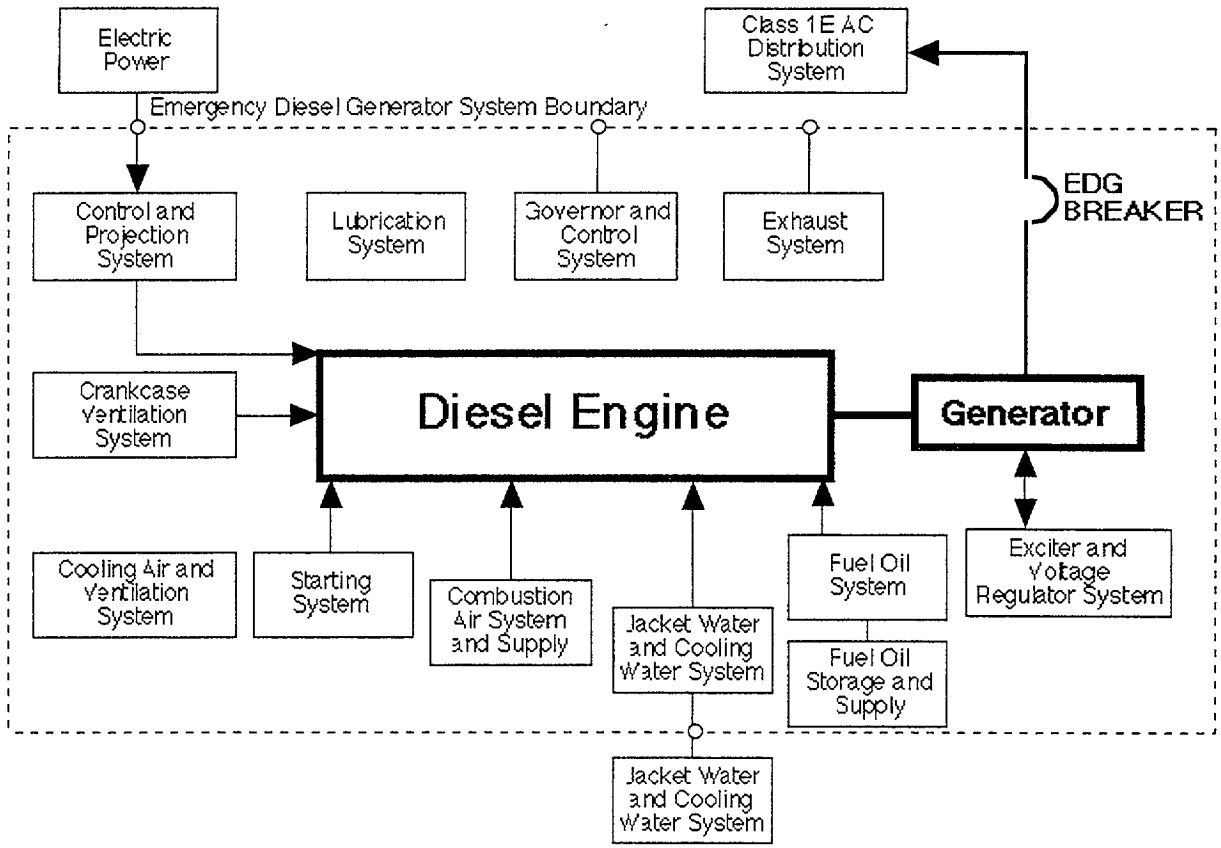


Figure 1. Boundary and Support System of Emergency Diesel Generator System

TABLE 2. Millstone-3 EDG Surveillance Requirements

Test Number (Refer to MP-3-TS)	**Purpose**	**Frequency**
4.8.1.1.1	Verify correct breaker alignments	Weekly
4.8.1.1.2 (a-f)*	Availability tests that start, load and operate the EDG for 60 min.	Monthly unless number of test failures ≤ 4 in the last 100 tests**
4.8.1.1.2.g	Perform inspection in accordance with manufacturer's instructions in addition to operating the generator for 24 hr.	18 months (every refueling)
4.8.1.1.2.h	Start both generators simultaneously to verify independence	10 years
4.8.1.1.2.i	Clean fuel storage tank	10 years

* Test 4.8.1.1.2.b is carried out every 184 days and involves the same steps of 4.8.1.1.2.a

** The test frequency is once per 31 days if the number of failures in the last 20 tests is ≥ 1 or ≤ 4 in the last 100 tests. If the number of failures goes up to ≥ 2 in the last 20 tests or ≤ 5 in the last 100 tests the frequency is increased to every 7 days.

schematically in Fig. 1 where the dashed box defines the boundary of the system.[4] Among various support systems, Fig. 1 shows a starting system which provides compressed air to drive a pneumatic starter, a fuel supply system that has enough fuel capacity for the continuous operation of the generator for six days, and a cooling system which utilizes a shell and tube heat exchanger to cool the generator, transferring heat through a forced air ventilation system.

The main function of the generators is to supply power to the plant safety system in cases of emergency in order to assure that the plant is maintained in a safe condition until offsite power is restored. In order to ascertain that the generators and their supporting system perform their functions they must satisfy certain load and response criteria by design. In addition to meeting their design requirements, the generators must have sufficient reliability to maintain the risk of core damage at an acceptable low value. Hence, Criterion 18: *Inspection and Testing of Electric Power systems* of Appendix A to 10 CFR Part 50 [4] requires that electric power systems important to safety be designed to permit appropriate periodic inspection and testing in order to verify the operability of the systems and the condition of their components. The main concern of this project is the availability surveillance tests that are carried out on a monthly basis and the intrusive inspections done every refueling cycle.[3]

Surveillance Requirements of the Millstone-3 Technical Specifications

The Millstone-3 surveillance requirements (SR), as specified in the technical specifications (TS)[2], may be categorized according to the surveillance interval. The surveillance interval of the tests varies from a weekly to a once per decade basis. Table 2 summaries the most important tests involved, their purposes and their respective testing frequencies.

Changes in EDG Testing, Inspection and Monitoring Requirements

Our work, performed from the perspective of the licensee, has focused on identifying EDG maintenance and inspection requirements that may benefit from modification. We have also been concerned with justifying these changes with the help of data, expert testimony and by exploiting the capabilities of on-line equipment performance monitors. Our tentatively recommended replacement requirements are shown in Table 3. They will probably be revised. However, it is clear that the resource requirements needed to demonstrate that current safety levels are being maintained are considerably fewer than are currently demanded by regulations.

Table 3

Proposed Revised Testing and Inspection Requirements

- o Replacement of (monthly) test 4.8.1.1.2 (a-f) by an automatically executed EDG test to start, load fully (within 60 sec. except within 11 sec. once every 24 months) and run for 24 hours, required to be performed every six months (after further experience this interval might be lengthened, depending upon the observed results)

- o Elimination of (inspection) test 4.8.1.1.2.g, replaced by a program of on-line monitoring of the EDG and its support systems during its required tests

- o Elimination of test 7.5.9 (endurance and load test perfumed once per refueling interval)

- o Performance of load combination tests 7.5.6 through 7.5.13 once per decade (rather than once per refueling interval)

Tests:

An examination of licensee reporting data [5,6] concerning the results of required EDG tests indicates that few EDG failure occur involving the EDG itself. Most of the failures observed involve support systems, which typically receive less attention for maintaining good material condition than does the EDG itself. Also, it is observed that many of the observed failures occur during the infrequent long-duration tests performed during refueling shutdowns. Similar results have been reported concerning EDG tests on US Navy nuclear-powered vessels [7,8]. Also, an examination of the MP-3 EDG failure analysis in the plant-specific PRA indicates that the failure modes interrogated by the currently required monthly tests contribute only two percent of the total EDG-associated core damage frequency. Thus, these tests appear at best to be of slim value. Our work is now focusing upon justifying performance of more demanding tests on the EDGs and associated systems, and eliminating the currently-frequent, but probably meaningless, tests now required by the technical specifications. The exact nature and frequency of the tests to be required is still being determined.

Table 4

Colt-Pielstick -- PC2V Engine Instructions (Annual/Refuel)

1. Follow all preceding instructions.
2. Remove and check injection nozzles for operation and opening pressure.
3. Remove, disassemble, clean and repair all air start valves and air start distributors. Clean/replace air start distributor filter.
4. Drain and refill governor and turbochargers with approved oil.
5. Drain, flush and refill outboard bearing with approved oil.
6. Check tightness on all foundation, block to base, oil and water line bolts.
7. Check sample of rocker lube oil for condition and contaminants.
8. Check turbocharger inlet casing and turbo casing water passages for scale. The inside surface of these casings is the best indication for adequacy of water treatment.
9. Check for tightness of exhaust manifold flange bolts to cylinder head (165-195 ft.lbs.).
*10. Check all safety and shutdown controls for appropriate pressures and temperatures.
*11. Borescope all cylinder liners.
12. Inspect the crankcase end of all cylinder liners.
*13. Check main bearing cap tightness and side bolts. Alternately confirm cap tightness to frame and saddle to .0015 feeler gauge
14. Visually examine gear train and drives, cam shafts and bearings, push rods and rocker arms.
15. Check crankshaft alignment and bearing clearances.
16. Check connecting rod bearing clearances with feeler gauges.
17. Inspect all ledges and corners in crankcase for debris which could indicate other mechanical problems. Confirm all cotters, safety wire and lock tabs are in place and tight.
18. Water test engine and inspect for internal and external leaks. Isolate J.W. surge tank and test entire systems at 40 psi. After engine is returned to operation and has reached normal operating temperature, remove each rocker cover and inspect for water leaks at top area of cylinder head.
19. Check alternator coils and poles for indication of movement (visual).
20. Drain and refill alternator bearing lube sump. If oil has contaminates, pull bearing cap and inspect journal.
21. Inspect and clean (if required) overspeed trip mechanism. Check operation according to overspeed trip test instructions.
*Identified as excessively intrusive (MP-3 systems Engineer)

Inspections:

Available data[5,6] and interview reports from individual power stations and the US Navy indicate that EDG inspections almost never reveal important component faults; however, they provide new opportunities for introducing defects. Thus, it appears that the need for the current practice of partial dismantling, and subsequent reassembling of the EDGs (see Table 3) during each refueling outage is unjustified, in view of the opportunities to damage or misalign the EDG in the process.

We recently asked the MP-3 EDG systems engineer[9] to review the current general refueling inspection guidelines and separate each of the requirements into one of three categories:

1) Items that can be justifiably eliminated from the Technical Specifications inspection program,
2) Items that can be performed on-line with the plant operating at high power, and
3) Necessary items that cannot be performed on-line.

Of the 21 general items (see Table 4), he indicated that a majority of the surveillances could be performed on line or at more extended intervals. He also indicated that none of the required items would fit into the third category. He also identified the most intrusive inspection items and recommended that they by eliminated or made less intrusive.

Notably, we have found that similar inspections are not required for EDG used in hospitals and federal air traffic control centers (see Table 5). Thus, we are recommending that such inspections be made far less intrusive and less frequent (i.e., once per decade, or - later - never).

Table 5.

Non-nuclear Industry EDG Reliability Practices

	MP-3	U.S. Navy	Cambridge Hospital	FAA
Monthly Loaded Test	1 hour	30 minute minimum	1 hour	1 hour
Yearly Loaded Test	24 hours	Unavailable	Semi-annually, simulate blackout, no set time	4 hours
Major Maintenance	18 months	Annually	Semi-annually, contracted	Annually
Overhaul	18 months	Infrequently	Infrequently	As needed

Monitoring:

EDGs and supporting systems have traditionally been monitored during required tests, to the extent that available technologies have permitted. However, such activities have not typically been recognized in required EDG reliability ensuring programs. Recent advances in computer technologies have greatly increased the value of monitoring, as a supplement to frequent tests and inspections, as the need for highly trained humans is replaced by development of smart instrumentation, able to identify trends and indications of incipient failures and degrading component performance.

From the available data, we have determined which systems are the best candidates for monitoring, and which parameters are of most interest. The systems of interest are the diesel itself, cooling systems, air systems, lubricating and fuel oil systems

turbot/superchargers, and instrumentation and controls. The last of these presents a serious concern, as we propose to increase the amount of instrumentation, while it is currently a significant problem. Table 3 lists the components and failure modes to be monitored, along with recommended monitoring parameters.

In the diesel, our goal is to accurately assess the chances that any failure mode currently covered in the technical specifications will occur during a given time period. Monitoring of cylinder pressures and temperatures, fuel injection, and bearing and cylinder vibrations covers the failure modes which are currently assessed with highly intrusive physical inspections. Also, oil analysis further guarantees proper operation, as is discussed concerning lubricating oil.

In the cooling systems, the major concerns are components such as pumps, valves, dampers, and fans, and the presence of leaks. For both the service water and ventilation, we have been formulating instrument systems to predict or locate weak components or leaks. Similarly, in the air systems, intake, exhaust, crankcase vacuum, and air-start, leaks and valves are the primary concerns. Pressure and flow sensors should allow small leaks and weakening components to be identified and located.

In the case of the lubricating oil system, instrumentation is used to predict and locate leaks, and to detect high or low pressure, high or low volume, and high temperature. In order to guarantee oil quality and the mechanical condition of the diesel accurately, chemical analysis of lubricating oil would remain a necessity in the absence of an acceptable sensor for determining the particulate content of the oil. Here, the buildup of combustible products or soot would indicate the presence of weak seals or rings, high water content would demonstrate gasket or engine block weaknesses, corrosion products would indicate oxidation problems, and metal particles would indicate insufficient lubrication or worn bearings or other critical components. Also, physical properties of the oil, such as viscosity, would indicate oil lubrication and high temperature performance.

In the fuel oil system, leaking and components like valves and pumps are certainly concerns requiring instrumentation, but also tank levels are a concern. Sensors can be used to eliminate storage and day tank level concerns which figure prominently in the EDG fault trees. Also, opacity sensors can be used in the light diesel fuel oil to guarantee cleanliness of fuel from tank scale or fungal growths.

The turbochargers and superchargers used are susceptible to the same sorts of failures as the diesels themselves, such as bearing failures, cooling failures, and lubricating oil problems. With vibration, temperature, and oil pressure sensors, turbocharger and supercharger faults can be predicted and repaired.

Against the recommended advantages above, there are certain disadvantages to the use of monitoring as well. To make these changes, the approval of the NRC would be required, involving a change to the technical specifications that govern plant operations. To change these technical specifications, the monitoring systems must not decrease safety and reliability levels as compared with the current physical inspections. The same possible failure modes should be tested, and no new serious failure modes should be introduced. As will be demonstrated further, we believe that current failure modes inspected can be tested equally or better with instrumentation. The greatest disadvantage is the possibility of introducing new failure modes. In particular, there are four possible new failures. The addition of intrusive vibration, temperature, pressure, and flow sensors can interfere with normal operations and prohibit correct system behavior, or can even introduce leaks or contamination in otherwise closed systems. The other errors possible would involve information reported and its use. Over-reliance on the monitoring systems could also lead to problems where the data reported are given more credence than good judgment and working experience. Also, the sensors could either falsely report a negative condition when none exists, or fail to report a negative condition when one should be reported. The former is a less serious concern, as a simple diagnostic check of the instrument could be conducted, or other related instrumentation could be checked for anomalies on report of an

error. However, the latter introduces new complications, as, without receiving any fault signals, there would be no reason to conduct diagnostic checks on the components being monitored. This problem requires that the instrumentation be extremely reliable or be used in voting systems, such as one using 2-out-of-3 systems failure logic.

Finally, instrumentation and control failures are a major concern, especially when more sensors are to be added to a system. The sensor problems reported are primarily trips of the diesel due to false negative signals. The occurrence of negative conditions which do not cause a necessary trip is extremely rare. This suggests that the false negative signals be followed up with diagnostic checks and consultation with other instrumentation, and system highly susceptible to give false positive signals be used in logical voting system This system would favor enhanced safety, with excess caution. To best represent the state of the system, however, false negative signals should be reduced as much as possible with higher quality sensing.

Research from INEL and plant experiences indicate that a monthly one-hour test run, as required in the MP-3 technical specifications, does not allow enough time to observe all possible failure modes, as some modes, such as vibration-induced failures, do not develop for several hours. In order to monitor the diesel through most of its possible failure opportunities, longer test runs would be required, but the increased reliability should allow monthly tests to be replaced with less frequent runs, such as on a quarterly basis. Thus engine wear would not be significantly increased, and the potentially harmful frequent starts would be reduced by two-thirds or more. Currently, we are seeking to demonstrate that diesel support systems could be operated on a monthly basis to insure their availability without running the diesel unnecessarily.

In the course of the project, two possible failure modes concurrent with the practice of pre-lubricating the EDGs have arisen, and are being explored currently. Both of these failure modes are exclusive to the opposed piston type of diesel engine. The first failure mode was experienced in Naval EDGs, which made the diesel unable to operate[6]. Prior to starting the diesel, lubricating oil could leak past the upper piston rings and fill the combustion chamber of a cylinder. When a start was attempted, the oil-filled cylinder performed as a hydraulic lock, preventing the motion of any pistons in the engine, failing it. The second failure mode was a problem characteristic to Fairbanks-Morse, or Colt-Pielstick opposed piston engines[7]. Similar to the previous failure mode, lubricating oil could leak past the upper set of pistons and fall into the combustion chamber. However, in these cases, the oil ran out the open exhaust ports and into the manifolds. In some cases, this oil ignited in the manifolds, causing a new diesel failure mode. The Fairbanks-Morse recommendation was to reduce the then-standard fifteen to thirty minute pre-lubrication to only two or three minutes. In consideration of the now constant pre-lubrication, these possible failure modes are currently being re-examined. The need for pre-lubrication is also in question, as engine wear was not necessarily significant, and we are now proposing fewer starts of the diesels.

Effects of Inspection Requirement Changes Upon Plant Operations:

It has become widely recognized that the times of greatest plant risk may not be when the plant is operating at high power, as had been commonly assumed for many years. Rather, when a plant is undergoing refueling its vulnerability for fuel damage due to fuel cooling failures may be considerably greater than when at high power. This is because of the greater complexity of plant configuration control. -- with an attendant increase in human error probabilities, and because of reduced redundancy in accomplishing the fuel cooling functions.

The requirements for EDG intrusive inspections and long duration tests exacerbate the possibilities of such cooling failures during refueling outages and may actually increase plant fuel damage risks. They also severely increase plant costs by lengthening such outages. We are now undertaking work to determine whether such inspections and tests should be moved on-line.

In examinations to-date of the MP-3 refueling outage schedule and risk profile it appears that the reduction of the outage critical path due to moving the EDG surviellances on-line would be modest (of the order of a few days). However, the risk implications could be large. However, fuel damage risks during outages are dominated by human errors. The major benefit of moving EDG work on-line may be to simplify the management of the outage, and thereby to reduce risks. Currently it appears so, but it is too early to say more.

CONCLUSIONS

Our primary results to-date indicate that most of the required EDG surviellances are not useful in reducing safety, and may actually reduce safety.

As the surveillance test and maintenance intervals are increased economic savings will be realized in a straightforward fashion. This is because the expenses for these activities scale with the number of test and repair operations. As their total over a plant's life is decreased savings will accrue directly. However, the greatest benefits of revised EDG requirements is likely to be reduced risks, by means of rationalizing those activities in terms of their overall risk and economic implications.

References

1) U..S. NRC, 'Evaluation of Station Blackout Accidents at Nuclear Power Plants', NUREG/CR-1032, June 1988.

2) Millstone-3 Technical Specifications.

3) Regulatory Guide 1.108, *Periodic Testing of Diesel Generator Units Used as Onsite Electric Power SysteMP at Nuclear Power Plants*, Revision 1, August 1997.

4) Regulatory Guide 1.9, *Selection, Design, Qualification, and Testing of Emergency Diesel Generator Units Used as Class 1E Onsite Electric Power system at Nuclear Power Plants*, Revision 3, July 1993.

5) Grant, G.M. et al. Emergency Diesel Generator Power System Reliability 1987-1993. Idaho National Engineering Laboratory, INEL-95/0035, February 1996.

6) Nuclear Plant Reliability Data System, INPO.

7) Grotsky, Peter. CVN-68 Class Emergency Diesel Generator (EDG) Reliability and Availability, 9233 Ser. 03X3/331, October 17, 1996.

8) Grotsky, Peter. Personal communication, November 1996.

9) Shanihan, B., per sonal communication May 1997.

XA9848568

WORK MANAGEMENT PRACTICES THAT REDUCE DOSE AND IMPROVE EFFICIENCY

D.W. MILLER, M. HULIN
University of Illinois,
Urbana, Illinois,
United States of America

Abstract

Work management practices at nuclear power plants can dramatically affect the outcome of annual site dose goals and outage costs. This presentation discusses global work management practices that contribute to dose reduction including work philosophy, work selection, work planning, work scheduling, worker training, work implementation and worker feedback.

The presentation is based on a two-year international effort (sponsored by NEA/IAEA ISOE) to study effective work practices that reduce dose. Experts in this area believe that effective work selection and planning practices can substantially reduce occupational dose during refueling outages. For example, some plants represented in the expert group complete refueling outages in 12-18 days (Finland) with doses below 0,90 person-Sv. Other plants typically have 50-75 day outages with substantially higher site doses. The fundamental reasons for longer outages and higher occupational doses are examined.

Good work management principles that have a proven track record of reducing occupational dose are summarized. Practical methods to reduce work duration and dose are explained. For example, scheduling at nuclear power plants can be improved by not only sequencing jobs on a time line but also including zone and resource-based considerations to avoid zone congestion and manpower delays. An on-going, global, benchmarking effort is described which provides current duration and dose information for repetitive jobs to participating utilities world-wide.

INTRODUCTION

In 1992, the Nuclear Energy Agency (NEA) established the Information System on Occupational Exposure (ISOE) to facilitate the global exchange of dose information. The goal of the program is to provide timely benchmarking of dose performance at nuclear power plants and promote effective dose reduction practices. Currently, over 300 nuclear power plants (70% of the world's operating plants), representing 17 countries, participate in ISOE making it one of the largest occupational exposure data bases in the world. National regulatory authorities from 11 countries also participate.

A Expert Group on Work Management was formed by the ISOE Steering Committee in 1994 to study global work management practices and their impact on occupational dose. Subject matter experts from Germany, France, Switzerland, Sweden, Finland, United Kingdom, Canada and United States participated in this international study.

WORK PHILOSOPHY

Operators of nuclear power plants generally establish their own standards to operate efficiently and safely. Utility standards are set to accomplish excellence in all aspects of nuclear power operations. Compliance with applicable regulatory requirements is also a significant part of work management. With respect to radiation exposure management, utilities endorse the ALARA concept because it is recognized that it is the right thing to do. ICRP 26 optimization concepts closely parallels overall work management objectives[1].

Occupational dose limits are set at levels considered to be safe as established by national and international scientific bodies. Both annual and lifetime accumulated dose are taken into consideration to assure all occupational doses are safe. Such limits provide operational flexibility as well as adequate safety as long as a highly visible and aggressive ALARA program is also in place. G. A. M. Webb, formerly of National Radiological Protection Board, UK, described ALARA as the optimisation of radiological protection: "A Developing Way of Thinking." Optimisation of protection, as developed by ICRP, has a sound philosophical basis. It promotes a management philosophy that associates quality control and excellence with safety and productivity, so that they are complementary rather than conflicting goals[2].

Richard E. Cunningham, U.S. Nuclear Regulatory Commission (retired), states that legislation and implementing regulations should avoid prescriptive specifications related to optimimisation methodologies and constraints. In part, this is due to methodologies and technologies usually changing faster than legislation and regulations which would result in sub-optimal conditions. High quality optimisation at the plant level is a continuing process of improvement with no endpoint but an increasing standards of performance curve[3].

WORK PLANNING

The objective of this paper is to identify the key elements of excellence in planning and execution of work that permit work activities at nuclear power plants to be accomplished safely and with minimal dose to the occupationally exposed workers. A key conclusion of the NEA international expert group who studied this topic is that when work is well planned, it is accomplished in less time (shorter outages), fewer man-hours (less dose) and higher plant availability (work efficiency).

WORK SCHEDULING

Work activities in nuclear power plants are carefully planned to assure that exposure to radiation fields is minimized. For example, proper planning reduces multiple entries as result of carefully planning each job step in a work activity. Plants that plan work most effectively have generally adopted a system of planning work activities by time, plant zone and support staff resources. The later two planning elements represent refinements from earlier power plant planning approaches which only organized work activities by time lines.

Work scheduling and planning refers to the process of planning a work activity so that the component, work area, primary craft and support staff are coordinated well on the outage schedule to achieve the highest practical work efficiency for the job without unduly compromising other concurrent jobs. This can be accomplished by implementing a disciplined approach to work planning and scheduling.

Outage experience has shown that planning must recognize not only the sequence of job steps on a time line but also the support services necessary to successfully complete the work in an efficient fashion. For example, planning by zone in the BWR drywell means assuring that multiple work packages for components in the drywell do not "stack" workers above other workers. Work inefficiencies, safety concerns and/or contamination problems can occur if the work area is congested. By scheduling work by zones and time, zone congestion is minimized by identifying trouble spots in the planning phase and providing an adequate degree of separation on the outage schedule.

Zone planning also evaluates all scheduled work on specific plant components to schedule when scaffolding is assembled, insulation removed and temporary shielding is installed. Improper planning can lead to multiple assembly and disassembly of the same scaffolding resulting in higher doses and work inefficiencies. The identification of potential work interferences on the plant master zone plan is often critical to the success or delay of scheduled work based on studies of plants which routinely achieve short outages.

WORK SELECTION

Selection of work to be included on a plant's outage schedule has become an area of increased management attention as nuclear utilities in many countries prepare for de-regulation of utilities in the future. Once the work scope is chosen, efficient work practices are critical to a utility's survival in the future highly competitive electric supply market. Many U.S. utilities have examined the European approaches to better understand the relationship between shorter refueling outages and reduction in occupational dose. Finland is the global leader in terms of shortest outage duration and low annual occupational dose.

Two Finnish nuclear power stations, TVO and Loviisa, have been among the world leaders in nuclear power plants. The plants consistently accomplish refueling outages in less than 25 days and outage occupational doses below 0,90 person-Sv per unit. United States attention has focused on European plant experience to improve outage management, specifically work scope selection. At Loviisa nuclear power station (PWR) their annual short outages (years 1,2,3) take 3 weeks and their long outage (year 4) takes 6-8 weeks. Outages at the BWR TVO (Olkiluotu) are normally of shorter duration (2 weeks).

The TVO plant works to a 10-year planning matrix. Only required work is approved at Loviisa; nice to do work is not allowed. Training of Finnish workers occurs in a carefully laid out plan from apprenticeship to journeyman levels similar to the German approach to craft worker training. Finnish attitudes about radiation protection and work performance is based on keeping the concepts simple and maintaining high performance accountability of plant workers and contractors[4].

B. Wahlstrom, Radiation Protection Manager, Loviisa Nuclear Power Plant, provides the following insights on evaluating the work scope for these remarkably short outage duration:

a. Jobs which are not performed cause no doses.
b. Many jobs will be suggested which should never be authorized.
c. If an outage will be prolonged by a single job, it will cause excessive radiation doses because other jobs also will proceed slower causing more time in the radiation area and more dose. Hence, postpone the work for a future outage after safety authority buy-in to the dose reduction justification.
d. Connect separate jobs into larger units performed during a long outage.
e. Recalculate overly conservative presumptions; use actual plant historical data, where possible.
f. Never perform Nice But Not Necessary jobs.
g. Every job will always take all the time it is allowed to take.
h. The optimum size of a work team is the smallest number of workers that can get the work finished on time.
i. Doing a job fast and well means doing it twice: Fast first, then well.

The Finnish approach is clearly where some aggressive U.S. nuclear utilities are heading. Several United States nuclear utilities have visited Finnish, Swedish, German, Swiss and French plants and returned to plan significantly shorter refueling outages. Adoption of multiple European work efficiency, work selection and planning processes has led to shorter outages and lower occupational doses at several United States plants over the past two years.

WORK IMPLEMENTATION

Work process controls are critical to the success of well planned outages. Radiation workers must be well trained before work in the plant is undertaken. Training needs to involve work process indoctrination for the plant's controlling documents including the maintenance work order, the radiation work permit, and industrial safety permit. The use of mock-up training is important.

The work site can be optimized by providing the necessary support equipment (scaffolding, temporary shielding, ventilation, area decontamination, insulation removal and lighting). Dose reduction techniques can be applied to the work site including system flushing, chemical decon and designating low dose waiting areas to stage craft workers. In certain situations, specialized tooling and/or robotics can be used to improve work efficiency and reduce dose. The repetitive nature of most component maintenance tasks at nuclear power plants justifies the resources expended to develop specialized tooling and robots. Although the initial cost may be high, over the 40-year life of the plant, the work efficiency and dose reduction benefits often demonstrate the merits of specialized tooling.

Feedback from workers is important to capture during the post-job debrief. Sweden has analyzed the dose reduction opportunities in part from worker feedback resulting in work management improvements including optimization of work force, better adapted tools, geographical transfer of work and use of past experience[5]. France has performed significant studies at multiple sites on work management efficiency related to working conditions including the effects of plant lighting, dress-out requirements, training, audio links and area congestion on occupational dose[6].

In BWRs, up to 65% of the total outage dose is received from work activities in the drywell[7]. Assignment of Drywell Work Coordinators and Managers whose sole purpose is work process control and monitoring has reduced work duration and dose in this critical plant location. The use of Make-It Happen Managers has also been an effective method of assuring continuous monitoring and field-coaching of the critical path work scope. Finally, dose accountability at the work foreman level is important to ensure buy-in to dose budgets at the task level.

WORK MANAGEMENT RESULTS

Achievement of dose reduction goals has been demonstrated at the Limerick Generating Station in (Pennsylvania, United States) during the past three refueling outages in 1994-96. Shorter refueling outages were accomplished by carefully selecting outage work and thoroughly planning the outage work. Limerick Unit 1 completed its outage in 35 days in 1994; Unit 2 in 23 days in 1995; Unit 1 completed its outage in 24 days in 1996. The four previous outages at Unit 1 had taken from 100 to 127 days.

European plants were visited by plant supervisors in 1994 to develop improved management approaches to optimizing outage performance from work planning to work implementation. Cofrentes in Spain and KKL Leibstadt in Switzerland were visited because of their similar design and outage durations

consistently below 35 days. The radiation protection practices observed at European plants were implemented at Limerick to achieve efficiency of work practices and adequacy of radiological controls. Specific radiation protection initiatives introduced at Limerick include an electronic dosimetry system, in-plant break areas, scrub suits, zone mapping and integration of the maintenance work order process and radiation work permit. Outage successes in 1995 & 1996 has assured Limerick's continued industry ALARA leadership as one of the lowest annual personRem BWRs in the US[8].

SUMMARY

Key to the European successes in work management is the quality of training provided to the worker, the longevity of workers in their craft, the disciplined approach to work scope selection and the comprehensive nature of the site planning matrixes (10 year planning matrixes). Adoption of some of these work management practices at United States plants have led to markedly reduced outage durations and occupation dose without compromising safety of the plant or worker.

REFERENCES

1. ICRP International Commission of Radiological Protection. Recommendations of International Commission on Radiation Protection, ICRP-Publication 26 (Pergamon Press, New York).
2. G.A.M. Webb, OPTIMISATION OF RADIOLOGICAL PROTECTION: A DEVELOPING WAY OF THINKING, Fourth European Scientific Seminar on Radiation Protection Optimisation, CEC, Luxembourg (April 1993).
3. R.E. Cunningham and C.A. McKenney, RADIATION PROTECTION OPTIMISATION THROUGH REGULATION: A VIEWPOINT FROM THE AMERICAS, Fourth European Scientific Seminar on Radiation Protection Optimisation, CEC, Luxembourg (April 1993).
4. B. Wahlstrom, UNDERSTANDING RADIATION, Medical Physics Publishing, Madison, Wisconsin (1995).
5. K. Egner, A RADIATION PROTECTION APPROACH TO THE IMPLEMENTATION OF WORK MANAGEMENT, NEA Workshop, Paris, France,(November 1995).
6. C. Viktorsson and C. Schieber, OCCUPATIONAL DOSE REDUCTION AT NUCLEAR INSTALLATIONS THROUGH WORK MANAGEMENT AND ALARA, Embedded Topical Meeting on Occupational Radiation Protection in NPPs, ENC meeting, LYON, Occupational Radiation Protection in NPPs (October 1994).
7. C. Viktorsson, WORK MANAGEMENT TO REDUCE OCCUPATIONAL DOSES, NEA Workshop Proceedings, Paris, France, (February 1992).
8. C. Maletskos, ed. RADIATION PROTECTION AT NUCLEAR REACTORS, Medical Physics Publishing, Madison, Wisconsin (1995).

IMPROVING AVAILABILITY AND RELIABILITY THROUGH BETTER USE OF TODAY'S TECHNOLOGIES

(Session 2)

Chairman

M. MARTIN-ONRAET
France

NEXT PAGE(S) left BLANK

PUMP SYSTEM CHARACTERIZATION AND RELIABILITY ENHANCEMENT

R.H. STAUNTON*
Oak Ridge National Laboratory,
Oak Ridge, Tennessee,
United States of America

XA9848569

Abstract

Pump characterization studies were performed at the Oak Ridge National Laboratory (ORNL) to review and analyze six years (1990-1995) of data from pump systems at domestic nuclear plants. The studies considered not only pumps and pump motors but also pump-related circuit breakers and turbine drives (i.e., the pump *system*). One significant finding was that the number of "significant" failures of the pump circuit breaker exceeds the number of significant failures of the pump itself. The study also shows how regulatory code testing was designed for the pump only and therefore did not lead to the discovery of other significant pump system failures. Potential diagnostic technologies, both experimental and mature, suitable for on-line and off-line pump testing were identified. The study does not select or recommend technologies but proposes diagnostic technologies and monitoring techniques that should be further evaluated/developed for making meaningful and critically-needed improvements in the reliability of the pump system.

1. INTRODUCTION

The Nuclear Regulatory Commission (NRC)-sponsored characterization of pump failure data for the years 1990 through 1993, inclusively, was prepared at the Oak Ridge National Laboratory (ORNL) and issued in January 1996 [1]. An aging report on turbine drives was also prepared and issued by ORNL in June 1995 [2]. Following these studies, an update report [3] was prepared to characterize data for 1994 and 1995. Most recently, a report [4] on diagnostics was prepared to address technical needs evident in the two characterization studies.

The pump data characterizations consider pumps, pump motors, turbine drives, and pump-related circuit breakers and therefore encompass the entire pump *system*. The characterization made possible the realization (see Fig. 1) that the pump-related circuit breakers in this, their first data analysis, were exhibiting a failure rate (i.e., significant failures only) exceeding that of the pumps themselves [3].

The more recent characterization study showed how the turbine drives for pump systems, though small in number relative to motor drives, are exhibiting a very high failure rate. The study

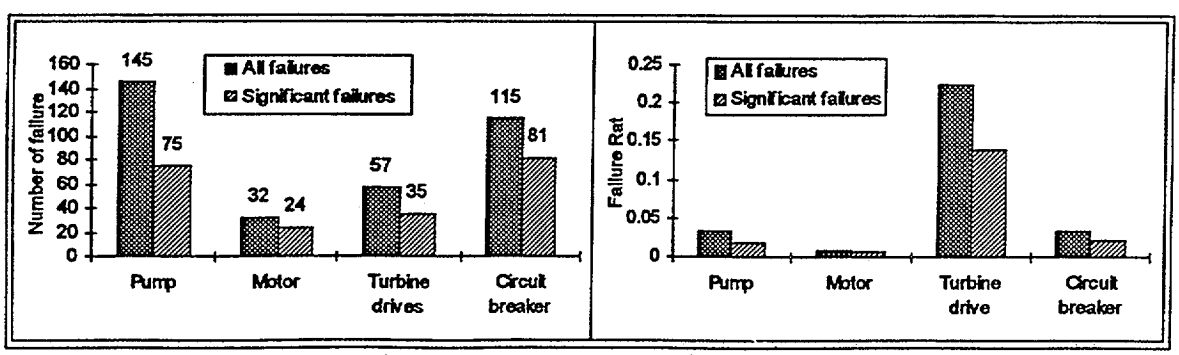


Fig. 1 Failure counts/rates for pumps, motors, turbine drives, and circuit breakers

*Present address: Lockheed Martin Energy Research, P.O. Box 2009, Oak Ridge, TN 37831-8038, United States of America.

also shows how regulatory code testing, that was designed for the pump only, does not lead to the discovery of other significant pump system failures. These findings, coupled with the need to utilize risk-informed methods in development of programs for in-service testing (IST) of components, made clear the need for a pump system diagnostic study.

2. INDIVIDUAL COMPONENTS

2.1. Pumps

Pump failures involve degradation in a number of areas such as internals (e.g., impeller, wear rings) and the bearing. The pump failure data from the two year study is summarized in Table 1 according to plant type and significance.

Pump failures vary widely depending on the pump system. As indicated in Fig. 2, failures are mostly in high-usage systems such as the Emergency Service Water (ESW) system [3]. The system usage in the High Pressure Safety Injection (HPSI) system varies from plant to plant but, in general, usage is high in this system. Failures also vary significantly by age group however, the trend is different for PWRs and BWRs.

TABLE 1 PUMP FAILURES BY AFFECTED AREA AND SIGNIFICANCE

Affected Area	PWR		BWR	
	All	Significant	All	Significant
Internals	34	31	14	12
Bearing	22	13	7	7
Seal, packing	36	8	7	2
Shaft, coupling, keys	10	6	4	3
Other	31	8	5	0

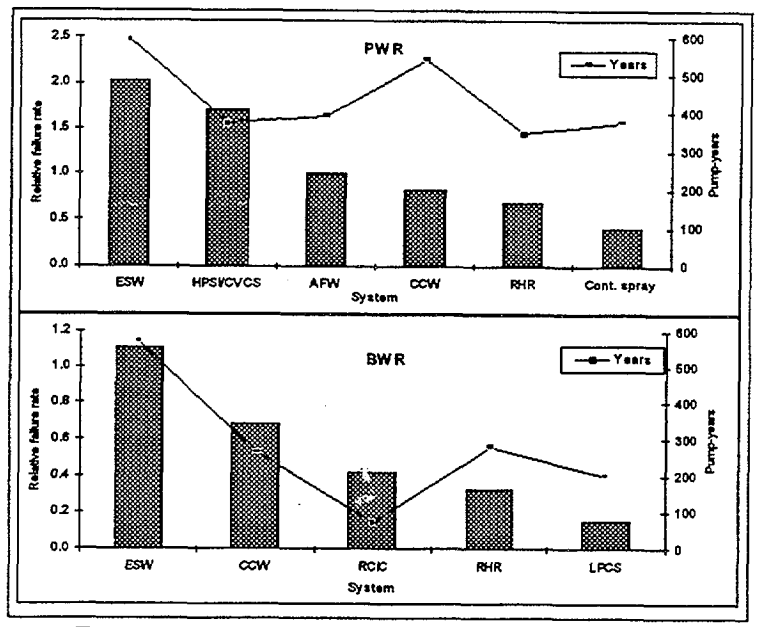


Fig. 2 Distribution of failures by System - PWR & BWR

There is little that needs to be said about motor failure data. The failure rate for motors is relatively low; when failures do occur they are generally severe, and the failures involve primarily bearing and stator degradation.

2.2. **Circuit Breakers**

As mentioned, circuit breakers experienced more significant failures than pumps themselves (i.e., 81 failures vs. 75 failures) based on the two year study [3]. In a high percentage of cases, the failures are quite severe in that they prevent the pump from performing its intended purpose. In fact, the four most frequent indicators of circuit breaker failure in the two year study are failure of breaker to close (32%), pump stops/spurious trip (13%), failure of the circuit breaker to charge springs (13%), and failure to trip (11%).

The failures are spread over many component areas as indicated in Fig. 3 and involve various types of electro/mechanical components. The failure mechanisms undoubtedly are also diverse. These considerations suggest that it will be a formidable challenge if corrective action or reliability improvement is sought.

2.3. **Turbine Drives**

The "turbine drive" is defined as an assortment of components (e.g., numerous steam valves and speed control devices) combined with the turbine drive to create a turbine drive *system*. Because of their small population, Code testing of pumps involved turbine drives in only 3% of the cases. The turbine drive failure rate is several times the rate for pumps and circuit breakers. This is of much concern since turbine drive pumps are so important in mitigating accidents involving station blackout failures.

3. PUMP SYSTEM TESTING AND INDUSTRY NEEDS

Significant failures are discovered through Regulatory or Code testing in pumps much more often than in other components of the pump system. In pumps, Code testing reveals 45% of the failures while it reveals only 13% of the failures for motors and 0% for turbine drives and circuit breakers. Even for the pump itself, the testing is of narrow scope. Code testing is effective only in detecting degraded hydraulic performance; its use of pump shaft vibration velocity to detect bearing failure is only effective in cases where bearing degradation is severe.

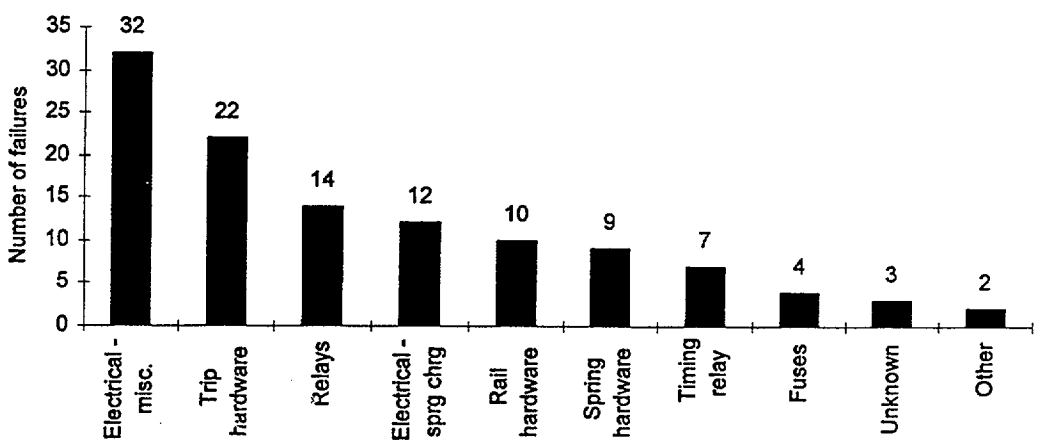


Fig. 3 Circuit breaker failures by affected area

Testing of pump bearing lubrication, motor stator megger tests, turbine drive speed regulation monitoring, maintenance/testing of circuit breakers per manufacturer's, and regulatory code testing of pump vibration and hydraulic performance have been performed in the nuclear industry since the beginning. Newer technologies such as pump motor current signature analysis have seen limited use at certain plants.

Many presently-used tests need to be upgraded or augmented to most effectively support IST. For instance, while the code-specified vibration tests that are performed on pumps as part of the surveillance testing are ineffective in detecting bearing problems, vibration spectral analysis, if performed correctly, *is* effective in the detection of bearing problems and other anomalies as well.

4.0 DIAGNOSTICS/MONITORING NEEDS

4.1 System or root causes of failures

In the diagnostics study [4], care was used not to analyze performance data without appropriate attention being given to system causes (i.e., root causes) of pump system degradation/unreliability. The usefulness of the study would be compromised if various tools for monitoring and diagnosing pump degradation were identified and eventually implemented while the root causes that lead to the degradation continue unchecked. Table 2 presents some potential system causes of certain failures. Examples are shaft misalignment, shaft imbalance, high vibration, poor pump/motor base integrity, and design weaknesses.

The importance of shaft alignment is known to be critical, however it is not possible to determine how many of the bearing and seal/packing failures are related to less-than-desirable precision in the alignment. Most of these system problems and/or root causes need to be precluded early on

TABLE 2 POSSIBLE ROOT CAUSES FOR SIGNIFICANT PUMP SYSTEM FAILURES

Component	Affected area	Possible root causes
Turbine drive	GV stem	Design (i.e., material selection), frequency of testing/low duty cycle resulting in a wet stagnant environment and corrosion
Circuit breaker Circuit breaker Turbine drive Motor	misc. electrical relays governor stator	Environmental stress, normal wear
Circuit breaker Turbine drive Circuit breaker Circuit breaker	trip-related HW trip-related HW Electrical - CS[a] spring hardware	Frequency/quality of maintenance, alignment, environmental stress
Turbine drive	GV	Corrosion, foreign material, normal wear
Pump Motor	bearing bearing	poor shaft alignment, hydraulic instability, high vibration,[b] oil contamination, loss of lubrication, normal wear
Pump	shaft/coupling	poor shaft alignment, hydraulic instability, high casing stresses, hydrogen embrittlement, high vibration[b]
Pump	internals	poor water quality, low suction pressure, off-design operation, normal wear
Pump	seal/packing	poor shaft alignment, hydraulic instability, normal wear

(a) CS = charging spring
(b) caused by a variety of factors, such as hydraulic and mechanical imbalances to the bearing (e.g., material deposition on impeller, cavitation, vane fracture), poor motor base integrity, and/or by stresses transmitted by attached piping

(e.g., by the use of precision alignment) and also detected through monitoring or found by inspection (e.g., integrity of pump base plate) in order to reduce the number of significant failures.

4.3 **Diagnostic technology and monitoring techniques**

Diagnostic technology and monitoring techniques that are (1) capable of detecting degradation and (2) useful, in some instances, for trending the aging of components were identified at the completion of the above data analysis. The pump system diagnostic tools suitable for off-line use are presented in Table 3 and the diagnostic tools suitable for on-line use are presented in Table 4.

4.3.1 Timed response and electrical monitoring

Nearly all of the significant failures of the pump-related circuit breakers involved a failure to close or remain closed. The failures were due to ordinary loose fasteners, cracked parts, gummed-up linkages, lack of lubrication, incorrect adjustment, worn hardware, and failed electrical components such as solenoids, switches, relays, etc.

Timed response testing involves a measurement of significant response times in single- or multi-part systems. Response might be measured beginning with a command signal and ending with the completion of the commanded sequence. This sequence can be a sequence of events such as ones brought upon by the rotation of a cam and activation of switches.

Other types of monitoring that may be applied at the same time signals are being obtained for timed response are the monitoring of current, voltage duration, and transition waveforms. Monitoring current or voltage duration for a circuit breaker relay or solenoid can reflect the effort required to activate, force required for full travel, and whether it successfully made the full travel. Transition waveforms are useful as an indicator of degradation of electrical components such as switches and motors. Switch bounce, current-induced arcing, and surge current are examples of anomalies that are evident with such monitoring.

4.3.2 Motor stator testing methods

An important, new, off-line motor stator test for three phase motors is the measurement of inductive imbalance. Inductive imbalance in the windings can be caused by poor manufacturing or rewinding techniques, emerging shorts between turns, partially open windings, phase-to-phase current leakage paths, and internal high resistance joints.

The primary methods of testing the motor stator on-line are electrical signature analysis (ESA), partial discharge tests, and high frequency waveform analysis. ESA uses fast Fourier transform (FFT) analysis of the motor current waveform to identify degradation of the stator windings. This degradation can either be shorted windings or significant changes in the winding capacitance or insulation integrity.

The partial discharge test can be performed on motors that operate on over 4 kv. This test determines whether localized discharges are occurring in the stator windings due to degradation of the insulation.

The high frequency waveform analysis method (developmental) uses special characterization of high frequency spectra to determine the presence of stator winding degradation.

TABLE 3 OFF-LINE DIAGNOSTIC/MONITORING METHODS AND PARAMETERS/CRITERIA

Affected area	Methods	Parameters/Criteria
Circuit breaker misc. electrical Circuit breaker relays	Periodic servicing	Manufacturer's specifications
Motor stator	Megger test and polarization index	Established test parameters - finds moisture
	ac and dc high potential tests	Established test parameters - can cause damage
	Inductive imbalance[a]	Trend and monitor imbalance in windings
Turbine drive governor	Monitor lubrication (flyball)	General oil quality - no dirt/water
	None (electrohydraulic units)	Either failed or not failed
Circuit breaker trip-related HW Turbine drive trip-related HW Circuit breaker electrical - CS[b] Circuit breaker spring hardware	Inspection	Manufacturer's specifications
	Periodic servicing	Manufacturer's specifications
Turbine drive GV	Inspection of valve movement	Stem must move freely
Pump bearing Motor bearing	Inspect lubrication system	Visual
Pump shaft/coupling	Alignment check/monitor	Precision alignment
	Inspection of coupling	Visual - no significant wear
Pump internals	Disassembly and inspection	No erosion, foreign materials, out-of-spec conditions in rotating hardware or wear ring
Pump seal/packing	Inspection	Visual - no leakage while off-line

(a) Development required
(b) CS = charging spring

TABLE 4 ON-LINE DIAGNOSTIC/MONITORING METHODS AND PARAMETERS/CRITERIA

Affected area	Methods	Parameters/Criteria
Circuit breaker misc. electrical Circuit breaker relays Circuit breaker electrical - CS	Timed response Current Transition waveforms	Command to response times Current level as an indicator of effort (circuit breaker motor) Waveform trending as indicator of component degradation
Motor stator	ESA[a,b] (FFT of electrical signals) Partial discharge tests High freq waveform analysis[b]	Most effective on rotor, TBD for stator Detects discharges in winding (for over 4KV motors) Developmental
Turbine drive governor	Monitor speed regulation	Apply limit to or trend speed fluctuations
Circuit breaker trip-related HW Turbine drive trip-related HW Circuit breaker spring hardware	Timed response	Command to response (e.g., latch) times
Turbine drive GV	None	(Minor degradation is apparent when online)
Pump bearing Motor bearing	Vibration/acoustic spectra analysis Thermography Lubrication analysis	Established frequency and acceleration limits Temperature limit at bearing Profile of particle count and size, contamination, viscosity, water limits, etc.
Pump shaft/coupling	ESA (FFT of electrical signals) Standard vibration analysis	Analysis can detect shaft misalignment/crack Limits of imbalance/misalignment
Pump internals	ESA (FFT of electrical signals) or hydraulic performance test	Flow instability measured using ESA or std testing/trending of flow, head, and power parameters - use established criteria
	Vibration spectra analysis Vibration/acoustic	Established frequency and acceleration limits Established vibration limits in the pump casing
Pump seal/packing	Thermal measurement Leak detection	Temperature limit Visual or use of sensors, leakage rate limit pump dependent

(a) Development required

(b) ESA = electrical signature analysis

4.3.3 Speed regulation monitoring

The mechanical flyball drive governors may exhibit minor degradation in the speed regulation of the turbine and may be monitored for speed regulation under start-up, transients, changing pump loads, and, of course, steady state operation. (Not applicable to the electrohydraulic turbine drive governor.)

4.3.4 Electrical signature analysis

ESA was developed, in part, at the Oak Ridge National Laboratory (ORNL) [5,6] and was used in a series of tests where the pump motor acts as a transducer for diagnostics. The motor in certain cases is an effective transducer of torsionally-related load phenomena such as relative precision in shaft alignment, suction conditions, and variation in pump hydraulic conditions. Rotor degradation monitoring is also possible since the amplitude of slip-pole side bands of 60 Hz and harmonics trend upward with increased rotor degradation, especially in larger motors. The technology is not fully developed and absolute determination of the extent of rotor degradation cannot presently be made. However, any technology that shows much promise for the detection of monitoring of diverse phenomena in both the pump and motor merits high emphasis.

4.3.5 Vibration - standard and spectra analysis

Standard vibration analysis is a commonly used tool for the effective monitoring of pump rotor imbalance, misalignment, and instances of severe (i.e., energetic) cavitation. However, vibration analysis is not as effective as ESA for the detection of motor rotor electromagnetic imbalance.

Vibration spectra analysis is an effective tool for the detection of pump and motor bearing defects. Accelerometers are generally placed on the bearing housings however other options can be employed such as eddy current shaft position sensors to sense shaft deflection.

4.3.6 Acoustic monitoring

Acoustic monitoring may be used on pump casings as is performed in a pump monitoring program initiated in Japan in 1993 [5]. Acoustic energy is trended and a spectral analysis is performed and these are analyzed together relative to specific operating conditions (e.g., rotating speed, flow rate, electrical power). High frequency spectral energy and high noise floor are general indicators of cavitation using this technology.

4.3.7 Thermography

IR thermography is the collection and analysis of thermal images to ascertain various types of component degradation. IR inspections are an ideal complement to a comprehensive monitoring program because the technology is noncontacting and analysis results are quickly and easily obtained. One advantage of IR monitoring of bearings is that it can quickly detect early signs of overheating by observing the temperature rises on the rotating shaft.

Post maintenance testing procedures that utilize thermographic analysis have been particularly helpful in diagnosing problems such as packing being too tight, inadequate cooling flows to packing glands, and seal clearances. Data analysis software is then used to catalog the data and develop historical trends.

4.3.8 Lubrication analysis

This analysis methodology has made numerous technological advancements in the past two decades. Nuclear plants use different types of lubricant analyses based on component requirements, and the maintenance goals of the particular organization. The common dilemma is that most plants must send their oil samples, some of which are radioactive, off-site to be analyzed. This is a very expensive and record-intensive. However, recent innovations to the predictive maintenance industry have enabled industries to not only perform their own oil analysis on-site but to collect, store, trend, and correlate the results with vibration analysis data on personal computers [7,8].

At least one utility (Arizona Public Service) has recently found [9] that in-house oil analysis is a powerful enhancement that can be coordinated with vibration monitoring programs for a very significant overall advantage in bearing monitoring. A visual microscope method is used to detect abnormal wear debris in the larger-than-5-micron range (i.e., where most abnormal wear is). This precedes any possible degradation indications by vibration analysis and it is used to determine the frequency of testing by both methods. When both methods are used together in this way, sufficiently early knowledge and confidence of impending failure allows for scheduled repair and frequently the bearing damage is mild enough to facilitate root cause investigation. This is an important example of how the management of a monitoring program (i.e., the integration of testing programs and maintenance) is as important as the choices of technologies and monitoring methods that are employed.

Because of the broad scope of techniques available, the reader is referred to a NUREG [5] that provides a reasonable summary of the more common techniques as well as additional references. The more common techniques are:

Spectrographic analysis
Particle count
Spectrometals analysis
Ferrographic analysis techniques
    direct reading ferrography (DRF)
    analytical ferrography
IR analysis
Viscosity
Total acid number
Total base number

There are additional analytical techniques which are critical to the evaluation of the lubricant condition of reactor main coolant pumps. These pumps present a special problem for a lubricant analysis program, since they operate for extended periods without an opportunity for sample analysis and are generally radiologically contaminated. These additional analyses indicate the effective level of the lubricant additives. With this information, determination of the remaining life of the lubricant can be made. Analyses critical to the evaluation of main coolant pumps include: rotating bomb oxidation test (RBOT), which accelerates oxidation of the lubricant to determine the useful life of the lubricant's anti-oxidation additives, and an anti-rust test, which determines the ability of the lubricant to inhibit rust formation.

5.0 CONCLUSIONS

Aging in the pump system can be monitored and controlled using a combination of the diagnostic and monitoring technologies and techniques combined, of course, with corrective maintenance. Some monitoring tools are simple to apply (e.g., hand-held IR sensor) while others are more difficult in the initial implementation (e.g., hard wiring to various circuit locations in

the circuit breaker). This study presented the methods and tools that can be used for monitoring and trending aging effects; what remains are decisions regarding which to use, perhaps on a plant by plant basis.

Recommendations resulting from this study are as follows:

1. A selection of suitable diagnostic and monitoring technologies and techniques, for highly ranked and failure prone component areas, should proceed as part of the IST program;

2. At the same time, consideration should be given to programmatically emphasizing practices that can significantly preclude pump system failures (i.e., root causes);

3. A diagnostic testing and monitoring demonstration facility should be created to support decisions regarding which technologies to use and development of methodologies and techniques;

4. Technology research and development should be performed for critical technologies:

   High frequency waveform analysis,
   Vibration spectra analysis,
   Electrical signature analysis

It is important for diagnostic engineers and technicians to carefully select the *combination* of tools that will be most effective in providing information on risk-important equipment. It is essential that new technologies or technologies that require additional development are given high program emphasis for they clearly will provide essential information and perspectives that cannot be gained from other available alternatives.

References

[1.] CASADA, D.A., "A Characterization of Pump and Pump Motor Degradation and Failure Experience in the Nuclear Power Industry," ORNL/NRC/LTR/95-24, Oak Ridge National Laboratory, Oak Ridge TN (Jan 1996)

[2.] COX, D.F., "Aging of Turbine Drives for Safety-Related Pumps in Nuclear Power Plants," USNRC Report NUREG/CR-5857 (ORNL-6713), Oak Ridge National Laboratory, Oak Ridge, TN, (June 1995)

[3.] STAUNTON, R.H., "A Characterization Update of Pump and Related Equipment Failure Experience in the Nuclear Power Industry (1994-1995)," ORNL/NRC/LTR/96-32, Oak Ridge National Laboratory, Oak Ridge TN (February 1997)

[4.] STAUNTON, R.H., "Improved Diagnostics and Monitoring Methods for Pumps and Related Equipment," ORNL/NRC/LTR/96-37, Oak Ridge National Laboratory, Oak Ridge TN (April 1997)

[5.] GREENE, D. A. CASADA D.A., "Detection of Pump Degradation," NUREG/CR-6089, ORNL-6765, Oak Ridge National Laboratory, Oak Ridge, TN, (August 1995)

[6.] CASADA, D.A., Oak Ridge National Laboratory, "Using the Motor to Monitor Pump Conditions," presented July 1996 in Washington, DC, published in "The Proceedings of the Fourth NRC/ASME Symposium on Valve and Pump Testing," NUREG/CP-0152, Board of Nuclear Codes and Standards of the ASME and the U. S. Nuclear Regulatory Commission, Washington, DC, (July 1996)

[7.] SPETTEL AND R. GARVEY, "On-site Oil Analysis: A New Tool for the Vibration Analyst," pp. 49-54 in Proceedings of the 17th Annual Meeting of the Vibration Institute, Willowbrook, Ill., (June 8-10, 1993)

[8.] Computational Systems, Inc., "PC-Based Integration of Spectrographic, Ferrographic and Vibrational Analysis data," P/PM Technology 4(1), 21-23 (Jan-Feb 1991)

[9.] JOHNSON, Arizona Public Service, "Part 2 - Current Program Integrating Strategies and Lubrication Technology," presented July 1996 in Washington, DC, published in "The Proceedings of the Fourth NRC/ASME Symposium on Valve and Pump Testing," NUREG/CP-0152, Board of Nuclear Codes and Standards of the ASME and the U. S. Nuclear Regulatory Commission, Washington, DC, (July 1996)

NEXT PAGE(S) left BLANK

DIESEL GENERATOR DATA ACQUISITION SYSTEM (DG-DAQ)

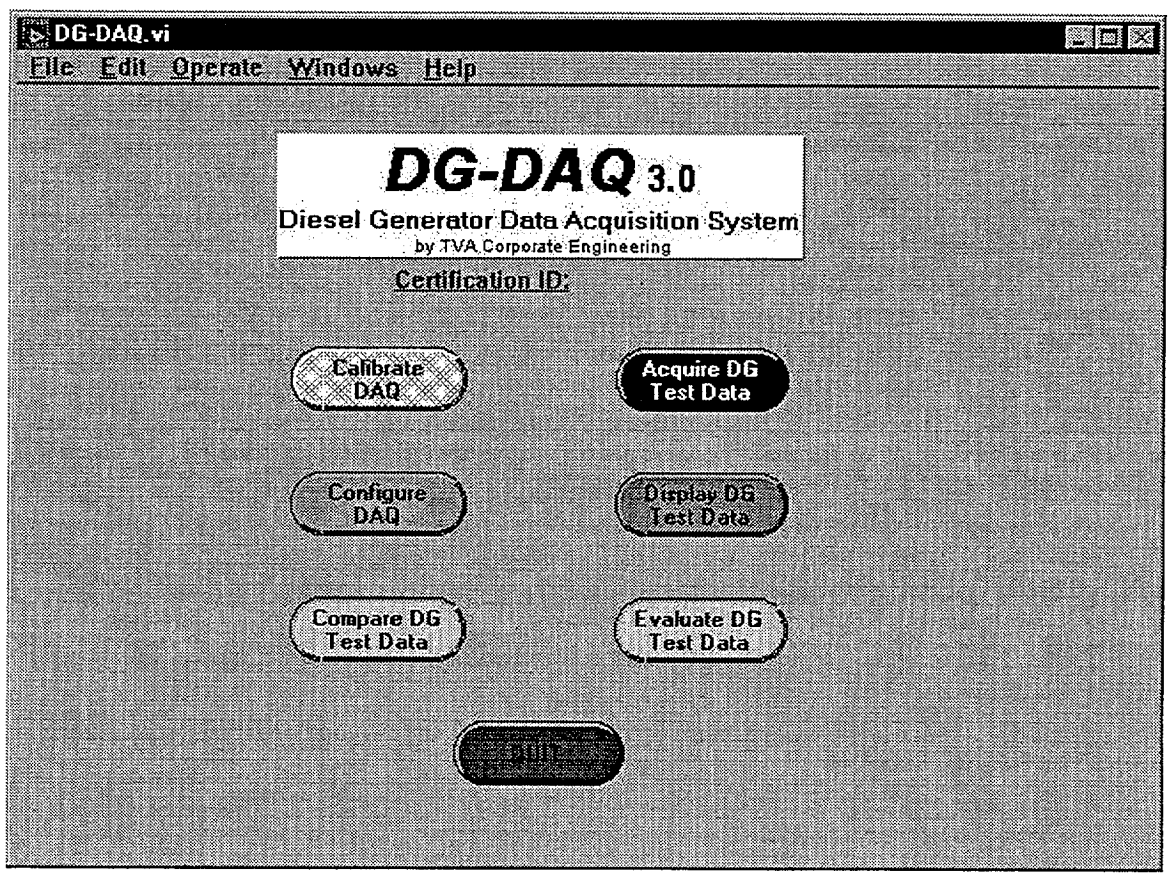
A TVA nuclear technology

XA9848570

M.D. BOWMAN
Engineering and Technical Services,
Tennessee Valley Authority (TVA) Nuclear,
Chattanooga, Tennessee, United States of America

Abstract

The Diesel Generator Data Acquisition System (DG-DAQ) is a technology developed by TVA for the purpose of performing surveillance and diagnostics on emergency diesel generator (DG) output parameters at TVA nuclear power stations. This computer based system provides a quick, reliable, and accurate means to record and evaluate DG performance and is also well suited as a diagnostic tool for trending and troubleshooting. TVA has traditionally used strip chart recorders to obtain DG output data during load sequence tests. The stripchart recorders required input signal conditioning via transducers, shunts, and decade boxes which had to be connected to internal panel wiring. This was a time consuming process and vulnerable to human (wiring) errors. It is estimated that the "stripchart" method of recording and evaluating DG test data cost each nuclear unit approximately 400 workhours per outage. The DG-DAQ system was designed to be used as portable test equipment to reduce the outage hours associated with DG testing. The DG-DAQ derives all DG output parameters from a single phase of voltage and current waveforms. Because the DG-DAQ uses "raw" voltage and current waveforms without the use of transducers, it can be easily connected to existing metering cutouts with no other connection or disconnection of plant wiring. The DG-DAQ system is used at all TVA nuclear power stations for DG surveillance testing as well as post-modification / post-maintenance tests. On the average, it has reduced the workhours associated with these tasks to less than 5 percent of their previous values.



1. OVERVIEW

The Diesel Generator Data Acquisition System (DG-DAQ) is a technology developed by TVA for the purpose of performing surveillance and diagnostics on emergency diesel generator (DG) output parameters at TVA nuclear power stations. This computer based system provides a quick, reliable, and accurate means to record and evaluate DG performance and is also well suited as a diagnostic tool for trending and troubleshooting.

Most US nuclear units are committed to some version of US NRC Regulatory Guide 1.9 [1] (formerly Safety Guide 9), which specifies minimum voltage and frequency values as well as recovery performance for transients caused by load sequencing. It also specifies maximum engine overspeed values for transients caused by load rejections. Even for plants not committed to specific numerical limits, there is usually a requirement that DG voltage and frequency performance be adequate to start and accelerate all loads within required time periods.

TVA is committed to ensuring that the DGs continue to meet their technical specification surveillance requirements and other licensing commitments associated with DG voltage and frequency performance. Since the mid 1980s, TVA nuclear power stations have used traditional strip chart recorders to record DG output data during load sequence testing, which consisted of generator voltage and current (rms), frequency, and power. The stripchart recorders required input signal conditioning via transducers, shunts, and decade boxes which had to be connected to internal panel wiring. This was a time consuming process and vulnerable to human (wiring) errors. After recording the test data, the stripcharts had to be evaluated by manually scaling the data throughout the load sequence. Even a simple evaluation, such as determining discrete minimum and maximum voltages during load sequencing, was a fairly time consuming operation, and the results were also vulnerable to human (scaling/measurement) errors. Determining continuous performance data (e.g. voltage and frequency recovery profile) required much more time to manually transcribe the data with adequate resolution. Some nuclear stations (such as Sequoyah) could not tolerate the inherent inaccuracies associated with signal conditioning transducers, such as bias errors and integration time constants. Because of this, "raw" voltage waveforms were recorded on high-speed, low-inertia stripchart recorders and then manually converted to rms voltage and frequency data by scaling the waveforms and calculating the desired values. Obviously, this was an even more time consuming process and was vulnerable to additional errors caused by non-sinusoidal waveforms during transient conditions. It is estimated that the "stripchart" method of recording and evaluating DG test data cost each TVA nuclear unit approximately 400 workhours per outage. Thus, there was a significant potential for savings.

2. DEVELOPMENT

TVA initially identified and purchased appropriate hardware and software for development of a prototype system. The concept was to develop a portable system to be used as maintenance and test equipment (M&TE). The system was developed using readily available data acquisition hardware and a graphical programming language designed by the hardware manufacturer. The prototype system was developed, assembled, tested, and demonstrated during pre-operational testing of the DGs at TVA's Watts Bar Unit 1. The prototype tests were successful and proved the feasibility of the DG-DAQ concept. Large amounts of data from several DG load sequence tests were recorded and evaluated in short amounts of time. The results compared favorably with data recorded by traditional "stripchart" methods, and comparison of the data demonstrated the potential superior accuracy of the DG-DAQ system.

The prototype was then further developed into a fully functional system that could be used as certified M&TE. This involved:

- development of an intuitive user interface for use by a variety of plant personnel (engineers, technicians, maintenance)
- development of unique software algorithms to accurately calculate power system parameters (true rms, frequency, power components) from a single phase of voltage and current waveforms with one cycle resolution

- semi-automation of data evaluation (automatic display of minimum/maximum values, and voltage/frequency performance during transients)
- optimization of system performance (memory configuration, hardware configuration, etc.) to allow use of computer hardware that is less than "state-of-the-art"

3. SYSTEM DESCRIPTION

The DG-DAQ system consists of a portable computer with an on-board data acquisition card, a high-isolation amplifier, and an attenuating terminal block. The data acquisition hardware is available from National Instruments Corporation. The software was developed using LabVIEW®, which is a graphical programming language available from National Instruments Corporation. The DG-DAQ system components are given in Table I.

TABLE I. DG-DAQ SYSTEM COMPONENTS

Computer and Operating System:	Portable PC, 80486 or greater, 32 MB RAM or greater, EISA expansion slots Windows 3.1 (386 enhanced mode) or Windows95
Data Acquisition Hardware:	National Instruments AT-MIO-16X, Multi-function I/O DAQ Card National Instruments SCXI-1000, Signal Conditioning Chassis National Instruments SCXI-1120, 8-Channel Isolation Amplifier National Instruments SCXI-1327, Attenuator Terminal Block
Software:	DG-DAQ (LabVIEW® application developed by TVA) NI-DAQ® (National Instruments' hardware drivers)

The DG-DAQ system layout is shown in Figure 1.

The attenuating terminal block can accept eight inputs up to 280 Vrms and can therefore be connected directly to existing potential transformer (PT) and current transformer (CT) secondaries. The terminal block signals are passed to an eight channel isolation amplifier, which provides differential inputs with high isolation and also sets the signal level to an appropriate range for the data acquisition card. The multi-channel data acquisition card performs A/D conversion on each signal with 16-bit resolution and sends the digital data into the computer where it is stored directly to the hard drive.

The DG-DAQ system derives all DG output parameters (Vrms, Irms, kW, kVAR, kVA, and Hz) from a single phase of voltage (Vab) and current (Ia) waveforms (shown in Figure 3). This is based on a unique algorithm which has been developed and tested by TVA. Because the DG-DAQ uses "raw" voltage and current waveforms without the use of transducers, it can be easily connected to existing metering cutouts ("PK" blocks) with no other connection or disconnection of plant wiring. If desired, additional inputs can be used to record other parameters, such as voltage regulator I/O, governor I/O, fuel rack position, field voltage, etc. This allows the DG-DAQ to be used as a diagnostic tool for trending or troubleshooting DG performance.

During data acquisition, each input is acquired, digitized, and stored directly to the hard disk using a high sampling rate that exceeds 40 times over-sampling. Recording time is limited only by the size of the computer hard drive, with one minute of data using about 200 kBytes of disk space per input. As the data is being recorded, the DG voltage and current waveforms are displayed in real-time on a virtual oscilloscope and a quick calculation of the power system parameters is displayed in real-time on virtual meters (Figure 2). This provides the operator with a visual confirmation that proper data is being recorded.

The Display panel allows the "raw" waveforms recorded by the DG-DAQ system to be read and displayed on virtual stripcharts at any level If magnification (Figure 3).

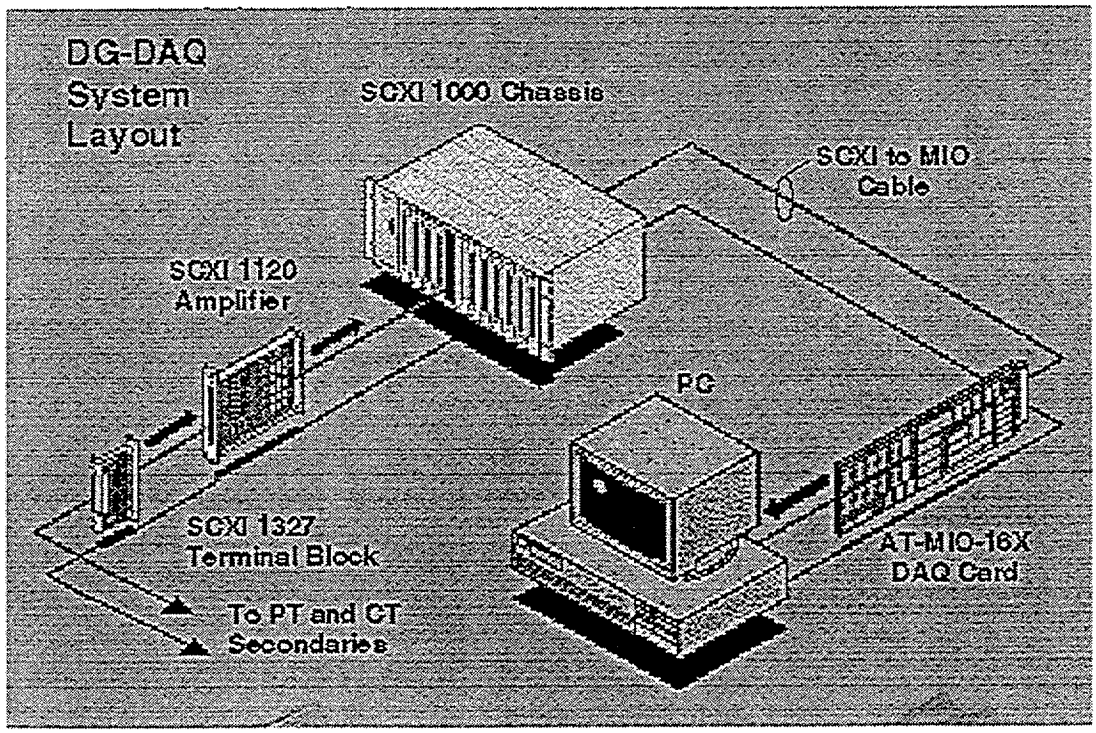


FIG. 1. DG-DAQ System Layout

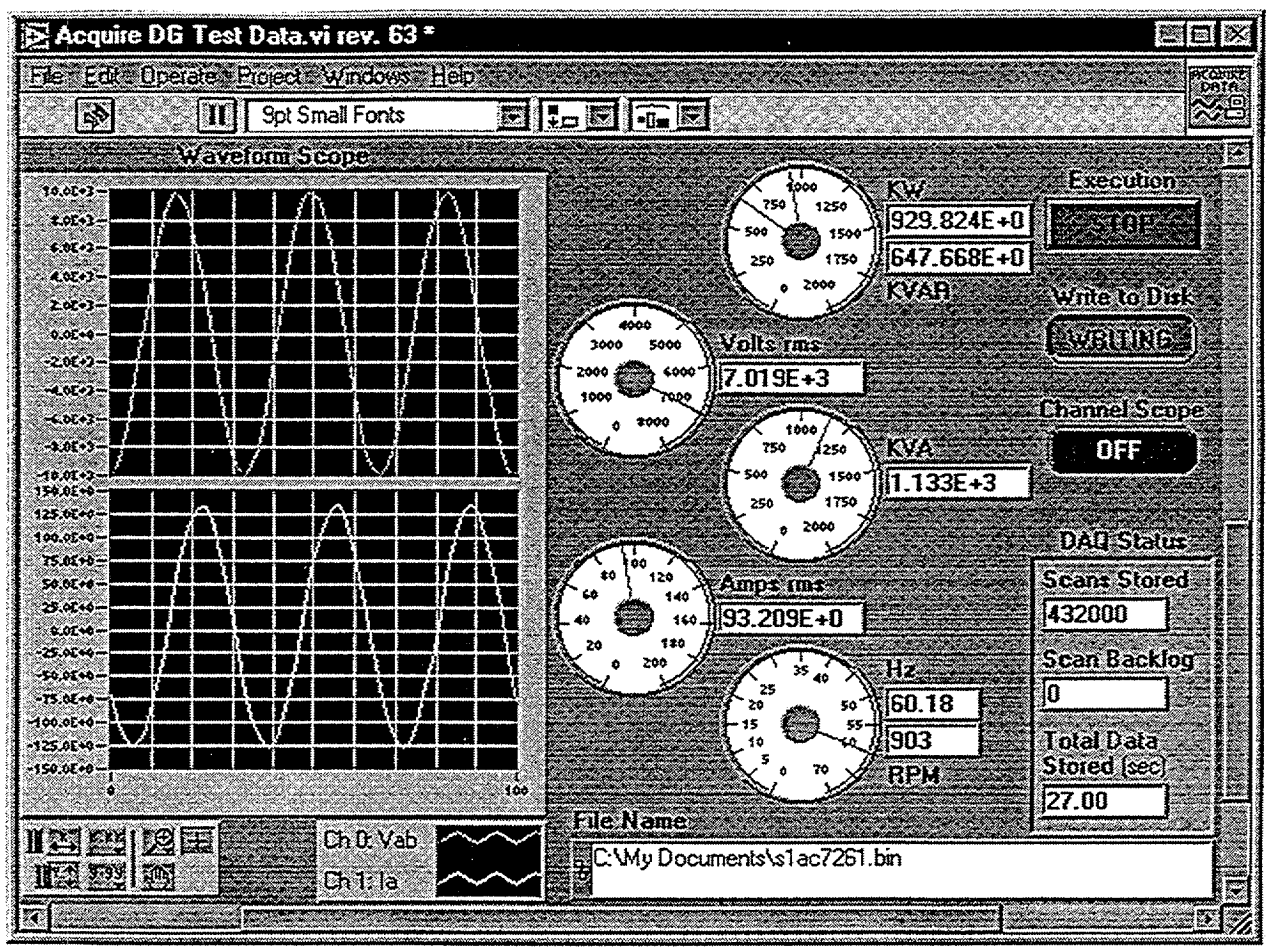


FIG.2. Example of ACQUIRE Panel

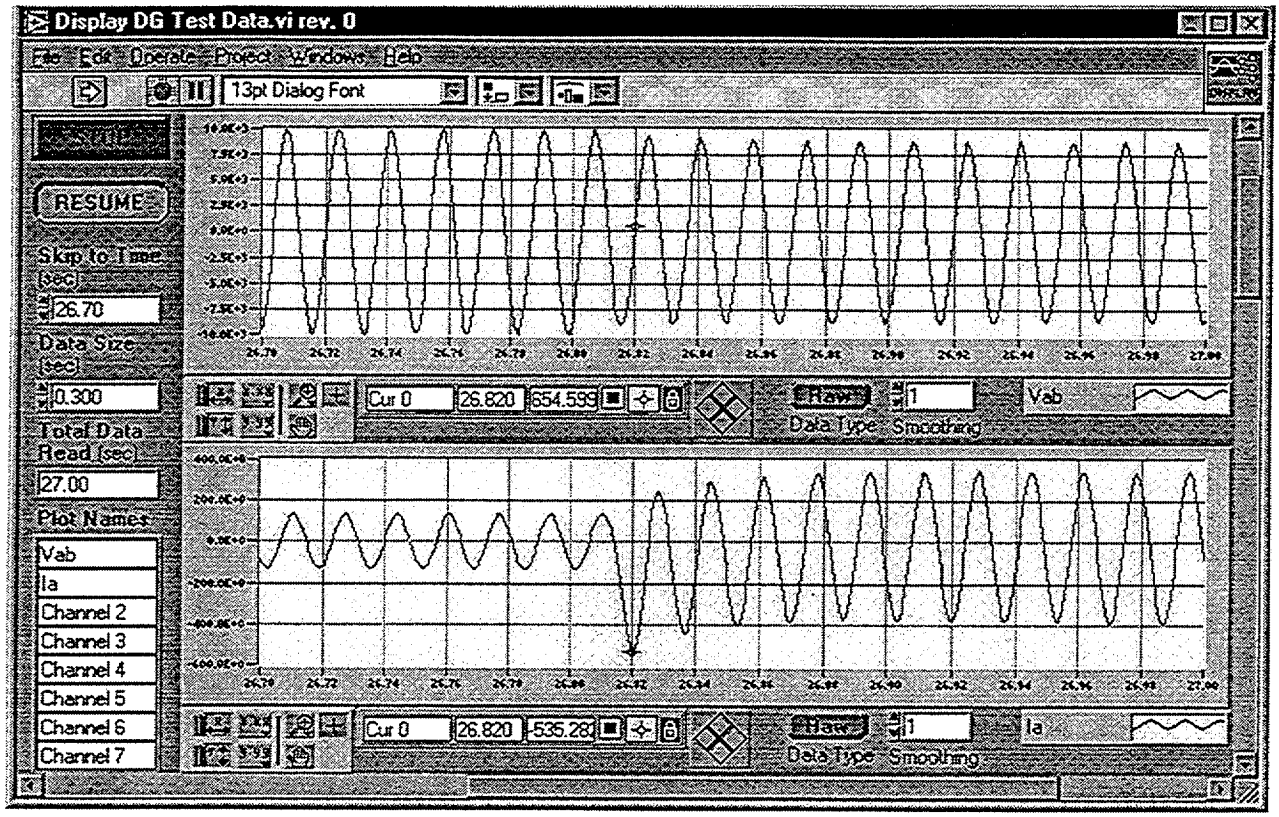


FIG. 3. Example of DISPLAY Panel with Voltage (Vab) and Current (Ia) Waveforms

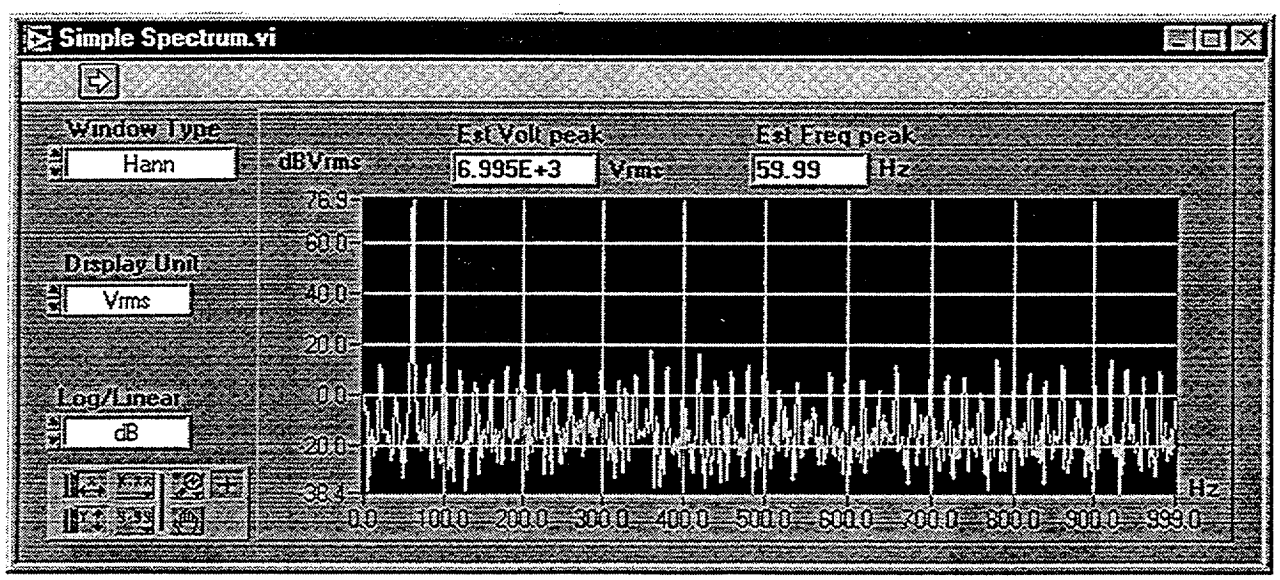


FIG. 4. Example of DG-DAQ Spectrum Analyzer

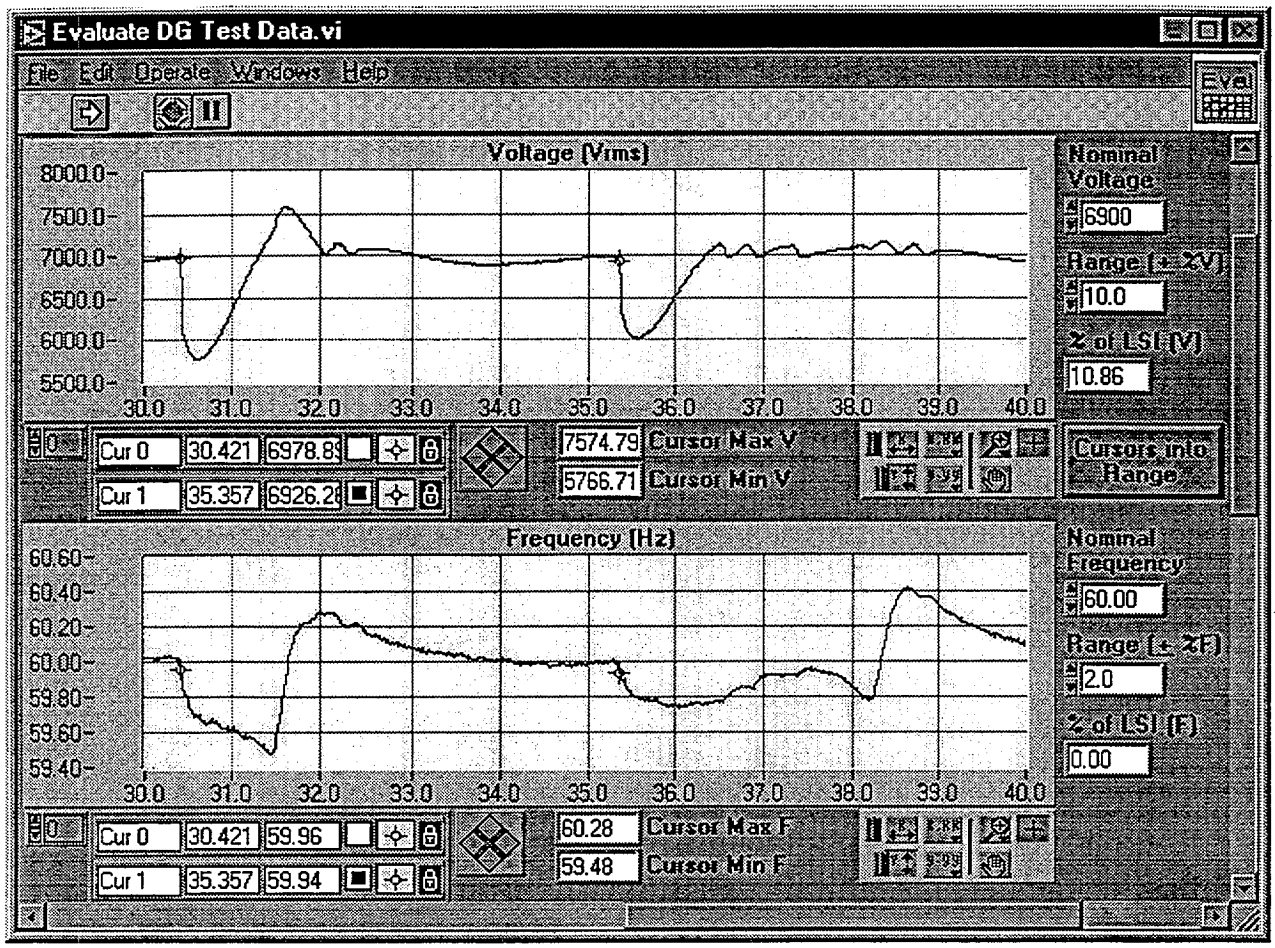


FIG. 5. Example of EVALUATE Panel with Derived Vrms and Hz Parameters

In addition, a spectral analysis of any input can be performed at any point using the built-in virtual spectrum analyzer (Figure 4).

The real strength of the DG-DAQ system is the ability to convert the voltage and current waveforms into more useful power system parameters for evaluation. The Evaluate panel reads the recorded voltage and current waveforms from disk and converts them into true-rms quantities. The waveform zero-crossings are used to derive the system frequency information, and the product of the voltage and current waveforms is used along with their phase relationship to determine all of the power quantities (kW, kVAR, and kVA). These derived parameters are displayed on virtual stripcharts for further evaluation (Figures 5 and 6).

The Evaluate panel also provides semi-automatic analysis of the data. The user simply locates the area of interest with data cursors, and the system instantly displays minimum/maximum values for voltage, frequency, current, kW, kVAR, and kVA. If the data cursors are placed at adjacent motor starts from a load sequence, the system also displays the Regulatory Guide 1.9 recovery performance. In addition, the user may "zoom-in" on any area of interest or determine cycle-by-cycle values of any parameter. Multiple data files can be displayed simultaneously, which is perfect for trending performance data between different DG units and/or different outages.

4. CERTIFICATION

The DG-DAQ system was certified in-house by TVA Central Laboratories for use as M&TE at all TVA nuclear power stations. The DG-DAQ was certified as a complete system consisting of the computer, all

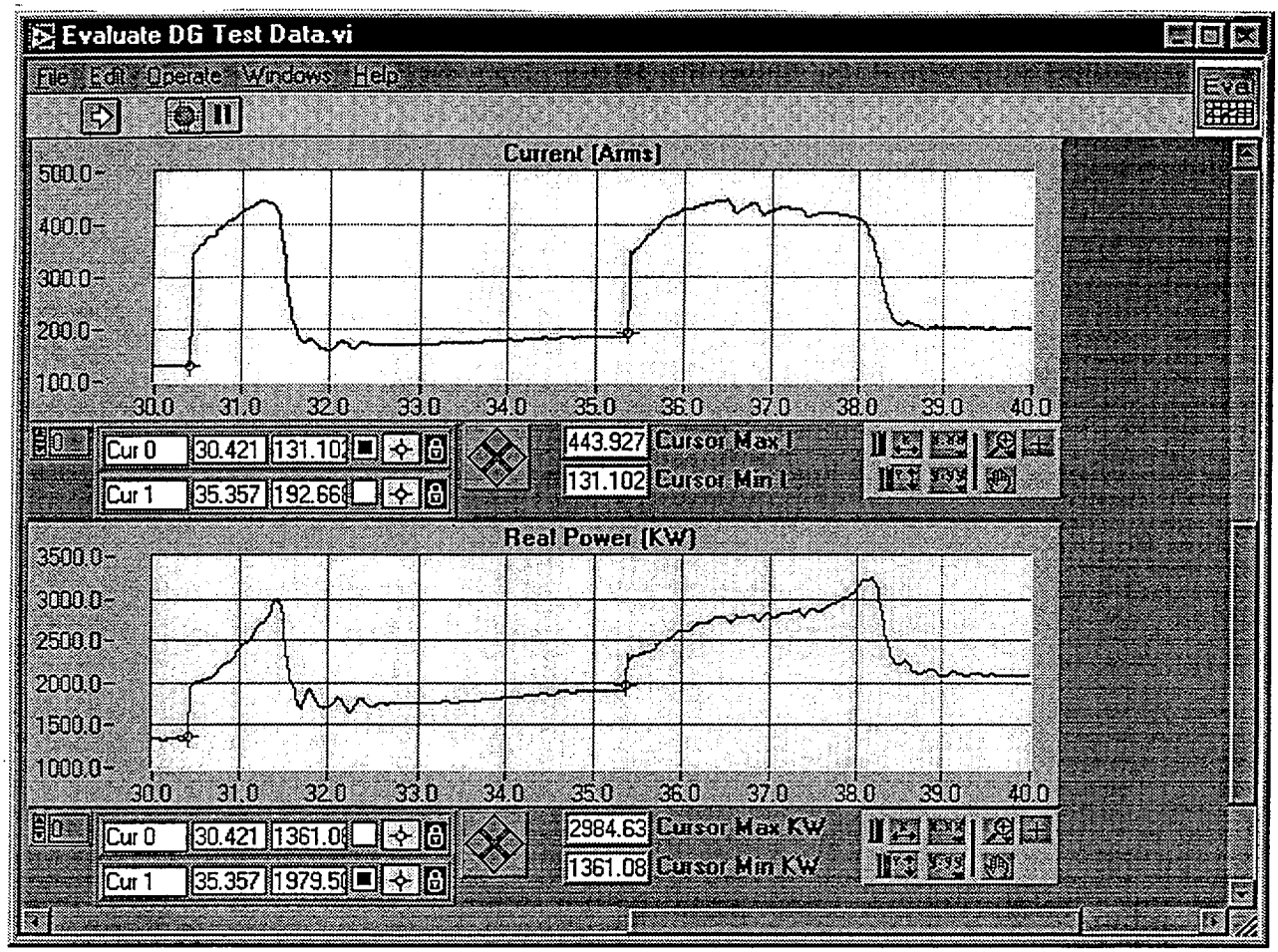


FIG. 6. Example of EVALUATE Panel with Derived Irms and kW Parameters

DAQ hardware, and integral software. The certification was accomplished in a two step process. First, Engineering issued a Certification Requirements Document which established the critical attributes of the system that could affect performance, reliability, and accuracy, as well as the required/achievable accuracy based on system hardware and software. Then, TVA Central Labs prepared detailed certification instructions, including calibration procedures, based on the Certification Requirements Document. Each DG-DAQ system is subjected to the calibration and certification procedure prior to use, and is periodically re-certified for proper operation and accuracy.

The DG-DAQ system is certified to measure the DG output voltage (rms) within 0.15%, current (rms) within 0.25%, and frequency (Hz) within 0.045%. The maximum data resolution is 1 cycle, which is the theoretical limit for rms and frequency computations.

5. PERFORMANCE

The DG-DAQ system has been used as the official test record during many DG tests at TVA nuclear power stations. These consist of surveillance tests to satisfy plant technical specification requirements as well as post-modification / post-maintenance tests. A brief description of some of these tests and use of the DG-DAQ system is given in Table II. Overall, the system has performed well and has reduced the workhours associated with these tasks to less than 5 percent of their previous values.

TABLE II. DG-DAQ PERFORMANCE IN ACTUAL TESTS

Site / Test	Test Description	DG-DAQ Use, Performance, and Benefits
Browns Ferry Unit 3 Restart Load Acceptance Testing (12 tests performed on 4 DGs)	Re-verification of DG performance. Load sequencing of all emergency loads in full-flow and mini-flow conditions. Largest-load rejection.	Used to record and evaluate DG voltage and frequency performance. Stripcharts used in parallel. Evaluation completed in 8 hrs vs. estimated 2 weeks for stripchart evaluation. Prevented potential impact to fuel-load schedule. Also used to record and evaluate internal exciter/voltage regulator parameters during trouble-shooting efforts for failure of one DG.
Browns Ferry Unit 2&3 Outage Load Acceptance Testing (12 tests performed on 4 DGs per outage)	Outage surveillance testing. Load sequencing of all emergency loads in full-flow and mini-flow conditions. Largest-load rejection.	Used to record and evaluate DG voltage and frequency performance. Also simultaneously recorded internal governor and exciter parameters for use in troubleshooting in case of failure. DG-DAQ has now replaced stripchart recorders for outage surveillance testing. This saves about 300 workhours per outage.
Sequoyah U1 & U2 Post-Modification Testing for Upgrade of the Electric Governor (12 tests performed on 4 DGs)	Post-mod testing following upgrade of electric governor. Manual load sequencing in emergency mode. Fast start time.	Used to record and evaluate DG frequency performance during manual load sequencing. Also used to evaluate exact fast-start time. Stripcharts used in parallel. Data evaluation completed in about 1 hr versus estimated 16 hrs for stripchart evaluation. This saved "LCO" time and prevented potential impact to the outage schedule. Also used to simultaneously record and evaluate internal governor parameters during tuning efforts.
Sequoyah U1 & U2 Load Sequence and Load Rejection Testing (8 tests performed on 2 DGs per outage)	Outage surveillance testing. Load sequence of required emergency loads. Full-load rejection and largest load rejection.	Used to record and evaluate DG voltage and frequency performance. Data evaluation completed in about 1 hr vs. 72 workhours for stripchart evaluation. Also simultaneously recorded internal governor and exciter parameters for use in troubleshooting in case of failure. The DG-DAQ has now replaced stripchart recorders for outage surveillance testing. This saves about 400 workhours per outage.
Watts Bar U1 Load Sequence and Load Rejection Testing (16 tests performed on 4 DGs per outage)	Outage surveillance testing. Load sequence of required emergency loads. Full-load rejection and largest load rejection.	Used to record and evaluate DG voltage and frequency performance for all outage surveillance testing. This saves about 500 workhours per outage versus stripchart recorders.
Watts Bar U1 Fast Start Testing (performed on all 4 DGs every 6 months)	Semi-annual surveillance testing. Fast-start time.	Used to record and evaluate DG voltage and frequency increase during fast-start. Determines the exact time to required speed and voltage independently. This allows independent trending of voltage and speed build-up.

6. SIMILAR DEVELOPMENTS

The type of hardware and software associated with the DG-DAQ system is also well suited for other surveillance testing. In fact, TVA Nuclear has recently developed a similar system to record and analyze test data from the Reactor Coolant System (RCS) cold and hot leg narrow range RTDs at the Sequoyah and Watts Bar nuclear power stations. Known as "RTD-XCAL", this portable data acquisition system is used to satisfy plant technical specification and testing requirements associated with RTD

cross-calibration, which is performed during heat-up following each refueling outage. The system is connected to the existing Reactor Protection System in order to obtain the RTD voltages needed to calculate RCS temperature. The system can perform a complete analysis of all 20 narrow range RTDs within 0.5 seconds. This allows the plant to perform RCS RTD cross-calibration as the plant heats-up and eliminates the time required to achieve isothermal conditions for manual voltage measurement. This will save about six hours of critical path startup time per outage.

REFERENCE

[1] US Nuclear Regulatory Commission Regulatory Guide 1.9, "Selection, Design, Qualification, and Testing of Emergency Diesel Generator Units Used as Class 1E Onsite Electric Power Systems at Nuclear Power Plants", Revision 3, (July 1993).

NEXT PAGE(S) left BLANK

UPGRADING ELASTOMER SEALS FOR NUCLEAR SERVICE

K.C. WITTICH, R. WENSEL, R. LAROSE, S. KURAN
Fluid Sealing and Dynamics Branch,
Chalk River Laboratories,
Atomic Energy of Canada Limited,
Chalk River, Ontario, Canada

XA9848571

Abstract

Pumps, valves and instruments in nuclear plants have historically contained whatever elastomer each equipment supplier traditionally used for corresponding non-nuclear service. The proliferation of elastomer compounds, and their sometimes uncertain reliability, is now being reduced by upgrading and standardizing on a handful of compounds that have each been verified to be high performers for their class of service conditions. The objective is to make cost-effective improvements in the reliability and integrity of equipment in Canadian-designed nuclear plants. The effort focuses on elastomer seals and includes: understanding sealing fundamentals, developing relevant data for superior compounds for each service, and improving quality assurance methods, including handling and inspection guidelines. In practice, discussions with plant personnel and review of plant records are the first step. Two severe-service examples are given where these needs have been met by the following progression of activities: inspecting and laboratory testing of seals removed from service, preliminary and qualification testing of improvements, introduction into service, and monitoring the upgraded seals during phase-in periods. Large gains in reliability and integrity have been demonstrated for simulated normal and accident service conditions of heat, radiation and other deteriorative influences. Significant savings in maintenance costs are also projected.

1. INTRODUCTION

In a nuclear plant, elastomer seals must function in many environments that do not exist or are uncommon in other industries. The best known of these is ionizing radiation, but nuclear seals often face high temperature water or high levels of ozone also. Performance requirements are unusually high because of the cost of breakdowns and maintenance in radiation fields, plus the need to keep the reactor safe at all times.

In equipment for nuclear plants, manufacturers usually supply elastomers (i.e., rubber-like materials) that are essentially identical to those they supply to other industries. Sales to nuclear plants are rarely large enough to warrant development of improved compounds, and data relevant to severe nuclear service rarely exist for commercially popular compounds. This sometimes results in equipment with seals of inferior or inappropriate elastomer compounds, or compounds of uncertain durability in service. It has also led to a proliferation of compounds being used, since each manufacturer has different favorites. Upgrading and standardizing on a handful of superior materials can greatly improve integrity, service life, and overall cost.

The need for equipment upgrading has been met in the Canadian nuclear industry by developing in-house expertise by the developer-architect-engineer for Canadian-designed pressurized heavy water reactors (PHWR). Improvements to elastomer seals have been ongoing since needs first surfaced in the sixties. Since then, the effort has developed into an integrated program with the objectives of upgrading elastomer performance, safety margin and service-life predictability in all operating and future PHWR plants. All aspects of elastomer seal optimization are being addressed.

2. OVERVIEW OF INTEGRATED APPROACH

The effort to upgrade elastomer seals falls into two categories: generic and service-specific. A key element in the generic work is identification of the fundamental properties that govern the mechanics of sealing. Also included is more applied work on:

- identifying and retrofitting improved elastomer compounds,
- developing and implementing new elastomer compound specifications and quality assurance procedures, and
- developing guidelines for installation, handling, and inspection of elastomeric components.

Service-specific effort often begins with identification of the need for an improved elastomer seal. This usually comes from discussions with plant personnel and review of maintenance and inspection reports and records of usage. The second stage of this effort encompasses:

- inspection and laboratory testing of seals removed from service,
- preliminary testing of possible improvements,
- qualification testing to demonstrate suitability of a selected improvement for service,
- introduction into service, and
- monitoring the "improved" seals during phase-in periods.

Sometimes, service-specific effort focuses on service-life prediction and environmental qualification. This uses "accelerated-aging" and simulated normal and accident service tests of elastomer seals and equipment under specific conditions of heat, radiation and other deteriorative influences.

3. ELASTOMER SEAL FUNDAMENTALS

An understanding of the mechanics of sealing with elastomers is required to upgrade them for severe-service, high-reliability applications in nuclear plants. Elastomers are extensively used for sealing at moderate temperatures because of their fundamental elasticity, resilience, conformability, toughness, etc. However, there is much more to sealing than simply squeezing an O-ring in accordance with handbook guidelines, as was dramatically pointed out to the world when the space shuttle, Challenger, exploded in January 1986 [1]. This does not always appear to be recognized by equipment manufacturers.

Taking an O-ring as an example, sealing is achieved when the leakage paths are small enough to prevent significant leakage. There must therefore be enough force to cause the relatively soft O-ring material to conform to the topography of the counterface (i.e., to in-fill the machining marks, scratches and other roughness). Initially, this depends on the amount by which the O-ring is squeezed from its original shape, which becomes flattened across the sealing "footprint", creating contact force [2]. This contact force decreases slowly over time, both through viscoelastic stress relaxation, which is reversible, and through compression set, which is permanent deterioration or "aging". Heat, ionizing radiation, ozone and other effects can accelerate the aging process.

When pressurized, an O-ring first deforms to seal potential leakage paths, then simply transmits any further pressure without further significant deformation, since the hydrostatic component of stress on an O-ring creates no deformation (elastomers are essentially incompressible). The deformed shapes of O-rings of typical hardness do not change significantly as pressure increases beyond 0.7 to 1.4 MPa (100 to 200 psi). In higher pressure applications, therefore, O-rings act almost as fluid-filled bags. The contact force and hence the sealing ability is generally "pressure-assisted" by the sealed fluid. This is different from conventional gaskets, which rely on large clamping forces and require heavy flanges.

4. ELASTOMER COMPOUND DATABASE

A database of relevant properties and behavior is key to elastomer selection and life prediction for severe service, such as in nuclear plants. This data must be compound-specific because within a given elastomer class (e.g., nitrile), the base polymer is compounded with varying amounts of fillers,

vulcanizing agents, anti-oxidants, anti-ozonants, processing aids, plasticizers and accelerators from any number of suppliers. These variables, and the method and degree of mixing and curing, all profoundly affect functional properties of the end product—the elastomer seal. This is illustrated by the fact that two commonly used ethylene-propylenes, developed specifically for pressurized hot water, differ by a factor of over ten in their time-to-failure in this service.[1]

Properties alone are not enough for the database to be usable for severe service. It must also include *service* -specific behavior. Most rubber manufacturers' data can be misleading, because: (1) the effects of the fluid are neglected (e.g., air versus water versus other fluids), and (2) the measured damage parameters, that life predictions are based on, often have little bearing on how a seal actually fails in service. (Parameters are more often chosen for testing convenience and standardization.) For instance, maximum tensile elongation before failure, which is often quoted as the damage parameter for O-ring life prediction, does not play a significant role in the mechanics of forming a seal, nor does it correlate well with properties that do.

Besides choosing the most appropriate damage parameter(s), the level of damage considered to constitute a failure must also be chosen judiciously. Compression set may be correctly identified as the most likely failure mode for a particular application, but its magnitude for failure may be poorly estimated. For example, a compression set failure criterion appropriate for a piston seal will severely underestimate life for a bolted flanged joint. A high compression set criterion is appropriate for a flange seal since the O-ring is in a static, highly squeezed face seal arrangement, with no extrusion gap and no changes of squeeze. In contrast, a low compression set criterion is appropriate for a piston seal which is dynamic, lightly squeezed, and has parts with tolerance stack-ups that create significant eccentricity between the piston and bore.

Naturally, the amount of testing must always be balanced by the value of the results. Consider that accelerated thermal aging requires data at four temperatures for reasonable extrapolation, and at each temperature the duration of the test must be iterated to obtain the desired level of damage (see Figure 1). Consequently, developing a compound-specific database can become very expensive. This is another reason to rationalize the number of compounds used in the field to the fewest that adequately cover the required range of applications.

5. ELASTOMER QUALITY ASSURANCE

5.1. Material Performance

To ensure that validity of the test data, the ingredients and processing variables for each chosen compound must be closely controlled for consistency, both in original qualification testing and in subsequent service. Manufacturing control can be verified by functional testing at appropriate intervals—more frequently for critical seals.

The most critical elastomer seals in main coolant pump seal assemblies supplied by the authors' company, for example, are produced in molds that have a cavity for simultaneous production of a test O-ring. By functionally testing this O-ring for set and extrusion resistance and comparing results with expectations, both the molding process and the quality of that batch of unvulcanized elastomer can be verified. Where possible, each critical seal is also individually serialized to ensure traceability. Receiving inspectors at a plant can then be supplied with full documentation to confirm the serviceability of that seal.

To ensure that the correct specific compound is received, purchasing specifications must not open the door to other compounds in the same class of elastomer. Otherwise, performance in service may be unacceptable (i.e., low safety margins, unreliability and frequent replacement). If alternative compounds are needed as back-up, each must be separately qualified. Purchase specifications, as a minimum, must require that each elastomer seal be traceable to the particular "batch" of ingredients,

[1] These results were found by tests of O-rings sealing 6.9 MPa, 232°C (1000 psi, 450°F) water. One compound failed after five weeks; the other had not failed after 52 weeks.

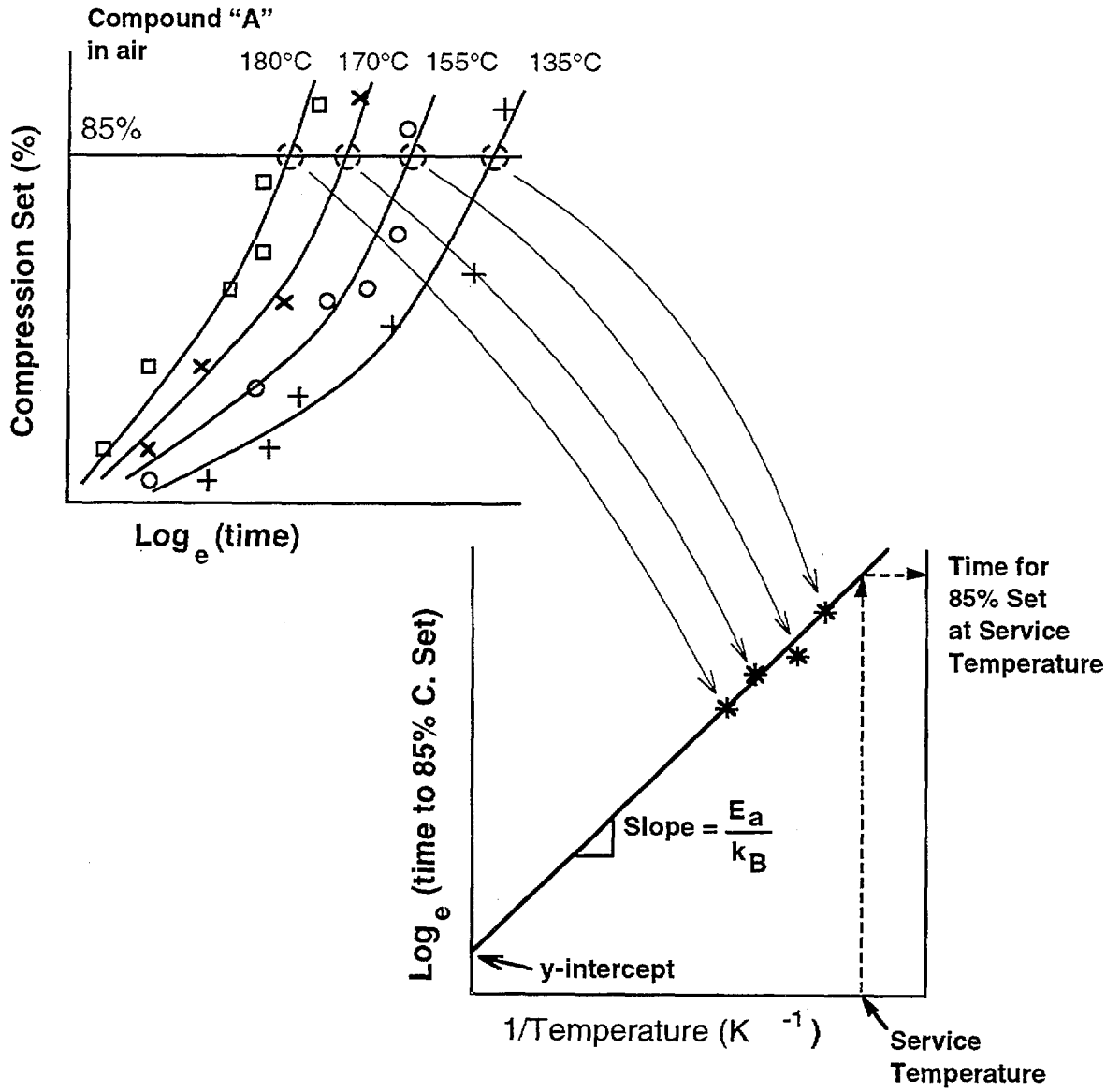


FIG. 1. Arrhenius thermal aging tests. This figure illustrates the number of data points required for a reasonable extrapolation.

mixed and processed together to form the unvulcanized stock from which the seal was made. A certificate of conformance must be supplied specifying the compound, its batch number, date of cure and seal size, along with the hardness, specific gravity and tensile strength of samples from that batch, as compared with the manufacturer's expected values.

5.2. Defects

Inspection methods and rejection criteria for defects are often neglected in quality assurance programs for seals. This can impact heavily on seal integrity and reliability. Possible defects include ones in the seal gland as well as in the elastomer seal, since machining marks and other irregularities in the gland surfaces can disrupt sealing just as much as scratches, pits, abrasions, and cuts in the seal itself.

Although defect rejection criteria for critical seals and seal glands are best established by service-specific functional testing, some general guidelines apply. Defects like scratches, machining marks ("chatter marks" in a lathe-turned part), or cuts that extend across the "footprint" of the seal are a prime concern. Whether these are acceptable depends largely on their steepness (i.e., their

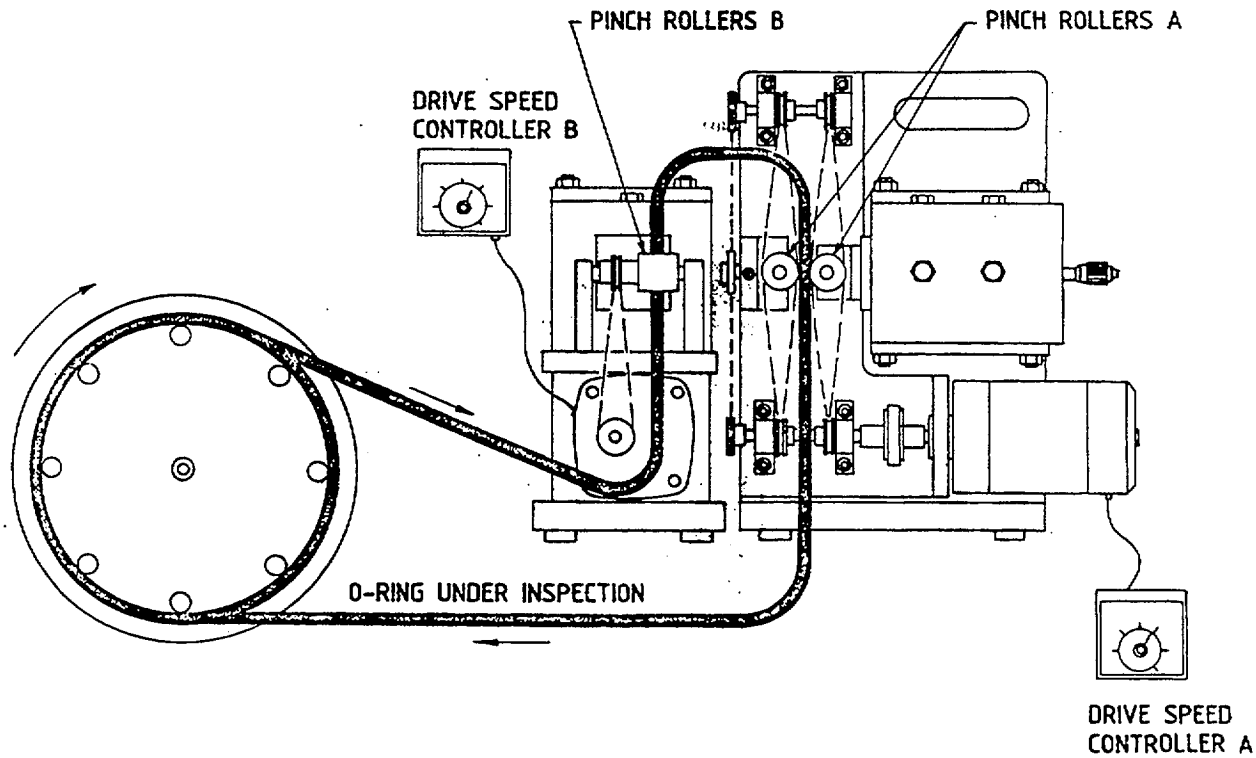


FIG. 2. Elastodynamic tester for detection of internal defects in O-rings.

depth-to-width ratio). This applies equally to defects in the surfaces of the seal gland. The deeper and narrower the scratch or groove, the more difficult for the elastomer to deform into it. Limits can be assigned based on test data and analysis [2].

Surface defects can be inspected by unaided eye. This requires stretching each region, since many defects, such as cuts and tears, are difficult to see in unstretched parts. Size can be compared to reference standards that correspond to acceptance limits, and (if necessary) measured using optical and mechanical aids (e.g., calibrated magnifier, depth-measuring microscope, stylus profilometer).

For detection of internal defects, such as inclusions, voids and regions of inhomogeneity in elastomer seals, a non-destructive tool called an Elastodynamic Tester has been found most useful. It measures reaction force resulting from localized dynamic squeeze. Figure 2 shows an automated system for elastodynamic testing of O-rings. The reaction force on two pinch rollers is measured while the O-ring is driven and squeezed between them. Localized internal defects are signalled by spikes in reaction force. Any generally high or low force, or variation around the O-ring, signifies abnormal properties when compared with a known baseline.

6. ELASTOMER SEAL STORAGE AND INSTALLATION

Elastomers are subject to deterioration with time, temperature, and other environmental influences. Ideal storage conditions are cool, dark, and free from contaminants (such as ozone, solvent vapor, etc.). Elastomer seals should be stored in a relaxed state, free from strain (i.e., not folded, twisted, or hanging on a rack). Their shelf life (expressed as expiry date) should be stated and be rationally based (e.g., if 90% of "as-new" lifetime for the particular service is deemed acceptable, and proper storage at the maximum allowable temperature is known to cause 1% loss per year, then shelf life is 10 years). Measurement of critical sealing properties (e.g., compression set, extrusion resistance, hardness) of O-rings of certain ethylene-propylene and nitrile compounds stored under proper conditions has shown them to be essentially unchanged after more than twenty years (for example, see Figure 3). Not all elastomer compounds are this stable, particularly not all nitrile compounds.

Rolling or twisting of an O-ring in its groove with bore-type assemblies can be avoided by ensuring smooth surfaces and correct lubrication. Only a thin film of lubricant is needed, and once applied, care is necessary to avoid introducing contaminants, particularly hairs and fibres, which readily create leak paths. However, excessive or inappropriate lubricant can cause failures (e.g., by causing swell or by restricting small flow passages or contaminating the rotary face seals in main coolant pumps).

7. CASE STUDIES

The following two cases of elastomer seal upgrades illustrate the potential for direct and immediate benefits to nuclear plant owners.

Early failures and frequent replacements of inflatable air-lock door seals in PHWR plants have consumed an inordinate amount of maintenance effort and money. A program to improve these is nearing completion. Bench-scale tests confirmed that in most plants the rate of seal retraction on

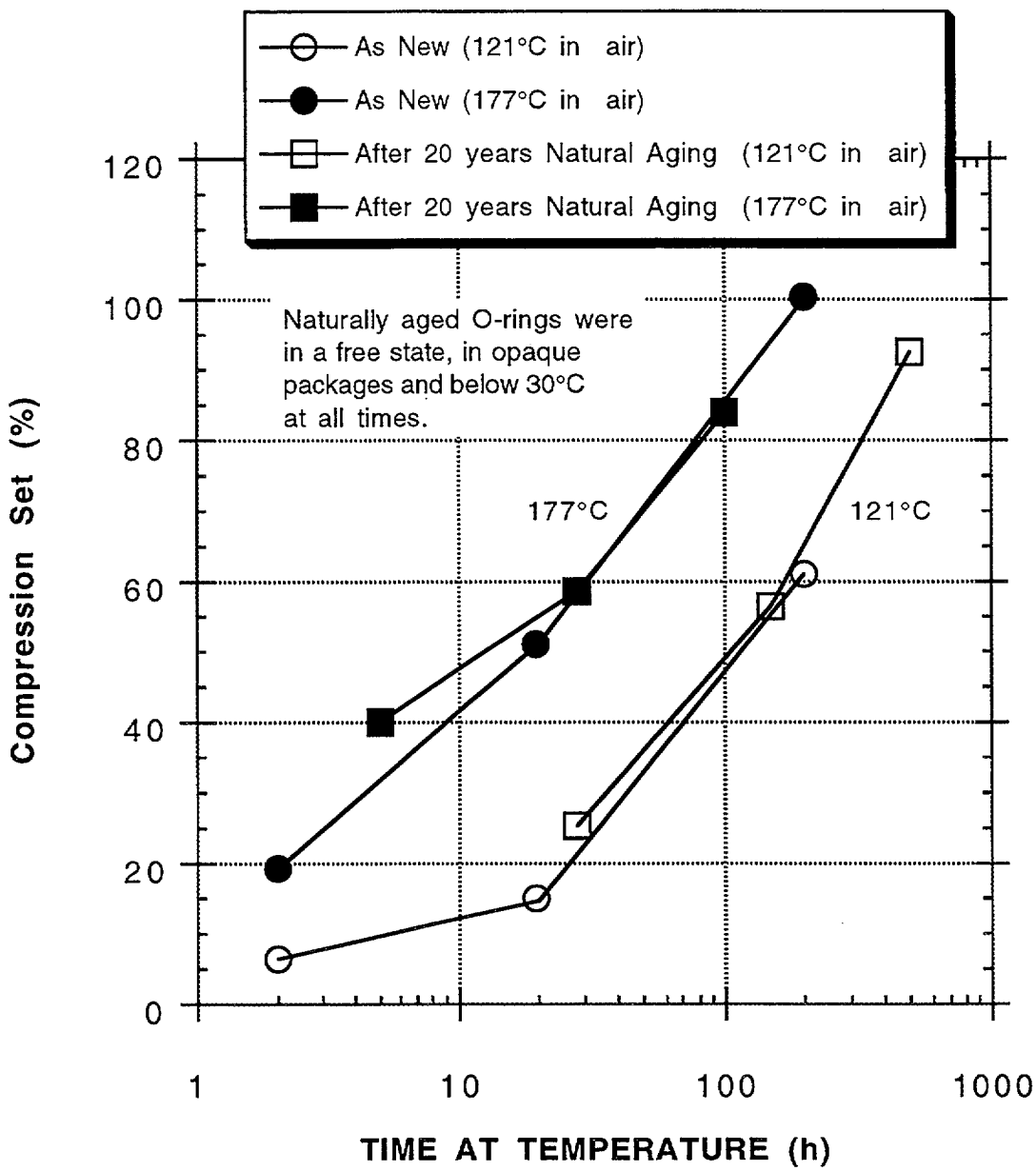


FIG. 3. Effect of twenty years of natural shelf aging on a specific nitrile O-ring compound.

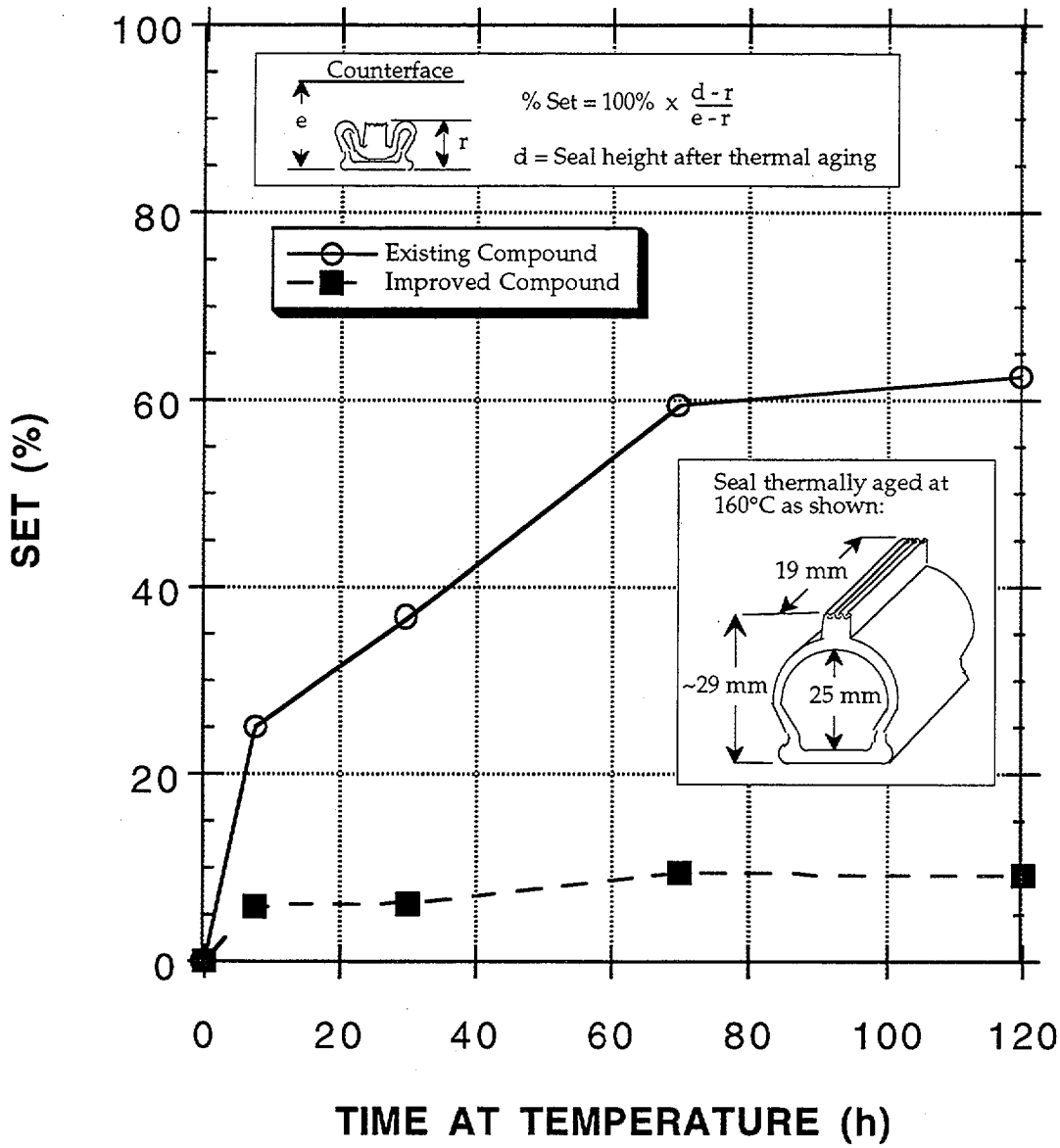


FIG. 4. Effects of thermal aging on compression set of inflatable door seal segments.

depressurization was problematic after thermal and radiation exposure. Differences in this rate were found to be due to subtleties in seal cross-sectional geometry and elastomer materials. Material properties were inconsistent—the compounds were not well specified or controlled. Tests also showed how the type and orientation of reinforcing fabric affected performance.

A program of aging and functional testing was initiated to select a more radiation- and ozone-resistant material, in cooperation with manufacturers. Figures 4 and 5 illustrate the improvement in compression set resistance to heat and radiation. Three-fold gains in life were realized. From a design and material improvement effort of ten person-months, a total savings of several hundred thousand dollars annually is expected, with corresponding gains in reliability.

A second example of an elastomer upgrade resulting in large savings and improved reliability in PHWR plants is the retrofit of improved fuelling machine snout plug O-ring seals. The O-ring in this case is in a piston-seal arrangement in a groove on the outside diameter of the snout plug (Figure 6). To facilitate insertion and removal of the plug, the groove is extra deep to give zero or low interference. Once inserted, the O-ring is expanded radially against the cylinder wall by an axial force

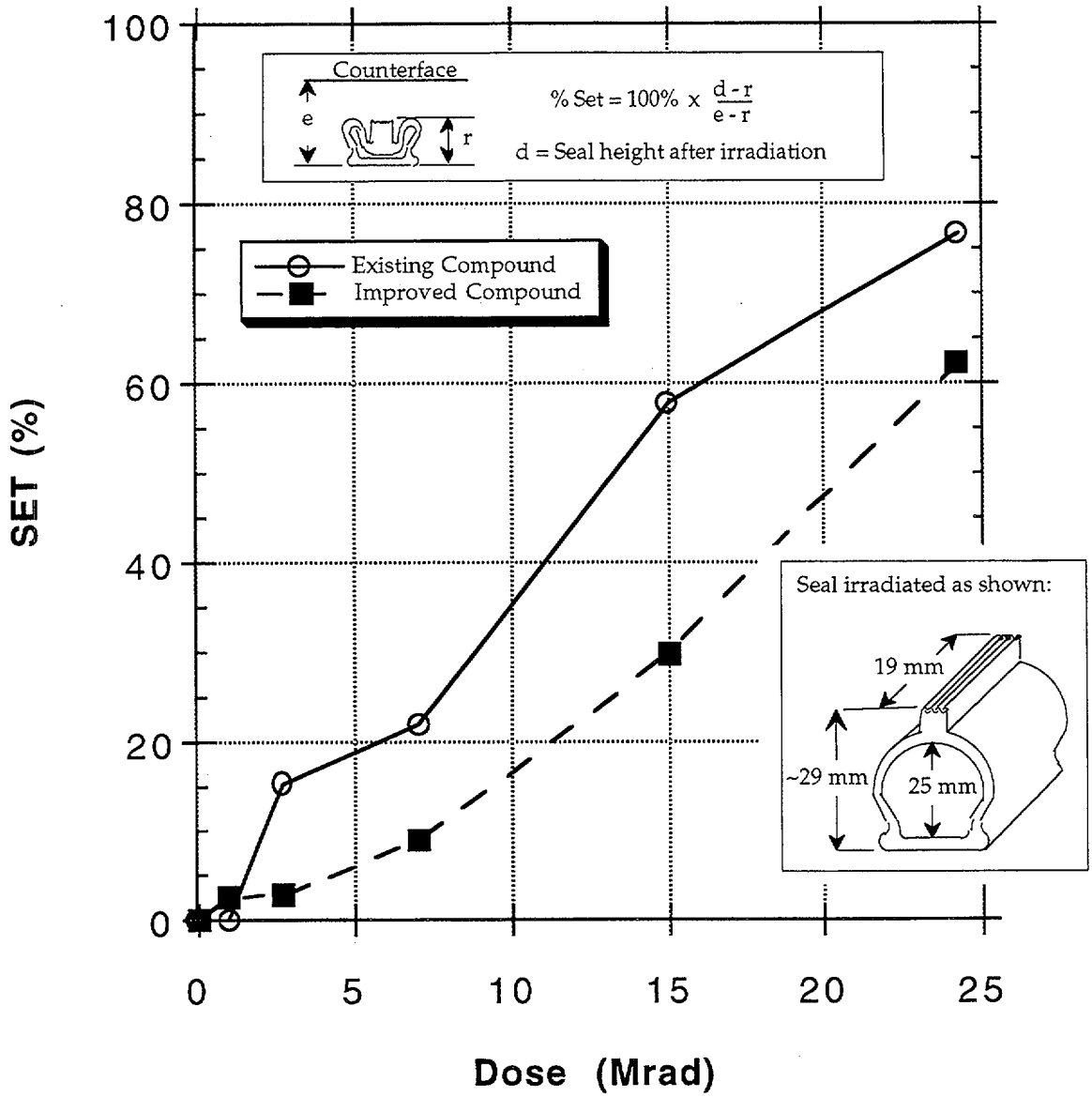


FIG. 5. Effects of gamma radiation aging on compression set of inflatable door seal segments.

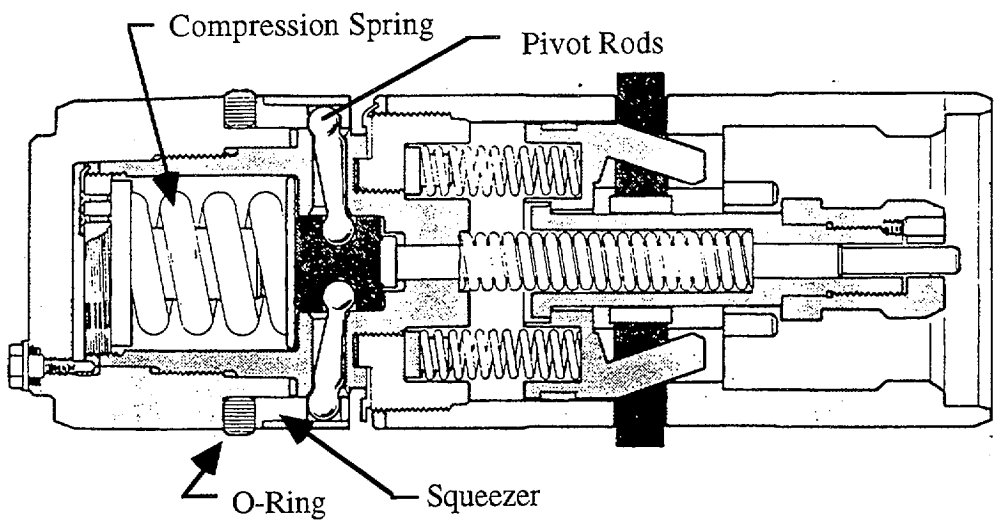


FIG. 6. Fuelling machine snout seal showing O-ring.

exerted through a spring-loaded squeezer (the O-ring is shown in the expanded position in Figure 6). For the 11 mm (0.43 inch) sectional diameter and 80 durometer O-ring used, this axial force (250-350 N per linear cm; 150-200 lbf per linear inch of O-ring) equates to the force for 20-30% squeeze of this O-ring (i.e., if squeezed between plates)—not an unusual amount. During each three-month period, the O-ring receives 10^5 grays (10^7 rad) of gamma radiation and is briefly exposed to 80°-180°C (175°-350°F) water approximately 200 times.

Previous O-rings were highly embrittled when routinely replaced after three months, often with chunks torn from them due to adhesion on the cylinder wall. Besides the leakage this caused, the chunks of rubber sometimes lodged themselves in components such as check valves in other parts of the fuel transfer equipment.

It was known from testing of the specific compound being used for these O-rings that the radiation dose had an insignificant effect on its compression set and hardness. Instead, thermal degradation, with adhesion to the wall and associated tearing stresses were the main problems to be overcome in selecting a better compound. From several well characterized candidates, the most likely compound was identified. A comprehensive program of service-specific qualification testing then confirmed its suitability. These O-rings now perform reliably in PHWR plants for four times as long.

There are many more examples of the high payback of elastomer seal upgrading. In addition to the direct payback in terms of increased service life and reliability, there are indirect benefits. The number of compounds becomes fewer. This simplifies the task of demonstrating service life and accident survivability, as is required in nuclear plants. It also reduces stores costs.

ACKNOWLEDGEMENTS

The air-lock door seal work described in this paper was paid for by the CANDU® Owners Group.

REFERENCES

[1] METCALFE. R., BASET. S.B., LESCO. R., and SELANDER. W.N., "Modelling of Space Shuttle Rocket O-Rings", Proceedings of the 12th International Conference on Fluid Sealing, BHR Group, Cranfield, England, (AECL Report AECL-11167) (1989).

[2] KURAN. S., GRACIE. B.J., and METCALFE. R., "Low Pressure Sealing Integrity of O-Rings Based on Initial Squeeze and Counterface Finish", Tribology Transactions, 38.2, (AECL Report AECL-11154) (1995).

NEXT PAGE(S) left BLANK

BORON INJECTION SAFETY SYSTEM MODIFICATION IN ATUCHA I NUCLEAR POWER PLANT

XA9848572

G. SALOM
Central Nuclear Atucha I,
Atucha

H. QUIROZ
Comisión Nacional de Energía Atómica,
Buenos Aires

Argentina

Abstract

The Boron Injection System is one of the Atucha I Nuclear Power Plant safety systems. This system is automatically activated by a trip of the safety system and turns the reactor subcritical by deuteroboric acid injection into the moderator.

The action of the system begins with the trip of the safety action and ends with the boron injection into de reactor. This is called the action time and it must be kept in an allowed range. In order to do that, in its original conception, the components were mounted into the reactor room, inside the containment. This location difficulties on-site inspection during reactor operation, and forces to shut down for maintenance and repairs.

The modification project consists in moving the boron injection system components, without changing the original required actuation time, from the reactor room to an outer place inside the containment where maintenance during the reactor operation is allowed.

1. INTRODUCTION

The Boron Injection System is one of the Atucha I Nuclear Power Plant safety systems. This system is automatically activated by a trip of the safety system and turns the reactor subcritical by deuteroboric acid injection into the moderator.

The action of the system begin with the trip of the safety action and ends with the boron injection into de reactor. This is called the action time and it must be kept in an allowed range. In order to do that, in its original conception, the components were mounted into the reactor room, inside the containment, this location difficulties on-site inspection during reactor operation, and forces to shut down for maintenance and repairs.

The Boron Injection System is normally in passive state, except during the repetitive tests, which consist of making the valves actuate for a few seconds.

The maintenance of injection boron system components caused plant disable several occasions, this is so because the actuation components are located into the reactor room, that involve to shut down the reactor for repairs.

The object of this work is to demonstrate the feasibility of moving the components outside the reactor room without increasing the system operation time.

2. DESCRIPTION

2.1. General description of Boron Injection System

The Boron injection system is a security system, whose function is turning the reactor subcritical by injection of deuteroboric acid into the moderator vessel. This injection leads to the reactor shut down and disconnect it from power generation.

The actuation of criteria this system are:

1- When the trip of reactor shut down appears, the first step is to produce the scram of control bar. This is the case that the subcritical stage (lesser than 70%), where not reached in a short time (3 seconds) .This may be so if the control bars do not came to the bottom position in less than three seconds.
2- When the Primary pressure presents a quick loss (more than 10 bar/sec.), and the pressure is lower than 108 bar. (this may be produced by leakage of the primary water cooler)
3- By hand activation trip from control room.

The Figure 1 shows the flow sheet of one of the tree branch of deuteroboric acid injection ($B_2O_3D_3$). To obtain the subcritical stage is enough that only two act, without consideration the actuation of control bar.

Two compressors feed up three sets of compressed air tubes at a pressure between 180bar to 200bar. Each set have 18 bottles of 50 liters each one, that means 900 liters per branch.

The valve TB11S03 is closed and keeps the vessel pressurized; the rest of the valves in the injection line are normally open.

The vessel TB11B01 is full of deuteroboric acid at 4% in water solution (160 liters) , this fluid is separated from reactor moderator water by the membrane valve TB11S11.

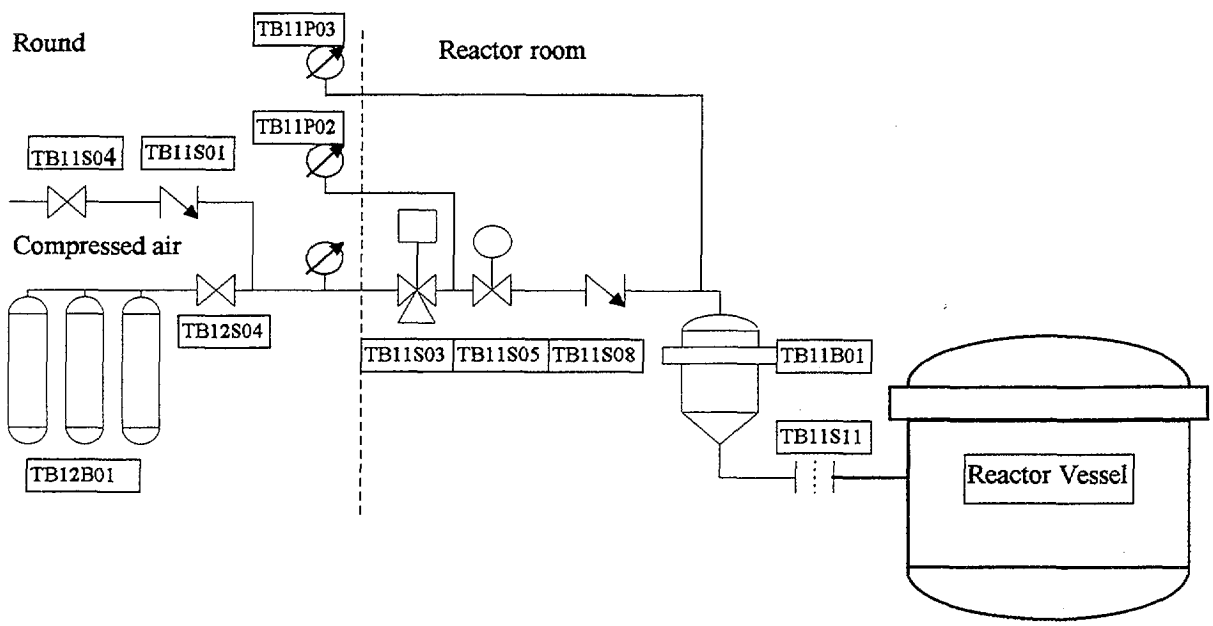


FIG. 1. Boron injection system.

When the boron injection trip signal, appears the pneumatic valve TB11S03 opens and pressurizes the boron vessel up to 175 bar. The membrane valve opens by rupture when the differential pressure between moderator and boron vessel 1 is more than 30bar.,

This system is tested periodically during power generation, by closing the electromagnetic-valve TB11S05 and assembling a calibrate orifice for venting on pressure measure branch TB11P03. (this prevents that any leakage of air in the valve from pressurizing the boron vessel and shutting down the reactor). During the test measures on pressure gage TB11P02 are taken. The system remains operative during the test because the valve TB11S05 opens when the trip is on.

In this system the time for decreasing the reactor criticality is crucial, because in case of power generation shut down the thermal power would increase in a few seconds reaching a maximum value then it would be decreased by action of the moderator, and some radioisotopes of higher neutron capture.

In case of boron injection a peek of 10,000MW would be reached in 0,5 second approximately.

Without boron injection, a peek would reach 60,000 MW. in less than 1 second.

2.2. Components Lay-out

The components are assembled in the Nuclear Power Plant according to the next distribution:

From compressors to TB11S03 valve excluded, they are placed in the round at 0 meters of level, outside the reactor room (this is an accessible area with radiological control, inside the contention) this include the compressed air bottles set, the regulatory system for the pneumatic actuation valve and pressure gages.

From the TB11S03 valve (included) to the reactor, they are located into the reactor room. This is an inaccessible zone during reactor power operation, whose access is restricted during maintenance time, because there is high activity and radioactive gases in this zone.

2. PROBLEMS FOUND IN THE SYSTEM

Since the start-up of the plant, some difficulties were found in the boron injection system which caused the power plant shut-down so as to repair the system. These problems were related to valves leakage's during repetitive tests.

The components can no be maintained or repaired directly during the operative period because they are placed near the proper reactor and control bars. Due to this fact, some problems in the system could lead to plant shut-down.

The seven more relevant events that might shut down the plant took up about 450hs including time of restart. On this time the power generation will be able around 4,000,000.00u$s. We have to take in account the radiological cost generated by repairing the system, which was estimated in 1Rem-man for each maintenance workers.

Based on this considerations, a modification proposal was made with the object of reducing the stopping time during system repairs or maintenance, and lessening the personal radiological risk.

3. PROPOSAL

The emergency boron system remains normally in waiting state and the electromagnetic valve is open except during repetitive tests. These consist of making the shot valve actuate for system corroboration. During these tests abnormal functions were detected by pressure measurement on pressure gages assembled on line. These abnormalities require intervention for its normalization.

In case of problems on one branch of the injection boron system, there is an presettled time of four hours to normalize the availability, over this period the plant must shut down. This time is not enough to repair some devices inside the reactor room, because any intervention need shutting down the reactor. Even if the problem is solved in short time, the service (power provision) can not start for a typical time of forty-four hours. The four hours may be sufficient enough if the system were located in an accessible area, like the one for heavy loads and entrance for big components, near the sets of compressed air bottles.

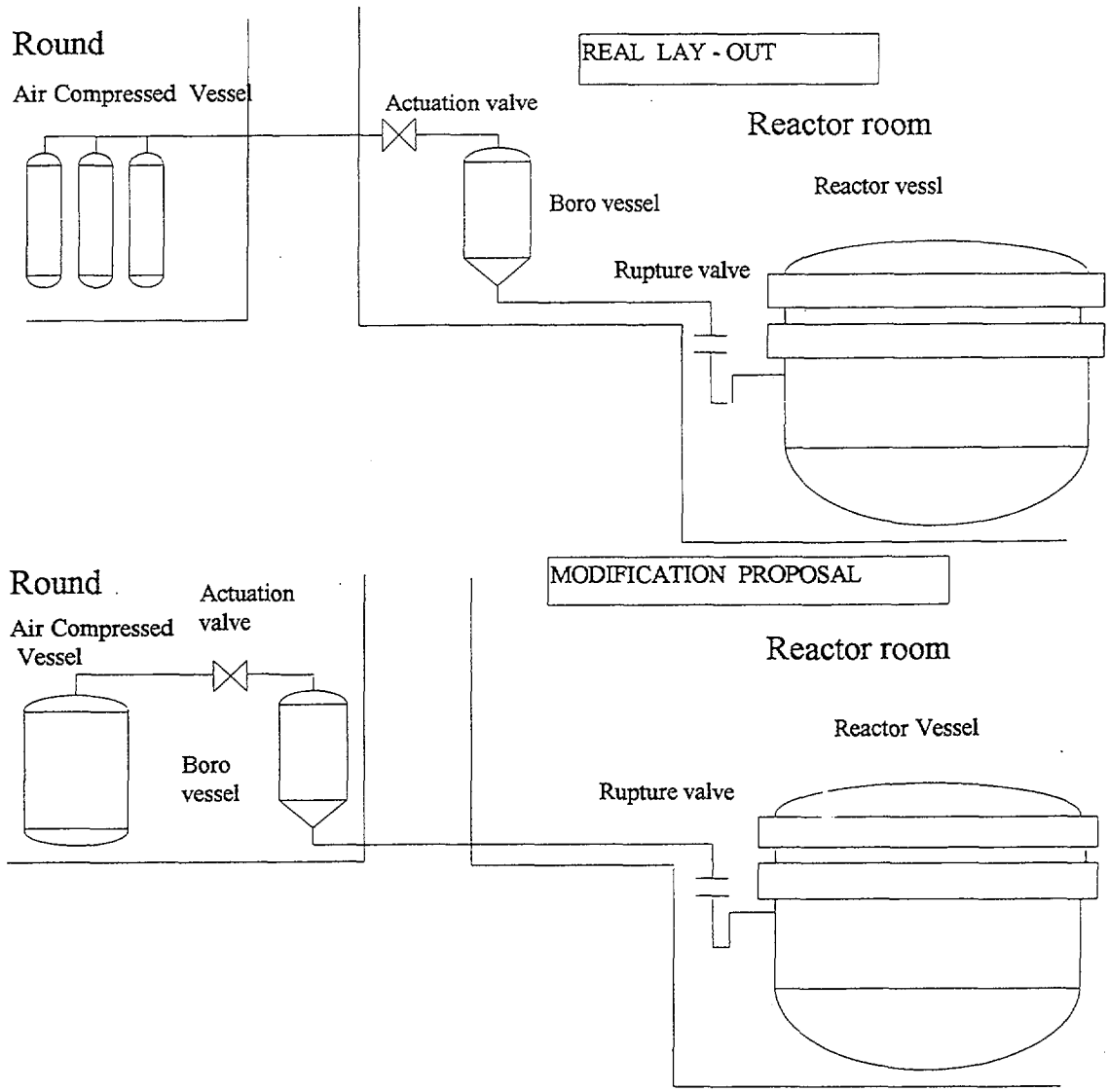


FIG. 2. Comparison between the real and the proposed emergency boron system.

Besides, the actual radiological condition on site is bad for workers, because the high radiological exposure and the high level of tritium and gases into the room. This facts generate the necessity of studying the moving of the conflictive components outside the reactor room to the round (in the actual site of pressure bottles) (Fig. 2).

The actuation time is critical in this system. Previous study (Ref [2]) showed that moving the valve S03 outside the reactor room (far from boron vessel) were practically impossible because the time required for pressurizing the pipe between the valve and the boron vessel is excessive. For this reason this proposal studies the moving of the total components outside the reactor room (Ref [3]). In this case a pipe full of water between B01 and S11 would be enlarged so that the pressurization would be practically instantaneous. But the pressure loss in the pipe would increase when the injection of liquid started.

For estimating the influence of modifying the system actuation time, we make a simple model of pipe between the B01 up to the discharge nozzle into the reactor moderator vessel. The time for injection 160 liters of deuteroboric acid from B01 to reactor moderator vessel is calculated by means of this mode, supposing a pressure impulse of 200 bar. and reactor back pressure of 115 bar. Over this model we compare the injection time for the real conditions against the proposed conditions. This period of time starts with the membrane rupture of valve S11, and finished when all 160 liters of deuteroboric acid stays into the moderator vessel. In this time we do include the trip signal elaborating time. The components response time and the boron diffusion time, because they remains constant in both configurations.

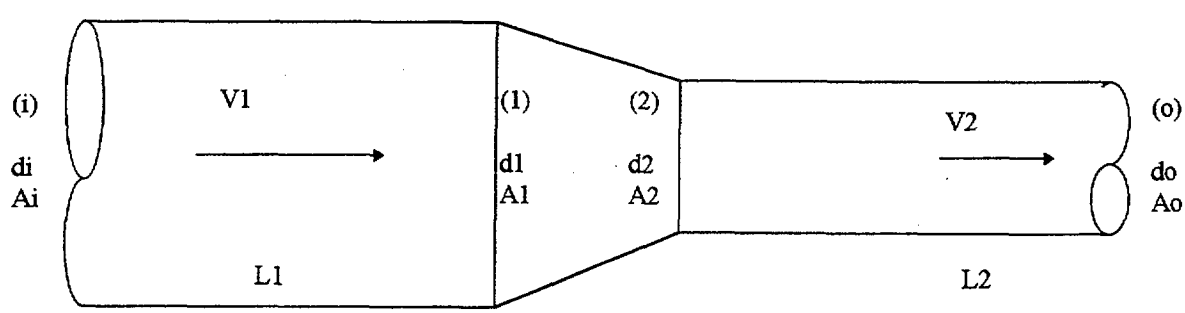
3.1. Mathematical model

We suppose that the system consists of two constant section pipe pieces joined by a reduction piece, the first part from B01 to S11, and the second part from B11 up to the extreme of pipe into the moderator vessel. The vessel B01 is not considered because their dimensions are negligible compared with the pipe length equivalent to fluid pressure drop and acceleration.

We consider two cases for valve S11, the first one does not take account of the pressure drop, and the second considers it like equivalent length of straight discharge pipe. The last one is the worst case in the drop pressure calculations.

3.1.1. *Calculation of the deuteroboric acid time injection*

We make the simplest model to determine the necessary time to inject the total volume into the moderator vessel (Fig. 3).



A: Inside Area L: Pipe Length. d: Inside Diameter v: Fluid Velocity

FIG. 3. Mathematical model.

i,1,2,o : Referential points

The pressure drop in the constant section pipe is calculated with the following expression:

$$\Delta p = \frac{f \times v^2 \times L \times \delta}{2 \times \times d} = C \times v^2$$

$$For.the.reduction:$$

$$\Delta p = \frac{Kc \times v^2 \times \delta^2}{2}$$

Where:
δ = Deuteroboric acid solution density.
Kc = Contraction coefficient.
g= gravity acceleration.

Newton's law is applied for studying the acceleration fluid:
Force = mass × acceleration

$$(pi - p1) \times Ai - C1 \times v1^2 \times Ai = \delta \times Ai \times L1 \times \dot{v}1$$

$$(p2 - po) \times Ao - C2 \times v2^2 \times Ao = \delta \times Aoi \times L2 \times \dot{v}2$$

Solving this equation system, we obtain the discharge fluid velocity (v2) as a function of time.

$$v2 = k \times \frac{\exp\left(\frac{2 \times t \times K \times \beta}{\gamma}\right) - 1}{\exp\left(\frac{2 \times t \times K\beta}{\gamma}\right) + 1}$$

Where:

$$\alpha = pi - po$$

$$\beta = C1 \times \frac{Ao^2}{Ai^2} + C2 + \frac{Kc \times \delta}{2}$$

$$\gamma = \delta \times L1 \times \frac{Ao}{A1} + \delta \times L2$$

$$k = \sqrt{\frac{\alpha}{\beta}}$$

$$B = \frac{2 \times k \times \beta}{\gamma}$$

From this equation we obtain the injection volume related to time, and so the necessary time to inject 160 liters of deuteroboric acid.

$$V = \frac{Ao \times K \times 2}{B} \times \ln\left[\frac{\exp\left(\frac{B \times t}{2}\right) + \exp\left(\frac{-B \times t}{2}\right)}{2}\right]$$

$$T = \frac{2}{B} \times \left\{ar\cosh\left[\exp\left(\frac{Vt \times B}{Ao \times K \times 2}\right)\right]\right\}$$

Where:

V= volume
t = time
Vt= Total injection volume.
T = Total injection time

We worked on seven cases from the TB11 subsystem. On this basis we explained the estimation of the next two systems (TB21 and TB31).

We considered the next combinations in each case:

1- The original system without pressure drop on S11
2- The modified system without pressure drop on S11 and 4 inch pipe.
3- The original system with an equivalent length of 0.47 meters of NW50 pipe, for pressure drop on S11.
4- The modified system with pressure drop on S11 same as item 3, and 4 inch pipe.
5- The modified system without pressure drop on S11 and 5 inch pipe.
6- The modified system without pressure drop on S11 and 90 degree reduction from 4 inch pipe to NW50.
7- The original system without pressure drop on S11 and 90 degree reduction from NW80 pipe to NW50.
8 y 9 - Idem 1 and 2 for TB21 subsystem
10 y 11- Idem 1 and 2 for TB31 subsystem

The results are resumed in Table I.

TABLE I. RESULTS OF THE DIFFERENT DEUTERIC ACID TIME INJECTION CALCULATION

Case	section B01- S11(m)		Drag coef.	Max. Veloc.	Injection time	Differential time
	Length	Diameter		(m/s)	(seconds)	(seconds)
1	6.00	0.0584	0.32	99.62.	1.464	0
2	16.50	0.0801	0.41	99.14	1.479	0.015
3	6.00	0.0584	0.32	77.85	1.843	0
4	16.50	0.0801	0.41	77.63	1.854	0.011
5	16.50	0.1032	0.47	99.39	1.466	0.002
6	16.50	0.0801	0.30	102.40	1.438	0.005
7	6.00	0.0584	0.24	101.99	1.433	0
8	5.60	0.0584	0.32	99.94	1.458	0
9	14.50	0.0801	0.41	99.47	1.472	0.014
10	5.00	0.0584	0.32	100.45	1.450	0
11	17.36	0.0801	0.41	99.00	1.483	0.033

The drag coefficient is related with the reduction on pipe diameter was taken from "Mecánica de los Fluido y Maquinas Hidráulicas " C. Mataix.

The first case is the referential time, its value is 1.464 seconds. If a graphical representation is made, we can see that the acceleration of fluid takes place during the first 0.2 seconds, this point represents practically the limit velocity of 99.62 m/s.

On the second case the time is 1.479 seconds, 15 milliseconds more than that of the actual system. On this case the reduction from 4 to 3 inches on S11 valve is considered as rough reduction (180 degree cone angle).

On third and forth case , the consideration of drop pressure on S11 valve did not make any significant difference from the previous case, just 11 millisecond more in the injection time. We see that considering the pressure droop on S11 does not generate important differences because this influences on the total injection time, not over its difference. We can see that taking in account more pressure drop(on intermediate valves, extremes, elbow etc.) decreases the importance of enlarging the pipe and introduces an advantage in the differential time calculation.

On fifth case the injection time is 2 milliseconds over the referential one.

The sixth case is similar to the second case with a reduction cone of 90 degrees. On this case the time results 5 milliseconds more than the referential time (seventh case).

The seventh case is referred to the calculation of the previous referential case supposing a gradual diameter reduction.

The eighth and ninth cases shows us that the time differences for TB21 is 14 milliseconds.

For both, the tenth and the eleventh cases, the time difference for TB31 is 33 milliseconds.

3.1.2. *Reduction of the pressurization time for pipe between S03 y B01*

According to test made in Germany on TB system (Ref./1/), the pressurized time on pipe from S03 to B01 vary according with the volume, the value obtain were: 147 milliseconds for 15,7 liters, on the actual system this time is shown in table II.

We obtain an important reduction on pressurized time, because there are an important reduction in the length of the pipe pressure gauge.

TABLE II. RESULTS OF THE TESTS MADE IN GERMANY

Subsystem	Volume between S03 to B01 (liters)	Time (seconds)	Differential time (seconds)
TB11	8.3	0.078	0.059
TB21	8.5	0.080	0.061
TB31	9.7	0.091	0.072
Proposal	2	0.019	

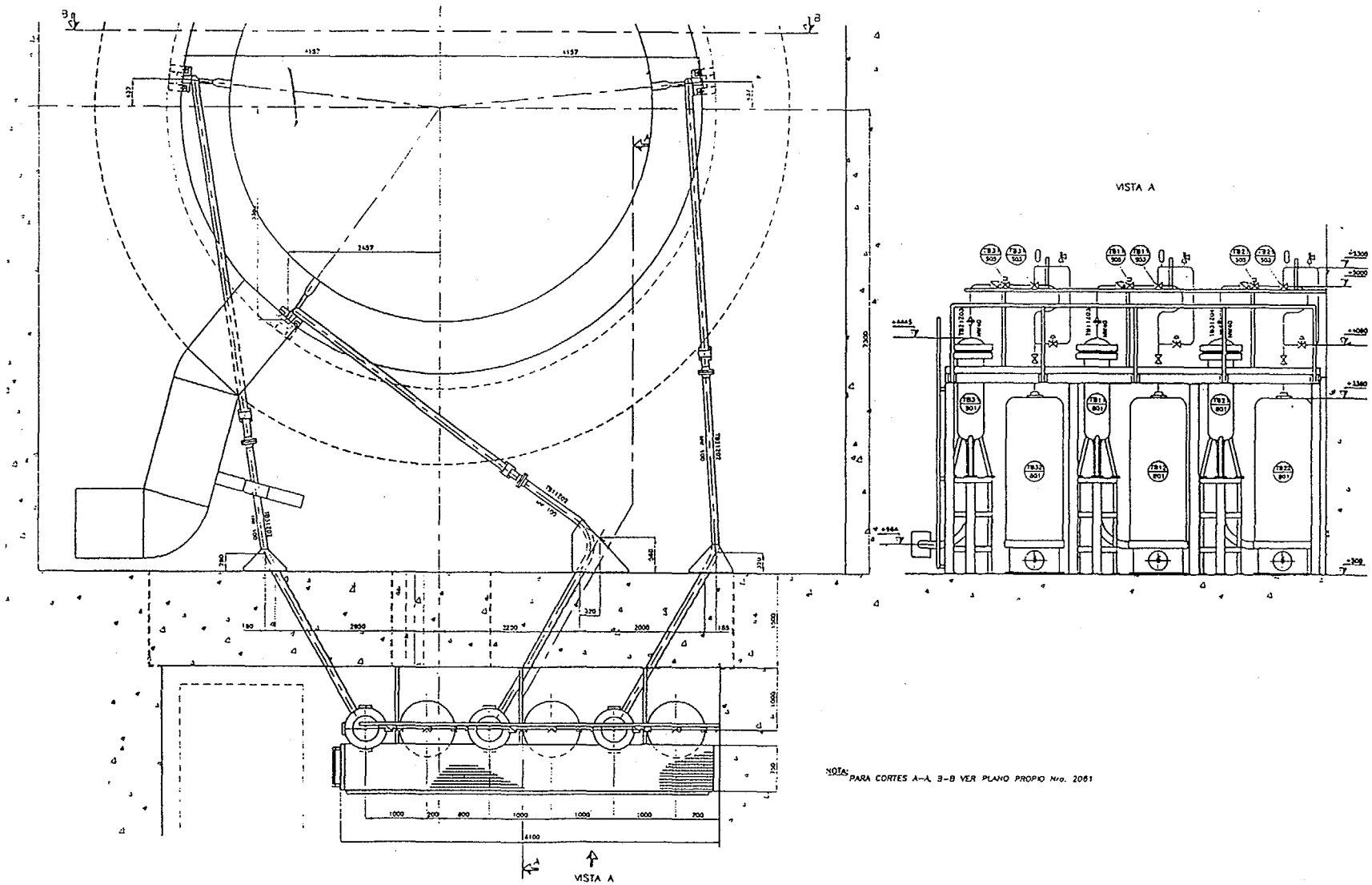


FIG. 4. General layout.

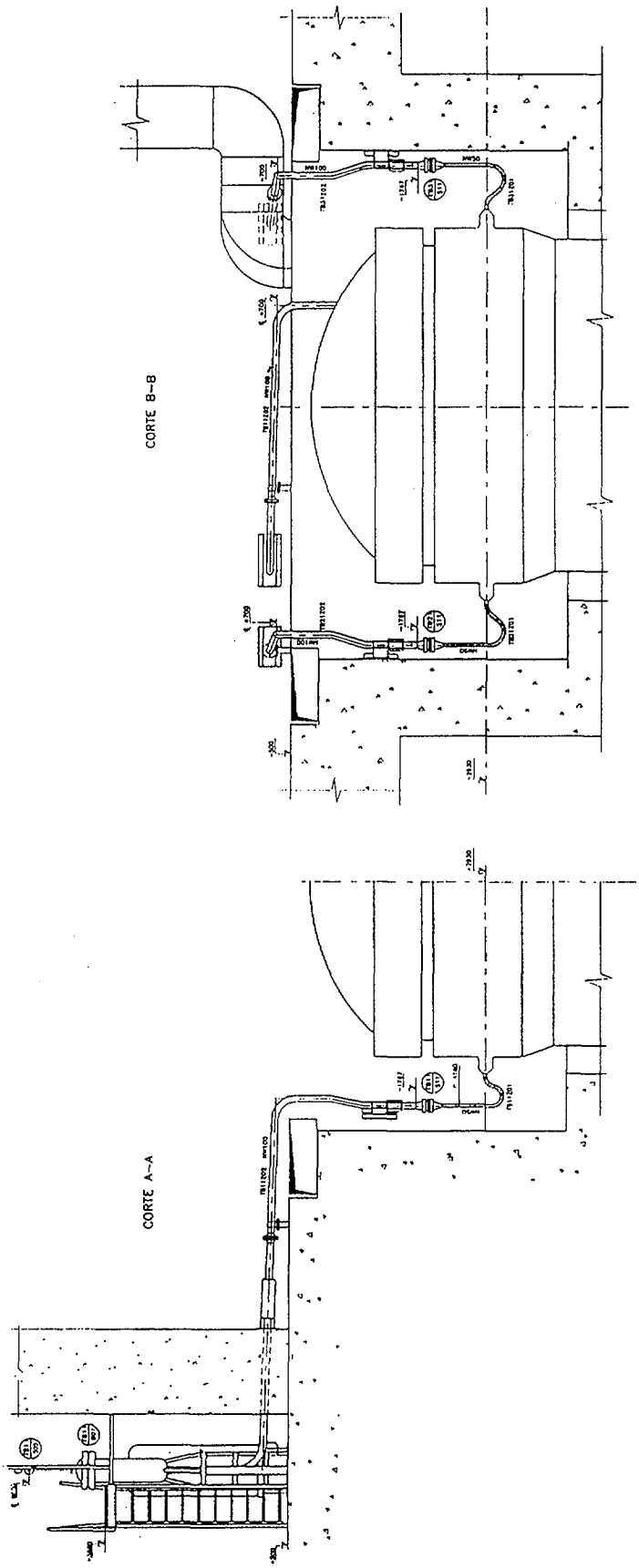


FIG. 5. Detailed layout, vertical section.

3.2. Results

As a result of the calculation we conclude that is possible to move S03, S05, B01 outside reactor room without increasing the injection time. The most unfavorable situation considered is valid (the one related to the alternative of 4 inches pipe prolongation) because the 14 milliseconds are compensated with the reduction of the pressurization time (59 milliseconds less on TB11 system, and even more in the others).

The pressure drop on the size reduction behind the valve S11 is important, due to the variation of the coefficient from 0.412 for row contraction to 0.07 for a cone of 10° (for a diameter relation from NW100 to NW50). For this reason the reduction section must be that of a cone of 10°.

In the actual system, the pressurized air is stored in a set of bottles made of carbon steel, this allows the oxide particles generated to travel throw the pipe and to deposit on the valve seat, this restricting the correct closure of the valves in the repetitive tests. To solve this problem we propose to change the compressed air bottles for a vessel made of stainless steel, with equal capacity for each branch.

4. ENGINEERING DEVELOPMENT

Based on the project, the necessary engineering work for relocating the components was done. On the enclosed draw (Fig. 4 and 5) we can see the general lay out of components, pipe and valves, forming a compact unit, outside the reactor room and accessible for maintenance during the power plant operation.

From the engineering study, we conclude that is possible to use the same boron vessel with modification of its outlet nozzle. Besides, it is possible to adapt the inlet nozzle of the valve S11 to avoid the reduction in pipe section between the valves and NW80 or NW100 pipe.

If we consider the dimensions in the discharge line of deuteroboric acid, the final computed time is shown in table III. The times are not increased for the modification.

TABLE III. FINAL COMPUTED TIME OF THE DICHARGE DEUTEROBORIC ACID LINE

Subsystem	Reference time (seconds)	Modified time (seconds)	Differential time (seconds)	Differential time for pressurization (seconds)	Total Differential time (seconds)
TB11	1.464	1.453	-0.011	-0.059	-0.070
TB21	1.458	1.456	-0.002	-0.061	-0.063
TB31	1.450	1.456	+0.006	-0.052	-0.056

REFERENCES

[1] Informe final sobre las pruebas y los resultados del sistema de parada de emergencia de boron Hecke Informe RTVA/v.H/753342 del 1.2.73

[2] Evaluación de las consecuencias de modificaciones en el sistema de inyección de boron P. Serrano S. Perez IT N° 101/85

[3] Propuesta de modificaciones al sistema TB IT N° 017/95

NEXT PAGE(S) left BLANK

IMPROVEMENT OF LIFETIME AVAILABILITY THROUGH DESIGN, INSPECTION, REPAIR AND REPLACEMENT OF COOLANT CHANNELS OF INDIAN PRESSURIZED HEAVY WATER REACTORS

XA9848573

B.B. RUPANI, R.K. SINHA
Bhabha Atomic Research Centre,
Mumbai, India

Abstract

This paper covers an overview of the work carried out for the life management of the coolant channels of Indian Pressurised Heavy Water Reactors.

In order to improve maintainability of the coolant channels and reduce down time needed for periodical creep adjustment, improved designs of channel hardware were developed. The modular insulation panel, designed as a substitute for the jig saw panels, reduces the time needed for accessing the space around the end-fitting significantly. A compact mechanical snubber has been developed to totally eliminate the need for periodic creep adjustment.

In addition, the paper also describes the technologies developed for performing some special inspection, repair and replacement tasks for the coolant channels. These include systems for garter spring repositioning by Mechanical Flexing Technique for fresh reactors and Integrated Garter Spring Repositioning System for operating reactors. A tooling system, developed for in-situ retrieval of sliver scrape samples from pressure tubes, is also described. These samples can be analysed in laboratories to yield valuable information on hydrogen concentration in pressure tube material. The current and planned activities towards development of technologies for improvement of the life time availability of the power plants are addressed.

1. INTRODUCTION

Current phase of the Indian nuclear power programme is based on 220 MWe and 500 MWe horizontal pressure tube type Pressurised Heavy Water Reactors (PHWRs). At present, seven 220 MWe PHWRs are under operation, one is under en-masse coolant channel replacement, four 220 MWe PHWRs are under construction and a programme of construction of additional reactors is under way. [1]

The schematic of a typical PHWR coolant channel is given in Fig. 1. The material of the pressure tubes of the seven Indian PHWRs is 20% cold worked Zircaloy-2, and in these reactors the garter spring spacers are loose fit around the pressure tubes. Subsequently the pressure tube material has been changed to 20% cold worked Zr-2.5%Nb alloy and the garter spring spacers are made tight-fit around the pressure tubes. Safe operation and life time availability of the reactor demand high assurance of structure integrity of the coolant channel, throughout the operating life of the reactor. In order to improve maintainability, inspectability and availability of the reactor, the development and implementation of the following approaches and technologies are necessary:

- Measures to extend the service life of the reactor
- Special devices for inspection of the coolant channels
- Design improvements to reduce downtime needed for periodical inspection
- Technologies to replace the coolant channels
- Analytical methodologies for assessment of safe operating life of the coolant channels

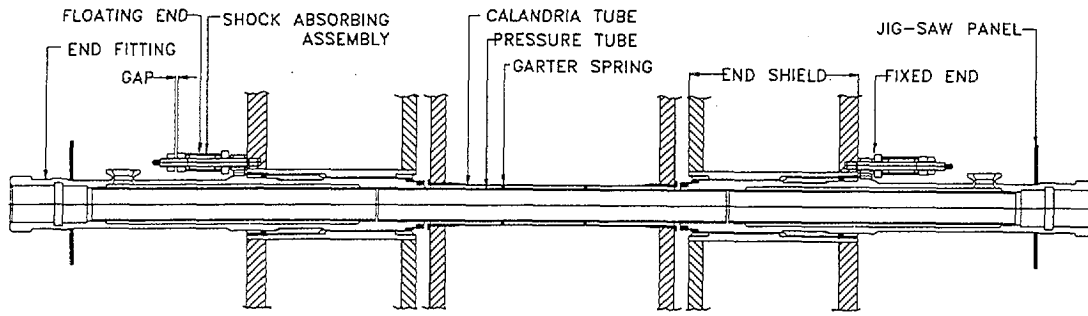


FIG. 1. Coolant Channel Assembly

2. MEASURES TO EXTEND THE SERVICE LIFE OF THE REACTOR

2.1. Life Extension of Coolant Channels by Garter Spring Spacer Repositioning

The annulus gap between pressure tube (PT) and calandria tube (CT) is maintained by annulus spacers called Garter Spring (GS) spacer. The loose-fit GS spacers, used in the first seven Indian PHWRs, have been found to be susceptible to displacement from their installed positions, mainly during the construction and commissioning stage of the reactor. This could result in occurrence of an early Pressure Tube-Calandria Tube (PT-CT) contact due to creep deformation of both tubes in that channel where such displacement of GS spacer is significantly large. The service life of a coolant channel may be reduced below its intended design life due to accelerated creep sag deformation of the PT followed by occurrence of PT-CT contact, when GS spacers are significantly shifted from their design locations.

The following systems have been developed for extending the service life of the coolant channels, when the GS spacers are not at their design locations. The displaced GS spacers are relocated to optimum positions in new as well as in operating reactors.

2.1.1. Mechanical Flexing Technique

GS spacer repositioning was carried out in NAPS-1&2 and KAPS-1 reactors after their hot conditioning using Mechanical Flexing Technique (MFT). The schematic arrangement for repositioning operation is shown in Fig. 2. The MFT employs a specially developed hydraulically actuated Pressure Tube Flexing Tool. The PTFT causes gentle cyclic flexing of the pressure tube, which enables the displacement of GS spacer [2]. A computer code "SCAPCA" (Static and Creep Analysis of Pressure tube and Calandria tube Assembly) was developed to assess the creep contact time on the basis of locations of GS spacers. This code also identifies the strategy of relocating the GS spacers to improve the service life of the coolant channels, if required.

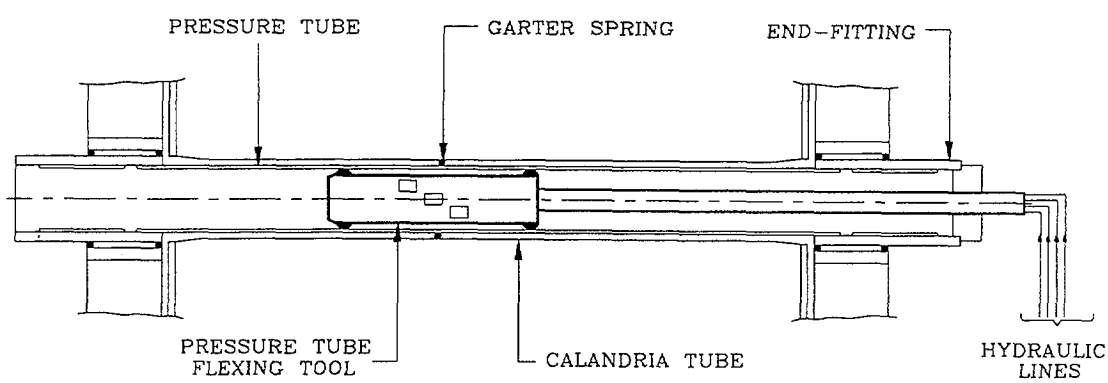


FIG. 2. Mechanical Flexing Technique

2.1.2. Integrated Garter Spring Repositioning System (INGRES-1S)

At time of construction of the first four reactors, RAPS and MAPS, displacement of GS spacers was not anticipated. For repositioning of the loose GS spacers in such operating reactors, a modular system called Integrated Garter Spring Repositioning System (INGRES-1S) for dry channels has been developed. The schematic arrangement of INGRES-1S is shown in Fig. 3. The major sub-systems of INGRES-1S are Pressure Tube Flexing Tool (PTFT), Electro-Magnetic Device (EMD), calibration set-up and feeding mechanism. The EMD consists of garter spring detection probe, concentricity detection probe, garter spring repositioning device and thermocouples. Operation of INGRES does not impose any unacceptable loads on coolant channels during its operation. The INGRES-1S has the following capabilities:

- Creation of restriction-free passage for the GS spacers
- Detection of location of the GS spacers
- Detection of the PT-CT concentricity
- Re-positioning of GS spacers as per identified strategies
- Accessibility up to centre of PT from one vault
- Measurement of temperature of GSRD

For operation of INGRES, the coolant channel should be defuelled and drained. An assembly of EMD is inserted through one end of the coolant channel, while the PTFT is inserted through the other end. After detection of locations of GS spacers and concentricity between PT and CT, the PTFT is operated to correct eccentricity between PT and CT at the location of GS spacer. This operation is done to provide a restriction free passage for the GS spacer. The GSRD causes GS spacer to move in the desired direction. This sequence is repeated after air cooling of GSRD, till the GS spacer is shifted to its desired position. The INGRES-1S was successfully used in nine coolant channels during first campaign in operating reactor at MAPS-2.

2.1.3. Integrated Garter Spring Repositioning System (INGRES-2S)

On the basis of experience gained during MAPS-2 operation, INGRES-2S has been developed for enhancement of performance. INGRES-2S has the following additional capabilities as compared to INGRES-1S.

- Improvement of restriction-free passage for the GS spacers
- Reduction in time, required for operation
- Accessibility of full length pressure tube from one vault with the help of 2000 mm long extension tubes
- Improvement in operating parameters of EMD
- Integration of all modules including two bending modules (BM)

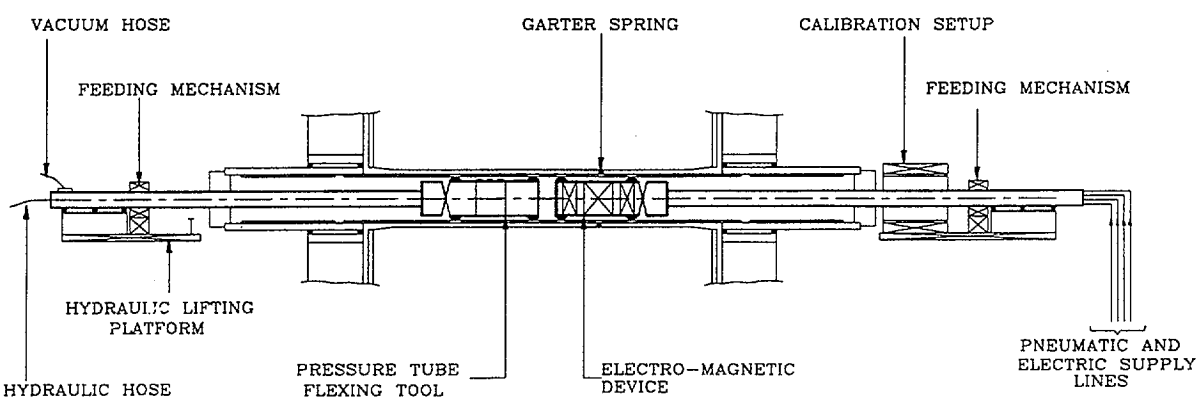


FIG. 3. Integrated Garter Spring Repositioning System (INGRES-1S)

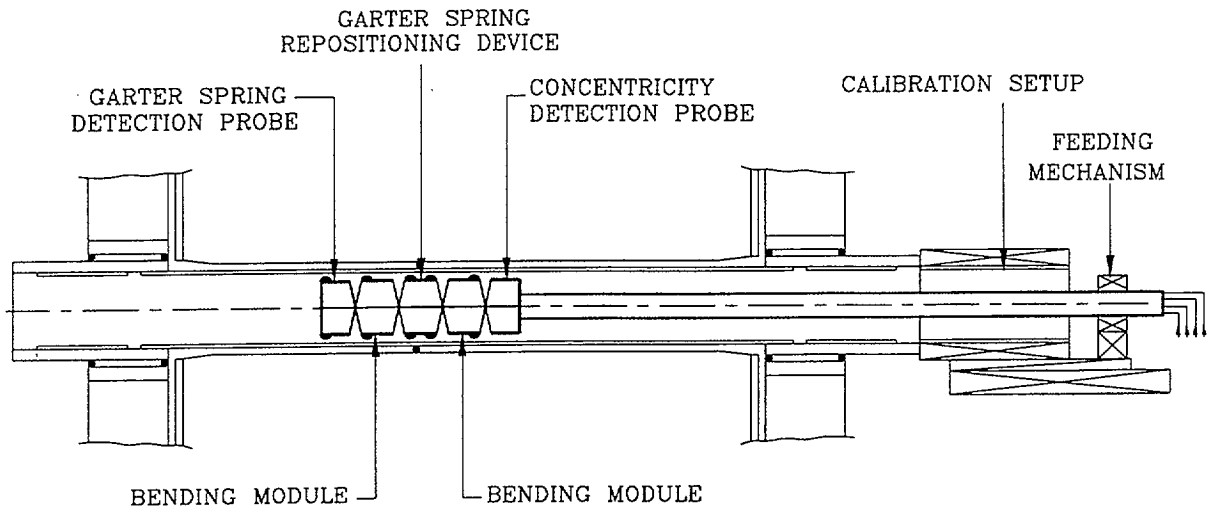


FIG. 4. Integrated Garter Spring Repositioning System (INGRES-2S)

INGRES-2S has been fully assembled at present. The testing of integral assembly of EMD and BM, called In-Channel Device (ICD), has been successfully completed. The qualification trials of INGRES-2S are being conducted. A schematic of the complete system of INGRES-2S is shown in Fig. 4.

INGRES-2S is being suitably modified for wet channel operation. The schematic arrangement of INGRES-2S delivery system for wet channel is shown in Fig. 5. Operation of INGRES-2S in wet coolant channel has the following additional capabilities as compared to operation of INGRES-2S in dry coolant channel:

- Special Closure Plug: To replace the normal channel closure plug (the replacement would be done using Fuelling Machine) before operation of INGRES and to retain pressure boundary of primary heat transport just before starting and just after completion of operation of INGRES.
- Closure Plug Actuating Mechanism: To operate the special closure plug to obtain a clear passage for ICD movement and to facilitate resealing of the coolant channel after completion of INGRES operation.
- Adaptor: To provide water seal for composite cables and to have junction box for electric, pneumatic and hydraulic connections to composite cables.

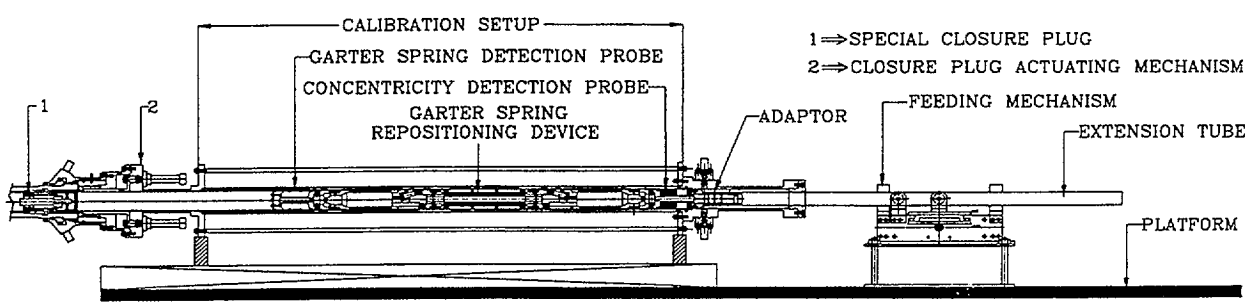


FIG. 5. INGRES-2S delivery system for wet channel operation

3. SPECIAL DEVICES FOR INSPECTION OF COOLANT CHANNELS

The regular In-Service Inspection (ISI) of the coolant channel of Indian PHWRs is performed under wet channel conditions, using a special system called BARC Inspection System (BARCIS). The regular ISI is sometimes required to be supplemented by additional visual inspection within the bore of the coolant channel components. For determination of equivalent hydrogen concentration in the pressure tube material, samples as slivers of 0.1 mm thickness and weighing about 50 mg are obtained. These special devices are discussed in the following paragraphs:

3.1. Dry Channel Visual Inspection System

The DRY channel Visual Inspection System (DRYVIS) is developed for carrying out visual inspection within PHWR coolant channels. Entire length of the bore of the coolant channel can be scanned with a good clarity, good resolution and reasonably accurate capability to size the indications found on the surface being scanned. The device can be remotely positioned anywhere within a given channel with low personnel radiation exposure. Once the device is placed in one of the ends of coolant channel manually, it can be propelled into the channel and withdrawn back to original location using remote control.

DRYVIS consists of a tool carrier system, CCTV system based on radiation resistance miniature camera, external lighting fixture, grating for sizing and axial position indicating system.

DRYVIS-1 & 2 are being used for visual inspection of the pressure tube and calandria tube respectively with basic design remaining same. The dimensions of tool carrier systems are suited to respective tubes. [3]

3.2. Sliver Sample Scraping Technique

For assessment of safe operating life of pressure tubes of PHWRs, it is necessary to estimate the hydrogen concentration in the pressure tube material, and to establish hydrogen or deuterium pick-up rate by the pressure tubes under service conditions. To carry out such assessment without removal of pressure tubes and to increase the availability of the reactor, it is necessary to obtain sliver samples of the pressure tube material without affecting integrity and residual service life of the pressure tube. [4]

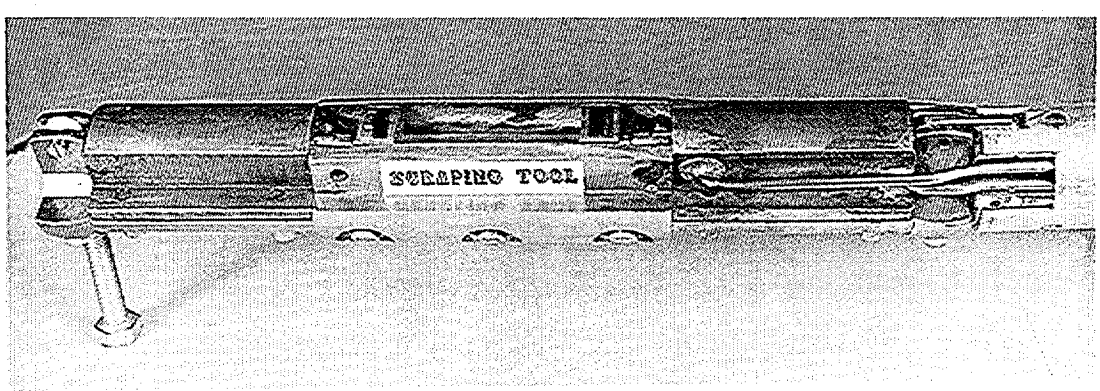


FIG. 6. Scraping Tool

A Sliver Sample Scraping Technique (SSST) has been developed to obtain samples from specified location within the bore of sagged (35 mm maximum) pressure tubes of PHWRs for determination of residual service life. During qualification trials, about 100 sliver samples have been obtained successfully from the irradiated pressure tubes, removed from RAPS & MAPS reactors for determination of operating parameters, evaluation of scraped region of pressure tubes and evaluation of material samples. In order to minimise personnel radiation exposures, a remotised driving system has also been developed for axial positioning of scraping tool in the pressure tube of a coolant channel at reactor site. A scraping tool is shown in Fig. 6.

4. DESIGN IMPROVEMENTS TO REDUCE DOWNTIME NEEDED FOR PERIODICAL INSPECTION

Components have been developed to increase the availability of the reactor and to reduce personnel radiation exposure as follows:

- Compact Mechanical Snubber: To eliminate periodic adjustment of gap for creep by incorporating a special device using as a shock absorbing assembly.

- Modular Insulation Panel: To reduce time required for overall creep adjustment and repair & maintenance works to be done on coolant channel by facilitating quick assembly and disassembly of panels.

4.1. Compact Mechanical Snubber

Axial restraint for the coolant channel, following postulated guillotine rupture of the pressure tube, is provided by a shock absorbing assembly (SAS). These assemblies are located on the both end-fittings of the coolant channel, as shown in Fig. 1. The functions of SAS are as follows:

- To absorb the shock or impact load in case of pressure tube rupture
- To permit axial elongation of coolant channel in a controlled manner

In present design, it is necessary to monitor the elongation of individual coolant channel and to carry out an adjustment of the gaps periodically to avoid the imposition of unacceptably high forces on the pressure tube and end-shields. Creep adjustment requires considerable personnel radiation exposure and also longer outage. In view of this, a device, called Compact Mechanical Snubber (CMS), has been developed to take care of above mentioned functions automatically.

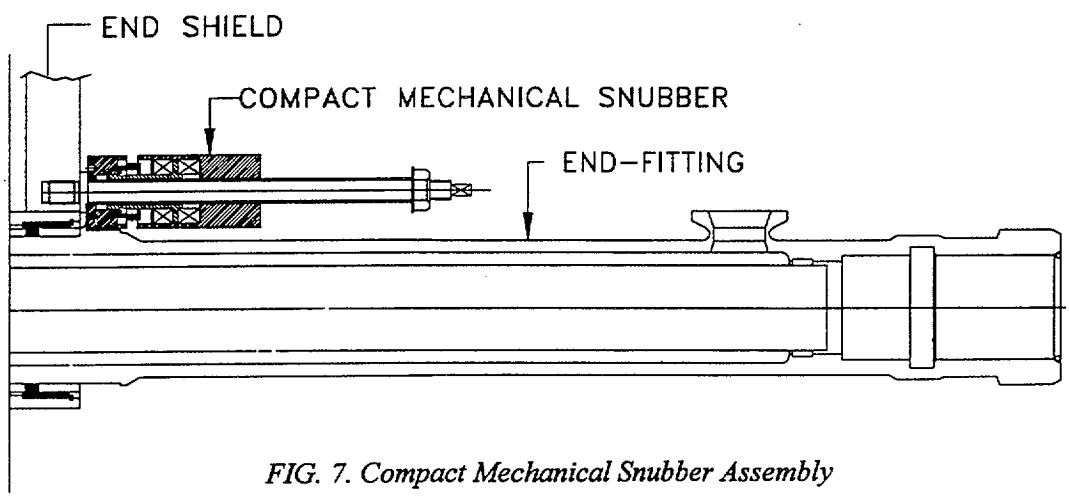


FIG. 7. Compact Mechanical Snubber Assembly

The CMS consists of major components, such as spring loaded sub-assemblies, non-rotating thrust-block, rotating nut and stud. An axial elongation of the coolant channel would be transmitted to the thrust block causing a resisting inertia force, proportional to the acceleration of coolant channel, being developed on CMS. Under the action of this force, the spring loaded sub-assembly would change its length. As long as the acceleration remains within the activation level of the snubber, it will permit the axial movement of the thrust block without any significant resisting force. However once the acceleration exceeds the activation level the non rotating thrust block gets locked up with the rotating nut, causing complete seizure of the snubber on the stud. The value of the activation level can be easily adjusted by altering a spring member. The schematic arrangement of the CMS, developed for RAPS and MAPS, is shown in Fig. 7.

4.2. Modular Insulation Panel

The construction of insulation cabinet at end fitting penetration is called Jig-Saw panel. These panels are required to prevent leakage of hot air into the fuelling machine vaults These panels fill the inter-space area among end-fittings. These panels form part of insulation cabinet in fuelling machine vaults. The present design requires considerable personnel radiation exposure for assembly or disassembly at the time of creep adjustment or any other repair or maintenance works to be done on coolant channels. In view of this new design called Modular Insulation Panel (MIP) is being developed as shown in Fig.8. This new design would minimise personnel radiation exposure and reduce plant down time considerably. A large number of MIPs has been fabricated and they are under qualification trials at operating reactor site. [5]

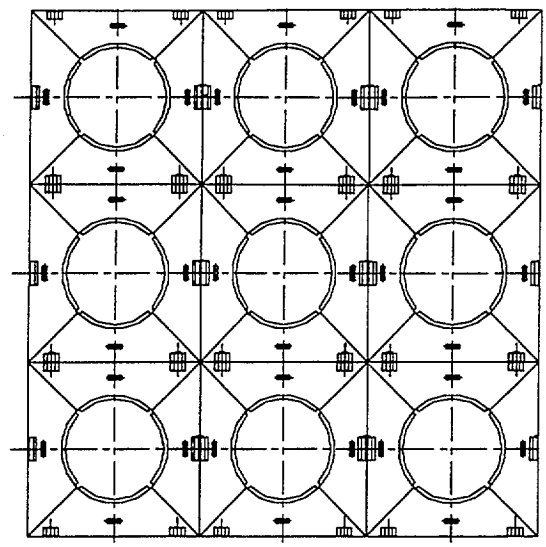


FIG. 8. Modular Insulation Panels

5. TECHNOLOGY TO REPLACE THE COOLANT CHANNELS

In-reactor service life of the Zircaloy-2 pressure tube is expected to be around 8 to 10 effective full power years. In order to enhance the life of a reactor using these pressure tubes, it is necessary to replace all the pressure tubes before their safe service life is over. Going by the experience of manual removal of pressure tubes in Indian PHWRs, it is expected that it would consume very high personnel radiation exposure for replacement of all coolant channels of one reactor. This would involve a long down time of a reactor and arranging a large trained man-power will be difficult.

Keeping this in view, a semi-automatic and remote operable Coolant Channel Replacement Machine (CCRM), as shown in Fig. 9, has been developed. CCRM mainly consists of a self elevating work table, cross travel system, co-ordinate table, remote operable overhead crane, alignment system and servo manipulator. A large number of tooling to perform various tasks for replacement and refurbishment has also been developed.

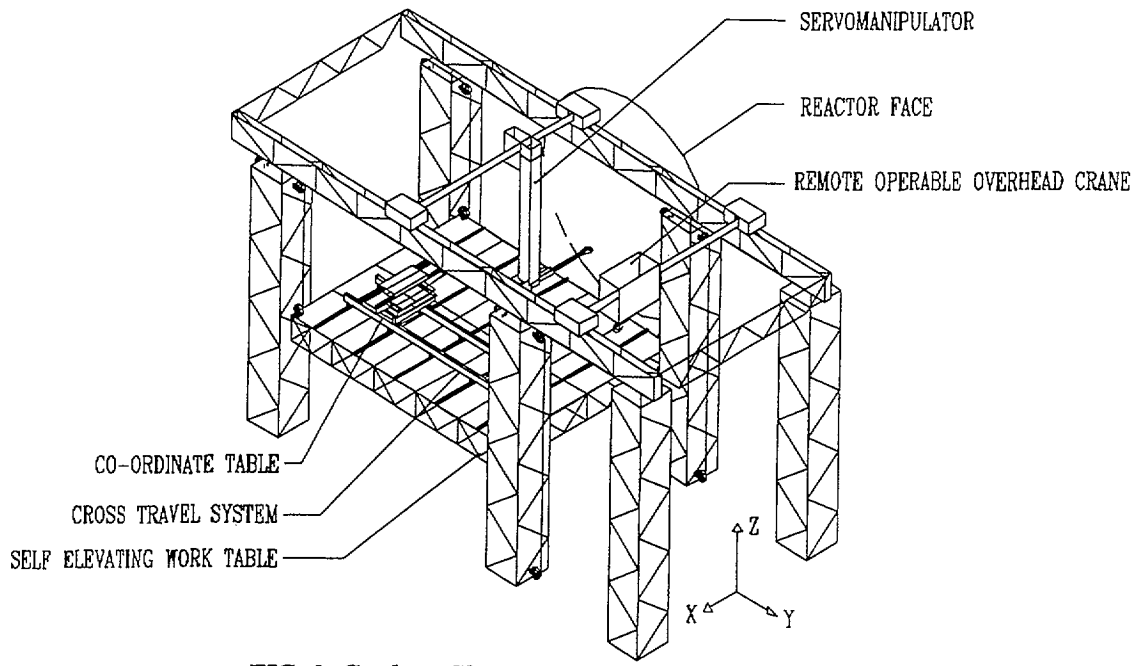


FIG. 9. Coolant Channel Replacement Machine

TABLE I. COMPUTER CODES

Computer code	Objective
(SCAPCA): Static and Creep Analysis of Pressure tube and Calandria tube Assembly	• To predict creep contact time • To determine the gap closing rate
(HYCON-95): HYdrogen CONcentration estimation	• To estimate the oxide thickness • To estimate Hydrogen concentration at any axial position along the length of the pressure tube • To estimate Hydrogen and Deuterium pick-up rate
(BLIST1D) & (BLIST2D): BLISTer estimation codes	• To study the relationship between time and depth of blister • To study the phenomenon of Hydrogen and Deuterium migration
(CEAL): A Code for Estimation of Assurance of Leak before break	• To estimate the critical crack length from fracture toughness • To estimate the leak rates through axial cracks in pressure tube • To assess required operator response time

6. ANALYTICAL METHODOLOGIES FOR ASSESSMENT OF SAFE OPERATING LIFE OF THE COOLANT CHANNELS

Methodologies have been developed in India to model and analyse the major life limiting mechanisms for pressure tubes. [6] Computer codes have been developed for determination of creep and growth related dimensional changes of coolant channels, deuterium pick-up rates in Zircaloy-2 pressure tubes, blister growth following occurrence of pressure tube-calandria tube contact, and operating domain to achieve Leak Before Break (LLB) of pressure tubes. These codes have been validated with reference to the data of In Service Inspection (ISI) and Post Irradiation Examination (PIE), available for the coolant channels of Indian PHWRs. The Computer codes, along with their objectives are listed in Table I.

7. CONCLUDING REMARKS

Technologies and facilities to carry out the required in-service inspection, life extension, and replacement for improving availability and reliability of the coolant channels of Indian PHWRs are either already available or in advanced stage of development. Capability to assess safe operating life of pressure tubes under the various degrading mechanisms has been developed in India in the form of computer codes. A large scale programme for carrying out en-masse replacement of coolant channels in the lead reactor, RAPS-2 is already under way. Future work will involve the augmentation of the current technologies for wet channel operation and automation to improve availability of current and future PHWRs. The computer codes would be tuned finely on the basis of data obtained from additional In Service Inspection and Post Irradiation Examination, performed on a large number of pressure tubes of Indian PHWRs.

ACKNOWLEDGEMENTS

The authors wish to thank their colleagues in the Reactor Engineering Division, BARC who have participated in the different activities, overviewed in this paper.

REFERENCES

[1] Sinha, R.K., and Kakodkar Anil, "Management Of Ageing of Pressure Tubes of Pressurised Heavy Water Reactors", IAEA Specialists Meeting on Technology for Life Time Management of Nuclear Power Plants, Tokyo, Japan (1994).

[2] Sinha, R.K., "Mechanical Flexing Technique for Extension of Life of Coolant Channels Having Displaced Garter Spring Spacers", BARC NEWS letter No.102, (1992).

[3] Rupani, B.B. and Kayal, J.N., "In Service Visual Inspection for Coolant Channels of Nuclear Reactors" National Seminar on NDE in Power Industry (NDE-92), Trichy, India (1992).

[4] Rupani, B.B. and Sinha, R.K., "Sliver Sample Scraping Technique for Application in Determination of Residual Service Life of Tubular Components", 14th World Conference on non-destructive Testing (14th WCNDT), New Delhi, India (1996).

[5] Rupani, B.B. and Sinha, R.K., "Modular Insulation Panel - A Substitute for Jig-Saw Panel", Internal Report, BARC, Mumbai, India.

[6] Sinha, R.K., Sharma, A., Madhusoodanan, K., Sinha, S.K., and Malshe, U.D., "Methodology for Assessment of Service Life of Pressure Tube in Indian PHWR", IAEA Technical Committee Meeting on Advances in Heavy Water Reactor, Mumbai, India (1996).

NEXT PAGE(S) left BLANK

XA9848574

BOHUNICE V-1 AND V-2 APPROACH FOR ACHIEVING HIGH AVAILABILITY, RELIABILITY AND SAFETY

M. LIPÁR, J. KERAK, Š. ROHÁR
Nuclear Power Plant Jaslovské Bohunice,
Nuclear Regulatory Authority,
Slovakia

Abstract

Long term operating experience of Bohunice units maintenance activities are overviewed in the paper. Based on common experience of WWER NPP operators, separate maintenance department was established at Bohunice NPP in very early stage of plant operation. Maintenance management, maintenance planning, outage management, diagnostics and monitoring, inspection technologies and backfitting activities are described particularly to demonstrate the capability of Bohunice maintenance department for most complex repairs and maintenance works of nuclear power plant components and equipment, including reactor and turbine itself.

1. INTRODUCTION

The WWER 440/V 230 was the first commercial model of the former Soviet WWER design of nuclear power plant constructed and operated in the former Czechoslovakia. The construction site, due to lack of local electrical power sources, was pre-selected on the south-west area of Slovakia. Another reason for this sitting was an availability of experienced personnel from the previous construction, commissioning and operation of experimental NPP A-1 (HWGCR) in Bohunice construction site. The units of V-1 NPP were consequently connected to the grid in 1978 and 1980.

The construction of next reactor twins, model WWER 440/V 213, was completed in 1984 and 1985. Improved design of V 213 model can cope with large LOCA accident scenario and it has the safety features that could provide relatively large safety margins.

The first reactor twins are administratively managed as a Bohunice V-1 NPP and second reactor twins as a Bohunice V-2 NPP.

Right after commissioning all of WWER units in Bohunice have generated an annual electricity production rate near to 3000 GWh which have been found as a reasonable contribution to the national energy system. After the split of former Czechoslovakia the total output of electricity from both units represents about 50 % of total electric energy production in Slovakia (Fig. 1).

After 10 years of operation, the design and operational safety of V-1 NPP and V-2 NPP have been re-evaluated. Based on results of the cost-benefit type analysis, the safety enhancement programme was established for V-1 NPP. The safety improvement program for V-2 NPP is under preparation and will be based on results of periodic safety review after 10 years of operation.

2. MAINTENANCE MANAGEMENT

Long-term operating experience of Bohunice units has shown that maintaining a high level of availability and reliability can be accomplished by systematic preventative maintenance and by high-quality of maintenance preparation, and maintenance quality control during outages with refueling particularly.

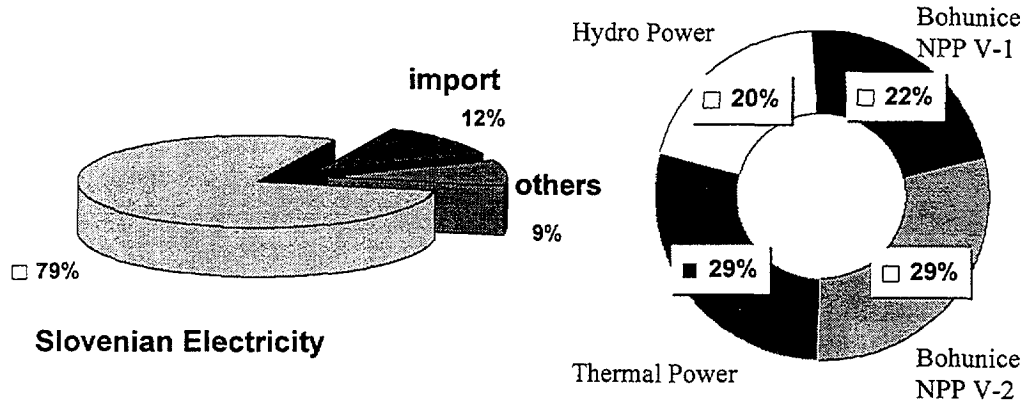


FIG. 1.Structure of production of electricity from power sources in Slovakia-1996.

Based on common historical experience, majority of WWER nuclear power plant operators established separate maintenance departments which are supported by sufficient personnel and equipment. Based on this philosophy, Bohunice V-1 NPP management in earlier pre-operational stage started preparation and recruiting of maintenance personnel along with operational personnel, being the first commercial NPP in Slovakia at that time. The conception to provide equipment and to train the personnel for most complex repairs and maintenance works of nuclear power plant components and equipment including reactor and turbine itself was followed at the establishment of Bohunice NPP maintenance division.

2.1 .Organization of maintenance group

The maintenance division in Bohunice NPP consists of the following departments:

- maintenance preparation
- in-service inspection
- pressure component maintenance
- rotating component maintenance
- workshop facility and civil structure maintenance
- electrical and lifting equipment maintenance

The maintenance of I&C equipment and partially the special electrical equipment and systems is the responsibility of the electrical and I&C departments within the NPP Operation Division.

2.2. Maintenance facilities

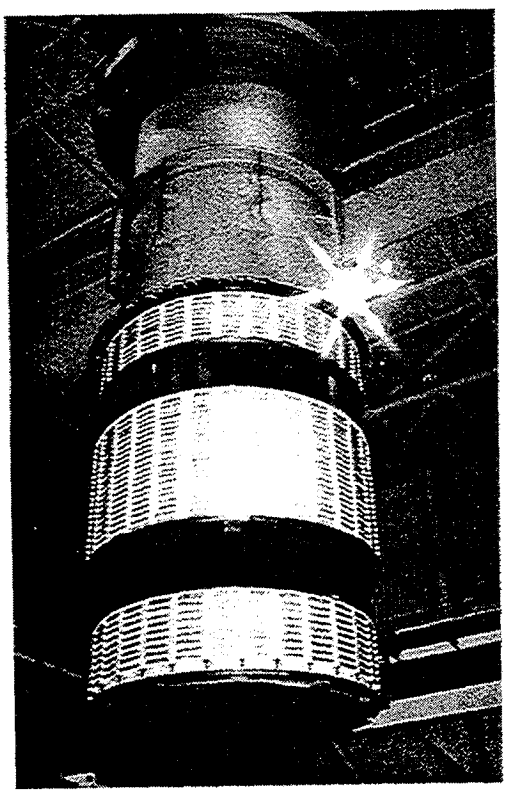
To ensure that maintenance will be carried out effectively, nuclear power plant has appropriate maintenance workshop facilities and laboratories, namely:

- mechanical shops (inside and outside the control area)
- electrical shops
- laboratories used for:
  - I&C equipment
  - decontamination
  - radiation protection equipment

2.3. Special facilities

For rehearsing works and personnel on the job training, the most important equipment or their particular sections are available as a full size mock-ups:

- reactor pressure vessel (model V 213)
- main isolation valve of primary loop
- main cooling pumps V-1, V-2
- steam generator header



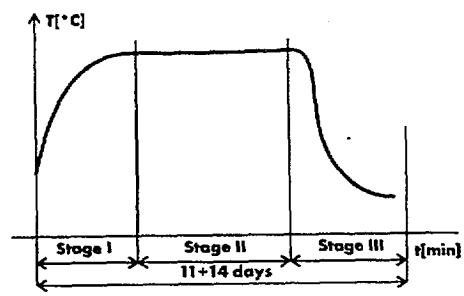
Regeneration annealing basic data

The activity consists of three stages:

Stage 1
- heating to working temperature by prescribed speed, at the same time reactor pressure vessel is dried

Stage 2
- keeping the annealing temperature

Stage 3
- cooling after regeneration annealing by prescribed speed.



Course of temperatures during regeneration annealing

FIG. 2. Annealing furnance.

- special valves
- special pumps
- special electrical equipment
- primary circuit pipes
- special maintenance equipment:
  - annealing furnace (Fig. 2)
  - sampling equipment for RPV of basic, and
  - weld materials

2.4. Special equipment and tools

- remote handling manipulators and remotely operated special purpose tools, both for RPV and SG
- automatic welding and cutting equipment
- remotely operated non-destructive testing equipment (see ISI)
- automatic in situ valve set lapping machine for all diameters
- remote viewing equipment such as mirrors, binoculars, telescopes, periscopes, boroscopes, fibroscopes, closed circuit television and remotely operated cameras
- communication systems such as direct line telephones, radio and communication equipment
- special containers for contaminated items
- shielded containers and portable shielding
- radiation protection clothing and equipment
- material and equipment for controlling and containing radioactive contamination
- fixed or rapidly assembled access equipment to reduce personnel exposure, such as permanent ladders or telescopic cradles
- photographic and video records

2.5. Administrative controls

The administrative controls cover all activities related to the maintenance program, and they are as follows:

- maintenance planning
- maintenance co-ordination
- maintenance work procedure development and revision

- in-service inspection
- work order authorization
- equipment isolation permit
- industrial safety permit
- fire hazard permit
- spare part and material management
- housekeeping and cleaning
- maintenance and in-service inspection recording
- modification and replacement control
- outage management
- special maintenance activities
- personnel training.

All these activities are carried out by maintenance division or by operation division (in the electrical and I&C areas).

3. MAINTENANCE PLANNING

To assure an optimal reliability oriented maintenance of the nuclear equipment, the plant management issues maintenance long-term plans. According to existing rules, the long-term maintenance plans for each unit have to be worked out (for period 4 or 5 years). Main goals for this planning come from the maintenance program requirements and planned items are as follows:

- planning of outages
- planning of the most important equipment overhauls
- planning of spare parts supply
- planning of maintenance supplier organizations contracting
- planning of finances.

The computer technique is used within all phases of planning.

The maintenance program, based on equipment suppliers' recommendations, safety analyses and reliability records of equipment based on operational experience is an input database for planning. The maintenance programme modifications concerning safety important equipment are subject for assessment and approval of the national Nuclear Regulatory Authority of the Slovak Republic (ÚJD SR).

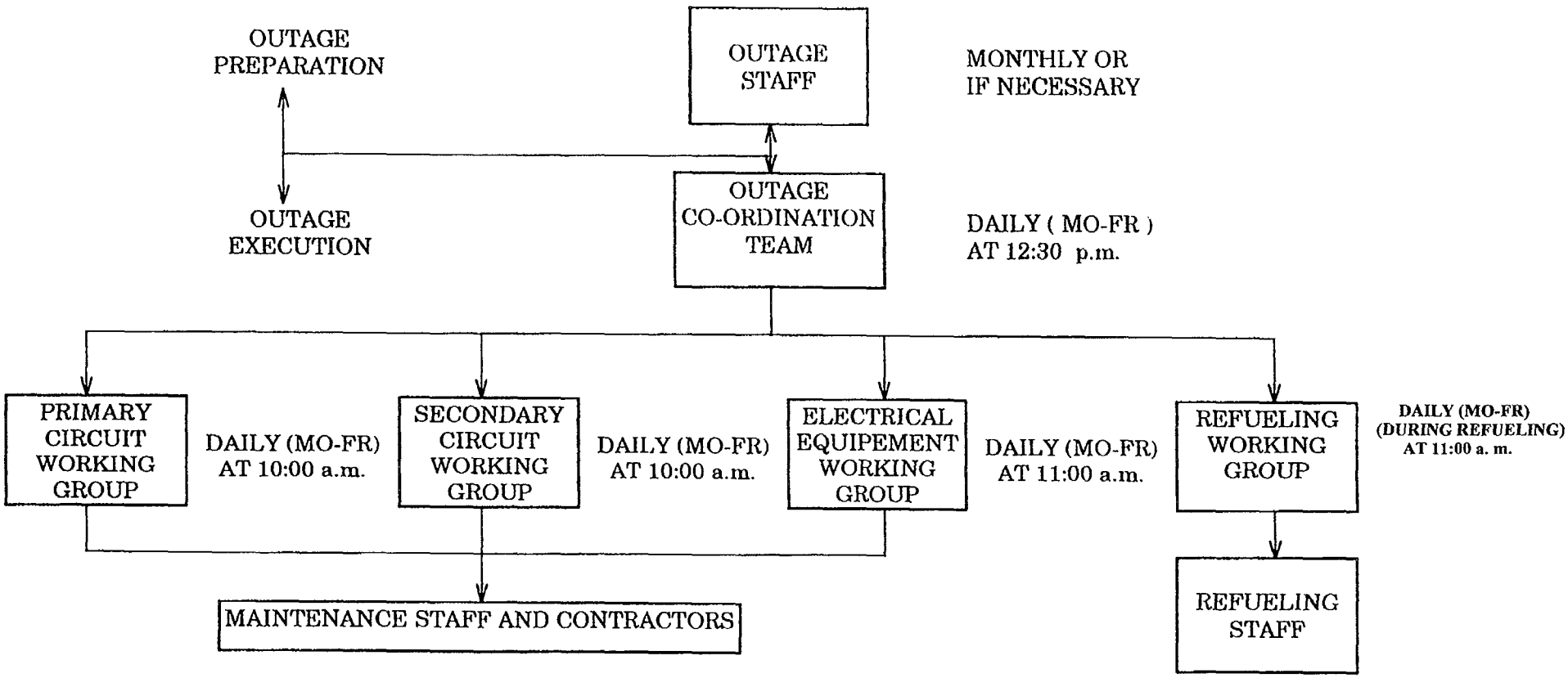


FIG 3. Bohunice outage organization.

Contribution of conceptional approach to maintenance based on long-term and short-term planning is reflected positively on plant availability. It can be demonstrated on time development of forced outages.

4. OUTAGE MANAGEMENT

Preparation, management and implementation of the outage maintenance activities are provided by the „outage staff", i.e. the establishment of temporary specific working groups in the following areas (Fig. 3):

- outage co-ordination group (outage unit operating mode control)
- primary circuit working group
- secondary circuit working group
- electrical and I&C equipment working group
- refueling working group.

All mentioned working groups are headed and supervised by the specialists from the Operation Division.

The major task of the outage staff is to provide both material and documentation preparation and co-ordination of actions requested by the equipment owners, regulatory body requests, conclusions of the safety committee and ISI evaluation conclusions. The Operation Division prepares a list of actions based on the above mentioned requests.

The outage staff meetings are held once a month, two to eight months before the outage. The meetings are held biweekly starting two months before the outage. The outage staff meetings are chaired by the head of the team appointed by plant manager. Representatives of all NPP departments who participate in the outage are the members of this outage staff (Fig. 4).

The outage co-ordination group co-ordinates all activities daily. The group meetings during the outage are held every working day. The task completion, assigned on the working group meetings, are checked and agreements on the major works are scheduled for the following days. The co-ordination group meetings are chaired by the specialist with shift supervisor experience.

During the refueling stage, the refueling working group members take part at the meetings of co-ordination working group. Works on technological equipment are directly supervised by the heads of working groups based on the approved schedules. The working group heads assign tasks to professional teams that perform the equipment maintenance.

4.1. Outage preparation

- The outage preparation starts with the outage staff opening meeting that must takes place eight months before the outage.
- Two months before the outage the basic scheduled owners requests are completed and a preliminary schedule of basic works is issued.

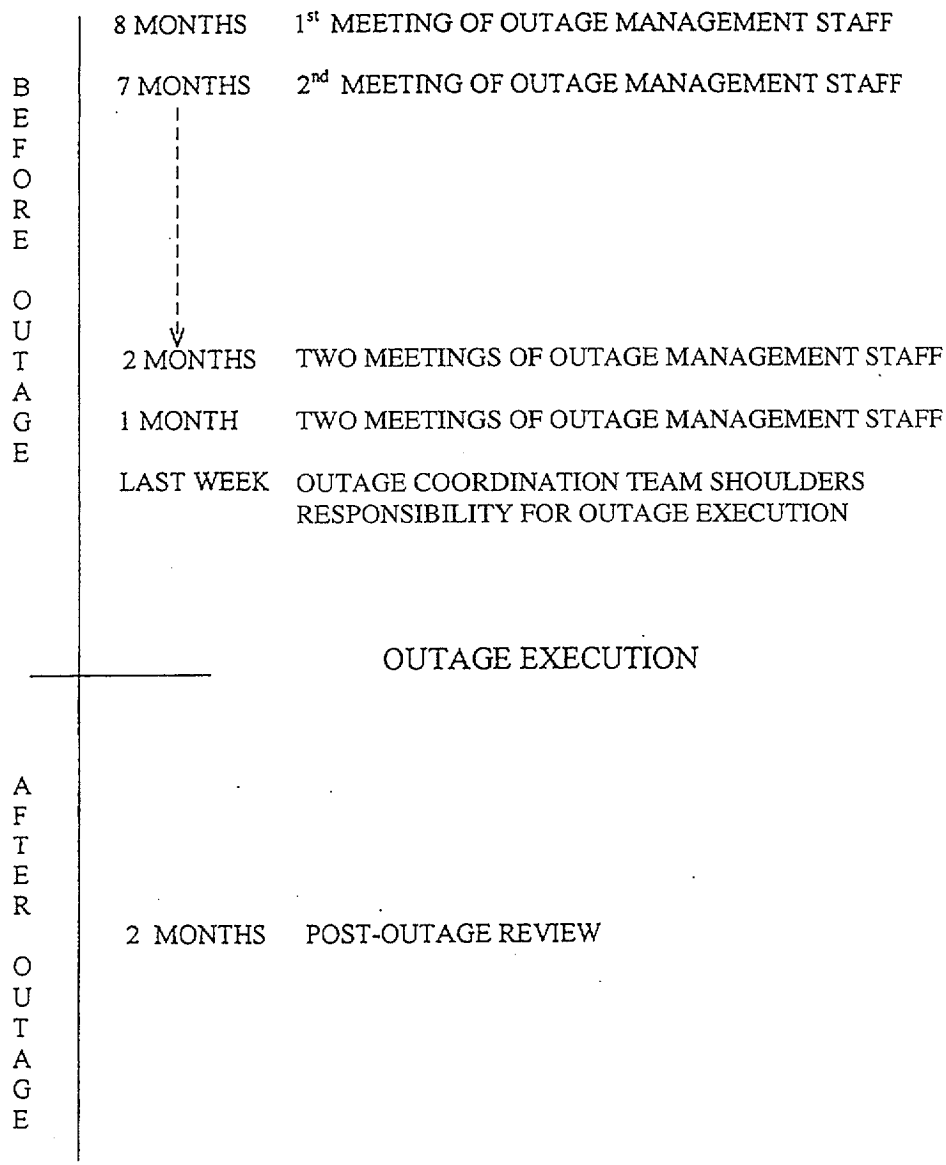


FIG. 4. Bohunice outage time schedule.

- One month before the outage work orders are issued and subsequently submitted to the maintenance implementation departments. Outage preparation is assessed on the plant management meeting.
- Three weeks before the outage the final overhaul schedules are prepared including the critical path specification.
- The works on the safety important equipment are listed and submitted to the regulatory body two weeks before the outage start.

The outage preparatory phase is completed by the approval of the records on preparedness of concerned departments. The approval takes place at a outage staff meeting.

4.2. Outage evaluation

- Ten days to the outage termination, during the equipment repair completion and revision stage, a staff meeting is held. The outage actions completion, the preparedness to the reactor heat-up, physical tests, power escalation and unit operation are recorded and records are issued by individual departments.

- After the reactor unit rated power has been achieved and stabilized, the outage staff final meeting takes place for preliminary evaluation.

- Within two weeks after the outage completion, the appointed departments submit the outage evaluation to the head of the outage staff.

- Within two months after the outage completion, the written overall outage evaluation is made by plant management.

5. DIAGNOSTICS AND MONITORING

Diagnostic and monitoring systems of primary and secondary circuits equipment have an important role to ensure reliable and safe units operation. Diagnostic and monitoring systems at V-1 and V-2 NPPs at Jaslovské Bohunice are fully comparable with the best equipped nuclear power plants in the world.

Monitoring systems provide a complex survey on status of the most important components, enable to plan maintenance or respectively directly to perform repairs of equipment in time. It also enables to determine an anomalous state of an equipment and in the case of necessity to organized shut-down of the equipment in time. In addition to that, some of the monitoring systems fulfills stringent criteria required by the „leak before break" status.

On-line monitoring are performed in the following areas:

- leakages from primary and secondary circuits
- vibrations of main components of primary circuit
- vibrations of rotating mechanical equipment
- loose parts in main components of primary circuit
- fatigue stress of most important components
- cold overpressure
- primary and secondary water chemistry
- electrical parameters of emergency power supply sources (DG).

Monitoring of equipment is continuously observed by specific plant personnel in the close cooperation with operating staff. Activities are exactly specified in operating procedures and manipulations are recorded in the operational log-books.

Another diagnostic systems or equipment are operated only during the specific maintenance periods:

- acoustic emission system
- electrical self - consumption system diagnostics (fast recording of parameters on AC and DC systems).

Leak monitoring systems are installed on primary high-energy piping systems of V-1 and V-2 NPPs. Detections are based on acoustic noise detection, humidity and radioactivity measurements in venting air from steam generator compartment. Acoustic noise measurement is also used for leak detection on steam and feedwater high energy piping. The same principle is being used for leak monitoring on high pressure ECCS pipelines and for leak monitoring on control rod driver channels on RPV head.

Vibration diagnostics is used to monitor mechanical state of RPV and SGs. Neutron noise diagnostics is used to monitor reactor internals. Main circulation pumps are continuously monitored using acceleration sensors and ultrasonic ones. Loose parts monitoring system sensors are installed on collecting places of primary circuit (10 accelerometric sensors on RPV, 6 on SGs and 6 on MCPs).

System for residual service time evaluation is installed on the primary circuit. Time dependent temperatures and pressures are recorded and evaluated after each fuel cycle. Acoustic emission system is used to monitor material defects of selected components during strength pressure tests. RPVs in the zone of nozzles, main coolant pipelines, surge lines to pressurizer and pressurizer vessels are monitored (using 159 sensors). Portable devices are used for diagnostics of vibration characteristics of rotating machines.

The events examples, recorded by diagnostic and monitoring systems, are:

- SG enclosure leakage detection from secondary side (the event is an example of cooperation of two diagnostic systems designed for leakage monitoring). A moisture raise within the SG enclosure was indicated by the diagnostic system, the acoustic system for primary circuit leakage monitoring displayed unchanged values of all the monitored primary circuit components. It was evident that primary circuit equipment was not the source of the monitored moisture raise.

- Primary circuit leakage monitoring systems play an important role among diagnostic systems. The following diagnostic indications help to prevent several events:

  I. internal leakage of the main isolation valves sealing

  II. internal leakage of the pressurizer safety valves

  III. leakage of cooling systems below the unit cap.

The above listed events were detected at the initial phase of their development and they were corrected by the in-time intervention.

- Free elements diagnostic system on V-1 NPP detected the event in 1995 when the monitoring system recorded an anomalous response at a sensor placed at the SG body. Responses were in correlation with raised level of a signal from the primary circuit leakage

monitoring acoustic system, sensor of which was also placed on the body of given SG. A specific working program was made (corresponding MCP shut down, feedwater pump shut down and feeding by the emergency pipe line). Dynamic water surges caused by discontinuous feedwater supply on feedwater control valve were the source of signals.

- Another example of complex usage of different diagnostic systems was represented by the RMS type signal raise detected by the AL S diagnostic system on a sensor placed close to MCP in 1991. The frequency analysis of this signal supplied by another supporting measurements excluded the leakage as the source of the anomalous signal and the friction process in the lower bearing area, or the well friction process in the impeller area were claimed. The MCP was shut down and two fragments of excavation disk of 2,5 x 5 x 5 mm size were found between labyrinth and casing during the overhaul.

The equipment with changing characteristics are included to the overhaul maintenance program.

5.1. Water chemistry

To monitor the water chemistry, the on-line data measuring system is installed. The following parameters are measured continually:

- hydrogen, oxygen, potassium concentrations and conductivity of primary coolant
- radioactivity of primary coolant (by gamma spectrometry)
- cation conductivity of condensate, feedwater and SG blowdown
- conductivity of condensate and feedwater
- oxygen concentrations in condensate and feedwater
- sodium and silica concentration in make-up water plant
- sodium concentration in condensate and blowdown
- boric acid concentration in primary coolant (replacement)
- conductivity of SG blowdown.

Additional monitors are planned to be installed during the gradual upgrading program of V-1 NPP.

6. INSPECTION TECHNOLOGIES

The systems and components are periodically examined and monitored according to ISI program. This program includes non-destructive testing methods: ultrasonic tests, X-ray tests, magnetic particle tests, eddy current tests, dye-penetrate tests, leak rate tests and visual tests. Wall thickness monitoring in selected locations is included in the ultrasonic and eddy current tests. The program also includes tests of steam generators and pressurizer safety valves.

ISI are required by the technical specifications approved by the regulatory body of the Slovak Republic. ISI program covers scope, type of inspection and periodicity. Equipment

modifications are incorporated in the ISI program using the modification sheets in the course of time. Both the ISI programs and modification sheets must be approved by regulatory body.

In-service inspection results are evaluated in order to judge whether the equipment is acceptable or whether remedial measures are necessary to ensure continued safe and reliable operation of the plant. The final review of ISI results is performed by a specific committee after outage. The experts from research institutes, manufacturers of main components equipment and the regulatory body inspectors are part of the committee.

The NPP specialists are continually up-dated with the latest developments in the area of non-destructive testing; ultrasonic and eddy currents testing in particular. Also new testing techniques of austenitic materials and welds and methods of data processing are followed. Robotic testing of austenitic welds in the primary circuit and pressurizer pipelines was introduced by means of the P-SCAN device. Those inspections are made in co-operation with RTD Company (Netherlands).

The group was established in 1994 for the mechanized ultrasonic testing of NPP primary circuit austenitic welds and has executed more than 300 weld tests on main primary piping, the pressurizer pipe welds, welds of reactor nozzles and the circumferential welds of reactor in the nozzles area.

The group tested the primary welds in the NPP Loviisa, Finland too.

The steam generators are tested by manipulator ZOK PG 01 developed and manufactured by Nuclear Power Plant Research Institute Trnava (VÚJE). Remotely controlled operations for testing, diagnostic and tubes plugging are made by this equipment.

Heat exchanging tubing and internal surface of collector are tested by eddy current method. Data collection and measured data analysis are performed by the system MIZ-18 (USA - Zetec). Material of the collector s internal surface and welded connections of the collector are tested by the ultrasonic method. Data collection and measured data analysis are performed by the system UIS (Canada).

Reactor pressure vessel inspections are made by Reactortest Company with maintenance division cooperation SIEMENS. ZMM 5 manipulator and instrumentation is used for that purpose.

Electrical equipment diagnostic is primarily performed to gathering of sufficient necessary information on its technical conditions and to avoid the failures. Secondarily, this implies to decrease the labor and reduce the costs for the electrical equipment maintenance. The following measurements are provided:

- measurement of insulation resistance versus time and polarization index determination
- HV test of equipment
- measurement of charging current versus time and voltage
- measurement of capacity and loss factor versus voltage
- measurement of partial discharges in the insulation system

- measurement of ohmic resistance of the equipment winding
- measurement of magnetization currents
- measurement of hour angle and transmission
- measurement of power and technological equipment with thermal camera.

The measurements are analyzed and compared with measurement of the previous years. All measurements are reported and the recommendations for further equipment operation are issued.

7. BACKFITTING PROGRAM

The early WWERs have been designed in a very conservative manner, with large inventories in the primary circuit and also the secondary circuit. These reactors have been shown, for instance to be able to withstand several hours of station blackout without serious consequences. Heat production is low with respect to the fuel weight, and the plant parameters, with large margins between the operating conditions and limits, provide great flexibility in coping with operational transients. The safety concept was based on the design rules and standards at the time of design and construction in the former USSR. The reactor pressure vessel was made of cylindrically forged ferritin steel. The primary circuit was manufactured using forged parts, with the exception of the cast austenitic pump and the main gate valve. The primary piping was made exclusively from austenitic stainless steel.

7.1. V-1 Bohunice NPP

No regulatory requirement in the former Czechoslovakia and no IAEA NUSS codes and guides existed at the time of V-1 design. The design of the secondary circuit was made in Czechoslovakia and some safety features were already included in the design, like superemergency feedwater system.

Over the years, changes of plant and safety systems have been carried out to enhance the safety and operational reliability. About 500 design changes were made up to 1985 (about 1000 up to 1996). Usually, the reasons for these changes were operating experience, occurrence of events and their corrections, or new standards and rules.

In 1985, the first program for safety enhancement was prepared. The main concern of this program was reactor pressure vessel embrittlement. In 1986, a comprehensive program was established for safety enhancement, including seismic upgrading.

Since 1989 several safety missions to the Bohunice NPP V-1 have been arranged to investigate the current status and to look for deficiencies of the plant. Safety missions were carried out by experts from Czechoslovakia, group of Austrian experts and group of SIEMENS experts, as well as by the IAEA (OSART, ASSET and safety review missions).

On the basis of conclusions and recommendations of safety reassessment the former Czechoslovak Nuclear Regulatory Commission (CSKAE) set 81 short term backfitting measures (Decision 5/1991). This decision was completed by setting 14 additional measures (CSKAE Decision 213/1992).

The technical content of Decisions 5/1991 and 213/1992 (for the so-called small reconstruction of V-1) includes the following items:

- material analysis and annealing of the reactor pressure vessels
- status of the leak before break concept
- diagnostic systems monitoring the vital equipment and systems
- seismic upgrading
- safety systems and confinement upgrading
- fire protection upgrading
- enhancement of reliability and of safety related systems and equipment (instrumentation and control system, super-emergency feedwater system)
- emergency planning
- radiation monitoring of the NPP and in the plant vicinity.

In 1993, the small reconstruction of the Bohunice NPP V-1, covering the above measures, was completed this has increased the plant safety compared with the original design.

The main results of the small reconstruction are:

- leak before break concept: the probability of a piping rupture exceeding
- 100 mm in diameter is less than 10^{-6} per year per unit three independent leak detection systems have been installed
- more precise analyses of the chemical composition of welds and base material of reactor pressure vessels and their regenerative annealing
- seismic upgrading to level 8, scale MSK 64
- Increase of the emergency core cooling system (ECCS) and the spray capacity and separation
- increase of the tightness of the confinement (40 times)
- increase of fire protection (reduction of the contribution to core damage frequency from 30 to 2% according to the level 1 probabilistic safety assessment before and after the small reconstruction)
- increase of the safety and reliability of the reactor protection systems and installation of emergency control panels
- increase of the safety, reliability and capacity of the emergency electrical supply system (two independent systems per unit)
- installation of diagnostic systems

- installation of main steam line isolation valves
- performance of level 1 PSA.

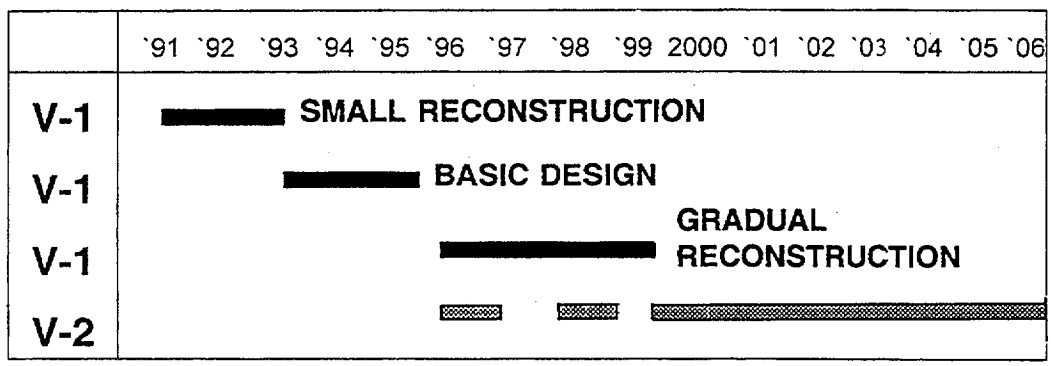
In February 1994, Nuclear Regulatory Authority of the Slovak Republic issued Decision 1/1994, including a number of safety measures which should bring plant safety to an internationally accepted level. Unlike in the small reconstruction, the intended safety upgrading will address plant design more deeply. A LOCA (200 mm) was considered as the new design basis accident (DBA). Comprehensive requalification of the safety related equipment and the ECCS, as well as improvement of the confinement leaktightness and the auxiliary systems (essential service water, instrumentation and control, electrical systems, fire protection) will be carried out.

Decision 1/1994 approved the preliminary safety analysis report „Gradual Upgrading of the V-1 Plant" and laid down the Nuclear Regulatory Authority of the Slovak Republic requirements for further operation (annual licensing) and the technical requirements. The technical requirements are aimed at achieving the following safety features:

- primary circuit integrity
- core cooling in operating and transient conditions
- improvement of the confinement safety function
- improvement of the supporting systems (service water, emergency power supply, instrumentation and control, fire protection)
- seismic reinforcement.

It is planned to implement all backfitting measures during plant outages in the period 1995-1999 (Fig. 5).

In view of the importance and scope of V-1 reconstruction, Bohunice NPP issued a tender for the preparation of guidelines for basic engineering. On 5 May 1994, a contract with SIEMENS



Schedule derived on:

- Existence of two different plant designs at Bohunice site
- Uniform future investments distribution

FIG. 5. Bohunice NPP's upgrading program schedule.

AG KWU for basic engineering was signed. For the implementation of gradual reconstruction, the REKON consortium was established in November 1995, consisting of two partners, the German SIEMENS AG KWU and the Slovak VÚJE Trnava Plc. In April 1996, a contract between the Slovak Power Plants SE, AS, and REKON for implementation of gradual reconstruction was signed. The goal of the consortium is to combine the know-how of the western nuclear power industry with the possibilities and experience of the Slovak or Czech suppliers.

The basic safety goals of safety upgrading will be implemented through the following measures:

- modification of pressurizer safety valves
- addition of steam dump stations on the main steam lines
- modification of the steam generator super-emergency feedwater system
- modification of the Madunice hydropower plant - establishment of the power supply source No. 3
- modification of the ECCS
- completion of the fire protection systems
- modification of the power supply systems, accounting for measures for separation of redundancies in essential and vital supplies
- modification of the instrumentation and control systems
- modification of the confinement spray systems
- establishment of a new confinement system for mitigating the consequences of BDBAs
- improvement of confinement integrity
- upgrading of the confinement strength
- establishment of a new filtered venting system
- completion of the modification of essential service water systems
- modification of heating, ventilation, air conditioning and cooling systems (HVAC)
- enhancement of the seismic resistance of safety relevant parts of equipment.

7.2. V-2 Bohunice NPP

V-2 NPP is equipped with 2 reactors WWER 440/V213, which are in operation since 1984 and 1985 respectively and with 30 years of the design lifetime they should be in operation till 2014 and 2015 respectively. Good operational results and favorable status of main components already lead to considerations to extend lifetime of V-2 units to about 40 years approximately. There is also certain potential to increase power of the reactor units by about 5-10 %.

Due to substantially more safety advanced design in comparison with old V230 units, V-2 units are much less controversial and do not require such large extent of design modifications.

Nevertheless, some significant design improvements have been implemented since 1990, mostly devoted to installation of in-service diagnostic systems, leak before break status, innovation of instrumentation and control system, replacement of electrical breakers, DC batteries, electrical protections, electrical penetrations, fire protection improvement, antiseismic upgrading, etc. Large effort is also devoted to elaboration of new symptom based emergency operating procedures.

Based on regulatory requirements, the up-dated safety report after 10 years of operation has been elaborated by the utility in 1995. Regulatory assessment of this report has been completed and the results lead to Decision No. 4/1996 on further operation of V-2 NPP. Decision includes 51 safety relevant conditions subdivided into 3 groups:

- improvements and completion of the safety report itself (1996-1998)
- safety upgrading measures short-term measures are already listed specifically, for long-term program detail elaboration it is required by the decision
- extension of the safety report to the format required for periodical safety review till 1997.

Comprehensive programme for V-2 NPP is under preparation. The deterministic and probabilistic goals were established.

The future development of backfitting program for V-2 NPP is based on priorities according to the following documents:

- Regulatory Decision No. 4/1996
- IAEA report EBP WWER 03/96
- V-2 NPP Safety Analysis Report, including PSA recommendations
- Operating utility own experience
- Investment program.

The V-2 NPP safety enhancement program consists of four stages:

1st stage 1984-1996 - implementation of urgent measures and periodic safety assessment

2nd stage 1996-1997 - priority evaluation, design preparation, implementation of urgent measures

3rd stage 1999-2006 - modernization and safety enhancement of V-2 NPP including increase power

4th stage 2006-2015 - life time extension.

8. CONCLUSION

Contrary to the activities aimed at improving availability and load factors, the safety enhancement program decrease units load and availability factors. Also operation of V-2 NPP in a permanent „Load - follow" operating mode in the power range 96 4% N_{NOM} for national grid frequency control, and the use of low-energy steam from turbine extractions for remote district heating additionally decrease the electricity production and units load factors (Fig. 6, 7).

Availability Factor
[%]

Year	Unit 1	Unit 2
1990	84.9	79.2
1991	85.7	76.2
1992	69.7	77.1
1993	68.7	62.0
1994	87.2	89.9
1995	86.8	85.6
1996	81.7	76.2

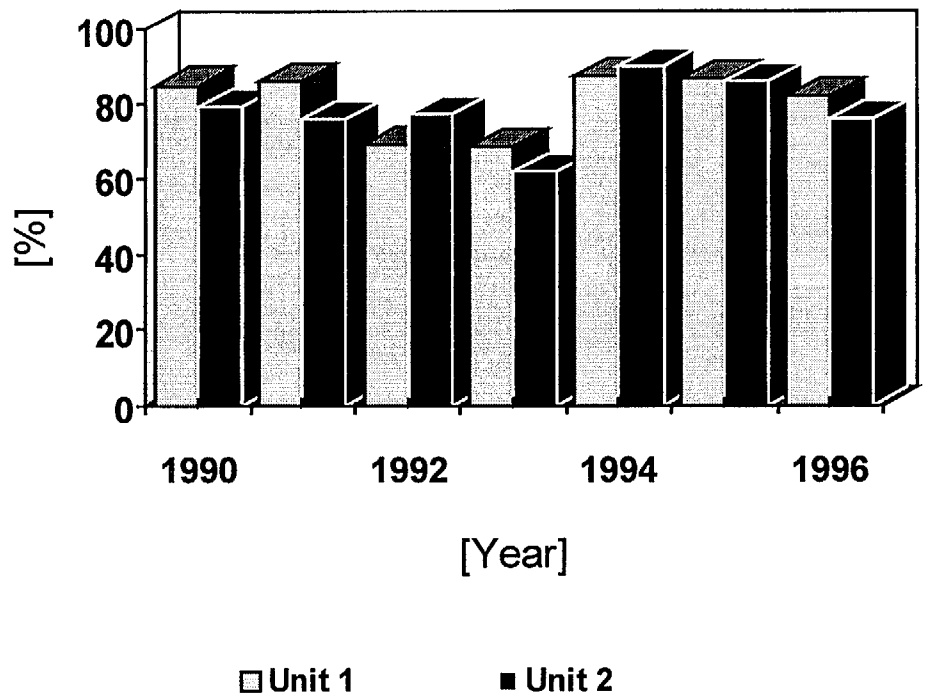


FIG. 6. Avalability factor EBO V-1.

Availability Factor
[%]

Year	Unit 1	Unit 2
1990	84.2	84.8
1991	76.7	84.9
1992	85.6	76.4
1993	88.1	83.8
1994	84.6	84.3
1995	77.5	87.7
1996	85.9	79.6

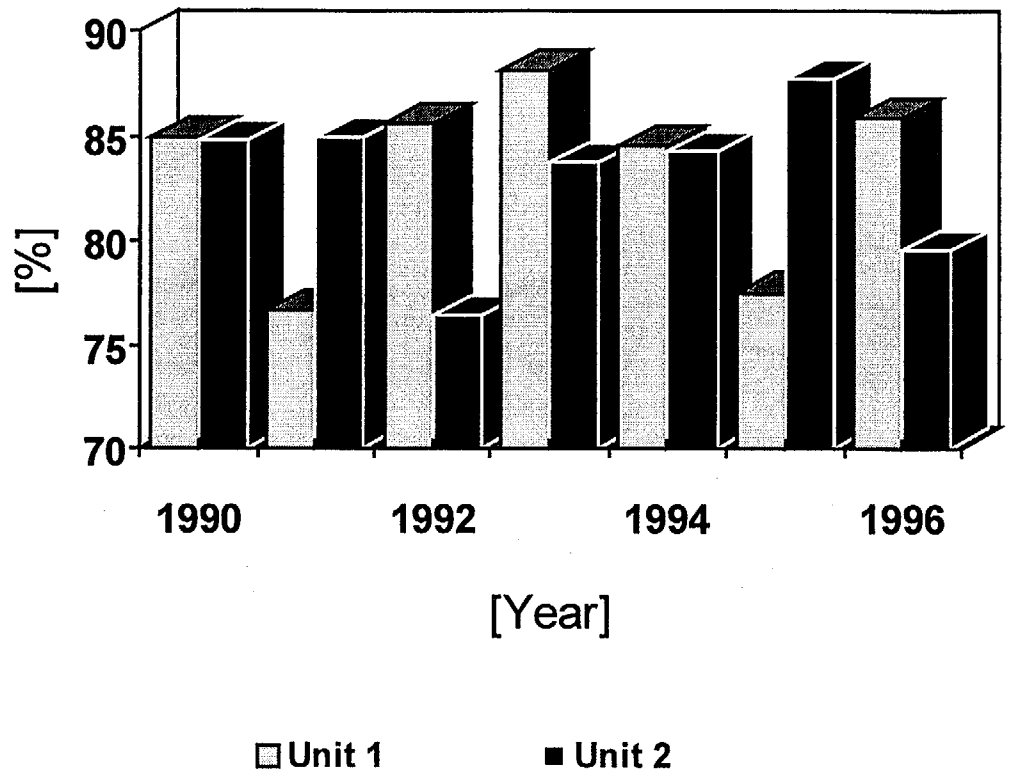


FIG. 7. Avalability factor EBO V-2.

Year	UCLF EBO [%]
1990	3.92
1991	2.55
1992	1.70
1993	2.86
1994	2.37
1995	1.66
1996	1.42
1997	1.28

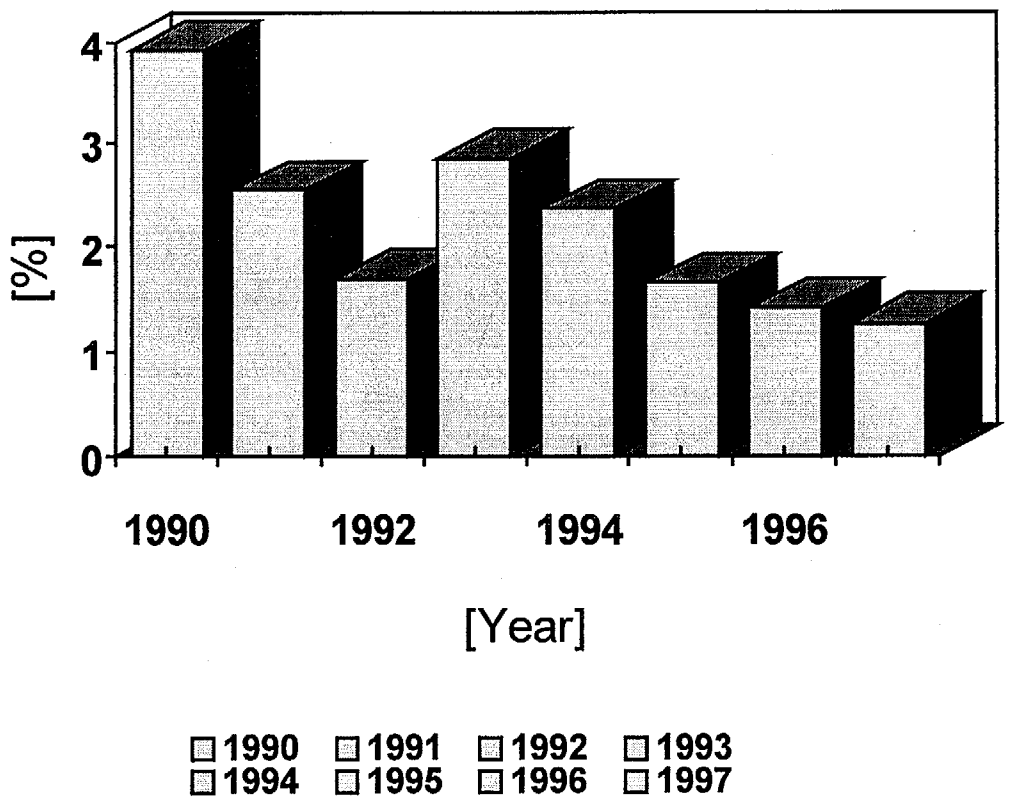


FIG. 8. Unit capability loss factor EBO

This can be seen in the pictures where history of annual availability are given. In case of V-1 NPP there is remarkable decrease of availability in period 1991-93 when the first stage of unit safety improvements were implemented and also another period since 1995 when second phase of gradual safety enhancement continued.

On the other hand, very serious attempt is made by the plant management and plant personnel to compensate decreasing plant availability factors by the increasing reliability and by decreasing the forced losses of electricity production. Recent achievements of decreasing this indicator can be seen on the figure 8.

NEXT PAGE(S)
left BLANK

RECENT ADVANCES IN TECHNOLOGIES FOR IMPROVING AVAILABILITY AND RELIABILITY

(Session 3)

Chairman

P. ALLEN
Canada

NEXT PAGE(S) left BLANK

XA9848575

PROTOTYPE EQUIPMENT STATUS MONITOR FOR PLANT OPERATIONAL CONFIGURATION MANAGEMENT

M. DeVERNO*, S. GROOM**, D. TRASK*

*Atomic Energy of Canada Limited,
Centre for New Energy Research,
University of New Brunswick,
Fredericton, New Brunswick

**New Brunswick Power,
Point Lepreau Generating Station,
Lepreau, New Brunswick

Canada

Abstract

CANDU plants, such as the Point Lepreau GS, have tens of thousands of operable devices. The status of each operable device must be immediately available to plan and execute future changes to the plant. Historically, changes to the plant's operational configuration have been controlled using manual and administrative methods where the status of each operable device is maintained on operational flowsheets located in the work control area of the main control room. The operational flowsheets are used to plan and develop Operating Orders (OOs) or Orders-to-Operate (OTOs) and the control centre work processes are used to manage their execution. After performing each OO procedure, the operational flowsheets are updated to reflect the new plant configuration. This process can be very time consuming, and due to the manual processes, can lead to the potential for time lags and errors in the recording of the current plant configuration. Through a cooperative research and development program, Canadian CANDU utilities and Atomic Energy of Canada Limited, the design organization, have applied modern information technologies to develop a prototype Equipment Status Monitor (ESM) to address processes and information flow for efficient operational configuration management. The ESM integrates electronic operational flowsheets, equipment databases, engineering and work management systems, and computerized procedures to assess, plan, execute, track, and record changes to the plant's operational configuration. This directly leads to improved change control, more timely and accurate plant status information, fewer errors, and better decision making regarding future changes. These improvements to managing the plant's operational configuration are essential to increasing plant safety, achieving a high plant availability, and maintaining high capability and capacity factors.

INTRODUCTION

Successful management of the plant operational configuration is a key component of station operations and is essential to enhancing safety, achieving a high plant availability, and maintaining a high plant capacity factor. CANDU[1] nuclear plants, such as the Point Lepreau GS, include tens of thousands of manually operated devices besides those operated through automated control and reactor protection systems. Multi-unit CANDU stations may have up to 160,000 operable devices. The operation of these devices on a daily basis requires strict controls and procedures to ensure safety, procedural compliance, and to provide correct up-to-date status information for future decision making. Efficient yet comprehensive work

[1] CANadian Deuterium Uranium

processes and information flow are needed to plan, execute, track, and record changes to the plant configuration and an up-to-date status of each operable device must be available to plan and execute future operational activities.

Historically, these activities are controlled using a combination of manual and administrative methods centered around the use of operational flowsheets and Operating Orders (OOs) or Orders-to-Operate (OTO)[2] procedures. Operational flowsheets, located in the work control area of the main control room, use coloured pins, dots, labels, and other markups to indicate the current operational status. This includes device and equipment status, jumpers, and work protection tags. As many as 200 operational flowsheets may exist for a single unit, and collectively are referred to as the plant operational 'pinboard'. When operational changes to manual devices are needed, the operational flowsheets are used to plan and develop OOs and the control centre work processes are used to manage their execution. The planning process must include the assessment of current device status, work protection, temporary jumpers, maintenance records, and other operations ongoing at the time. After developing, reviewing, and approving the OO, the work activity is authorized. During execution of the OO, the operator must sign-off each step as it is completed. Upon completion of the OO, the pinboard (operational flowsheets) is updated as required to reflect the new plant configuration and the paperwork (OO and related information) is filed in the work permit area and the records department. Overall, this process can be very time consuming, and due to the manual processes, can lead to the potential for time lags and errors in the recording of the current plant configuration.

Improvements to plant configuration management can have beneficial effects throughout the entire plant infrastructure. This has been the driving force behind programs to augment the manually intensive processes with computerized systems. The first such program in the Canadian CANDU industry was the development of the Equipment Status Monitor (ESM) [1] by Ontario Hydro for use at its Darlington NGS. The ESM replaced the traditional processes with a computerized system that facilitated the generation of OOs, maintained the status of all manually operated devices using electronic flow sheets, and included provisions for facilitating the field operation using electronic equipment verification. The intent of the system was to track the state of all manually operated devices, reduce the chance of operator error, and provide up-to-date device status to station staff. However, technological limitations imposed by the hardware and software available at the time limited the overall effectiveness of the Darlington ESM.

Subsequently, there have been many technological advances in the use of hand-held tablet computers, Computer Aided Design and Development (CADD) systems, electronic equipment identification and verification, and hypertext technologies. These technologies can facilitate the design and development of a low-cost ESM system offering improvements to the original concept. As a result, through a cooperative research and development program, Canadian CANDU utilities and Atomic Energy of Canada Limited (AECL), the design

---

[2] OTOs and OOs are the same. OTO is Ontario Hydro terminology whereas OO is used in NB Power.

organization, have applied modern information technologies to develop a new next generation ESM prototype to address the processes and information flow for efficient operational configuration management. The ESM integrates electronic operational flowsheets, equipment databases, engineering and work management systems, and computerized procedures to assess, plan, execute, track, and record changes to the plant's operational configuration. This paper presents an overview of the prototype ESM system including its operational context, high level system functional requirements, prototype design description, and benefits of the ESM towards improving plant availability, capacity factors, and safety while lowering the overall operations, maintenance, and administration costs.

OPERATIONAL CONTEXT OF THE GENERIC ESM SYSTEM

Station staff must have an accurate understanding of the current operational state of all plant systems and devices, as well as an accurate picture of the reliability and availability of all devices should changes to the operating state of the plant be required. The operational state of the plant is influenced by maintenance activities and changes to the plant design. Similarly, feedback on the operability and reliability of plant equipment provides critical input to the design and maintenance processes. It is thereby recognized that the process of managing the plant's operational configuration impacts virtually all functional groups within the station. Having correct, up-to-date plant status information ensures that optimal decisions are made and acted upon. Fewer mistakes occur, plant safety and reliability are enhanced, and higher plant availability and capacity factors follow. The operational context of the generic ESM system is shown diagrammatically in Fig.1.

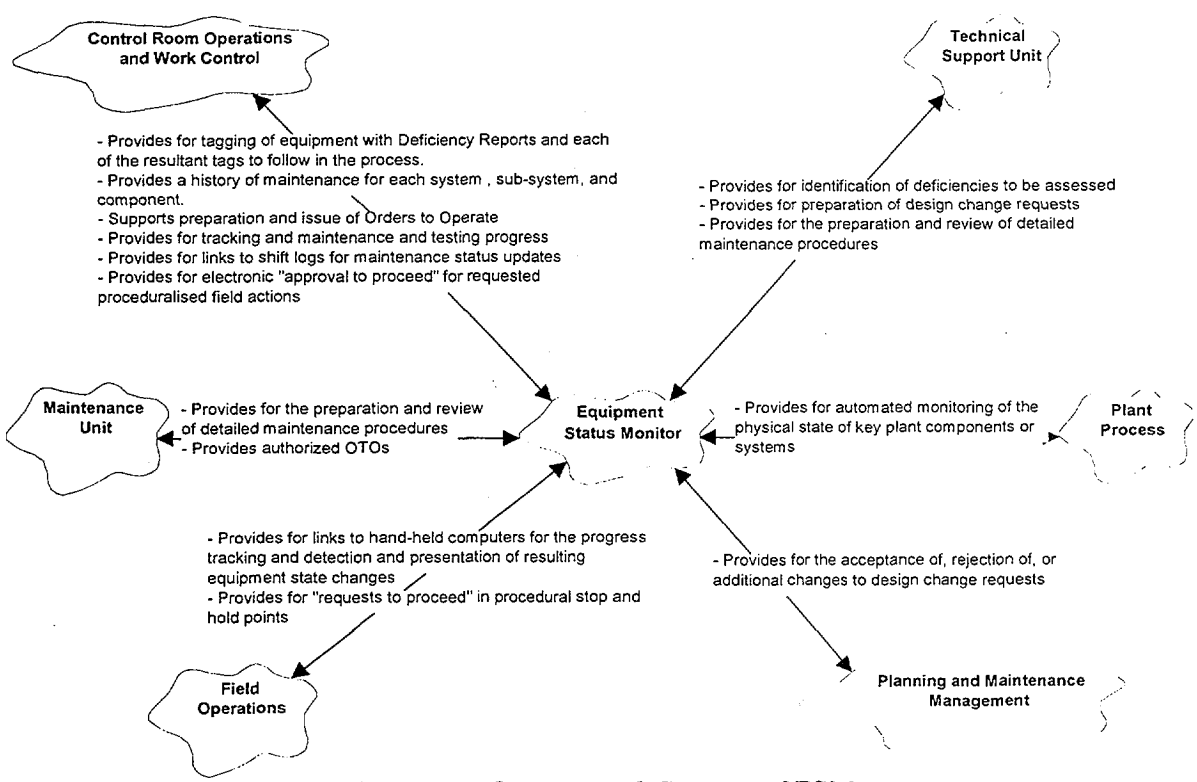


Figure 1: Operational Context of ESM.

HIGH-LEVEL ESM FUNCTIONAL REQUIREMENTS

Managing the plant's operational configuration requires the integration of design, maintenance, and operational information into an end-product that in itself is maintainable and manageable. The resulting system must provide process improvements, higher efficiency and effectiveness over the currently used manual processes. In addition, the system must successfully integrate with other plant data systems [2,3] supporting operations, technical support, maintenance, and administration.

At the core of the ESM is equipment status. Each operable device in the plant has an associated status, which may be unique to the class of component. For instance, a pump may be 'On' or 'Off', and a valve may be 'Open' or 'Closed'. The ESM system must be able to manage and maintain the creation, revision, and updating of all device types and status information associated with each operable device in the plant. This includes adding/deleting devices, changing the status of any device, and presenting this information to the user through simple operator interfaces.

A key component of the ESM is the presentation and ongoing management of plant operational flowsheets. Each flowsheet is a representation of a Process and Instrumentation Diagram (P&ID) where detailed design information not pertinent to operations has been removed and other information added to facilitate the operational processes. The ESM must be capable of maintaining electronic operational flowsheets including the implementation of revision control procedures. The ESM must be capable of retrieving and displaying any flowsheet with the current device status, work protection tag information, and up-to-date jumper records. Standard viewing functions such as panning and zooming must be available, and the system must provide hard copy prints.

Temporary changes to the plant are documented in the form of jumper records. Traditionally, jumper records are hand-drawn on the operational flowsheets held within the control centre's work control area. The ESM must be capable of accessing or incorporating a jumper record database and include mechanisms to display jumper record information. In addition, the ESM must be able to display jumper information on the operational flow sheets and include tools to update the jumper records and flowsheets under administrative control.

Work protection tags are labels that are placed on field devices to ensure work safety and protection, and to ensure that the condition of the device is guaranteed and maintained. Tags of different names and colours are typically used within the plant in accordance with the station policies and work procedures. The ESM must include mechanisms to manage the definition and application of work protection tags. This requires a work protection tag database and processes compliant with station work protection procedures. This activity is especially important during the generation and execution of OOs where work safety is potentially at risk. The ESM must be capable of accessing, viewing, and updating work protection tag information.

The maintenance histories of the plant components and associated deficiency reports are important to ongoing plant operations, the preparation of OOs, and other work processes. The ESM must include interfaces to the Work Management System to access maintenance histories and deficiency reports pertaining to all operable devices.

The ability to prepare, execute, and track OOs is a fundamental ESM requirement. The ESM must be capable of managing the initiation, creation, field execution, and completion of all OOs. Mechanisms to create and modify OOs include the revision of previously generated OOs, the use of 'point-and-click' methods using the operational flowsheets in conjunction with 'pick lists' or 'pull-down menus' of appropriate actions, or through combinations of these two mechanisms. During the creation of an OO, the ESM must be capable of displaying all relevant information from the operational flowsheets, jumper records, work protection, maintenance histories, and deficiency reports as may be required to research and complete the OO procedure. The ESM must also include facilities to manage the OO work flow in compliance with station policies and procedures. For OO execution, the ESM must include the use of a hand-held computerized procedure system. The system must include all of the necessary communication interfaces, embed and enforce the approved procedural work flow, facilitate equipment identification, handle shift turnovers, and generate time-stamped logs of the operator activities and events. Successful completion of the OO must result in the updating of the plant configuration maintained by the ESM databases and operational flowsheets.

Authorization, security, and database management must be built-in features of the ESM in order to ensure compliance with station policies and procedures, and to ensure that information within the ESM is not in any way altered without the appropriate permits. The ESM must include security measures to limit system use and OO authorizations to approved personnel in accordance with station policies and procedures. Since the ESM will contain a significant amount of information within its own database, as well as have access to other plant information systems, it is necessary to implement appropriate database management practices in order to ensure system integrity and longevity. The ESM must include mechanisms to maintain the equipment lists and operational flowsheets in compliance with the engineering and CADD systems, and to maintain the other ESM database components as necessary.

The ESM is envisaged to be the focal point of a large amount of plant data. However, it is not expected that the ESM becomes the repository of all of the information, but rather is able to query other database systems and display the appropriate information to the user. Therefore, the ESM must include the appropriate interfaces to the engineering and CADD design databases, drawings, and models. Interfaces to the plant work management system are also required for the retrieval of work histories and deficiency reports, maintenance plans, work-in-progress reports, and other such information that may be pertinent to the preparation of OOs and the monitoring of the plant equipment status. Furthermore, interfaces to plant historical databases and other process systems are needed for the automated retrieval of information associated with automated devices within the plant.

ESM DESIGN OVERVIEW

The advent of new computer hardware and software technologies has created opportunities for improving the work processes within nuclear power stations. This has been most prominent in the areas of information technologies where small, powerful, hand-held computers that resemble writing tablets, and object-orientated software tools allow the development of operational support systems well beyond the expectations of only a few years ago. These tools have been incorporated into a prototype ESM system to support the preparation, execution, and tracking of operating orders and the management of the plant's operational configuration.

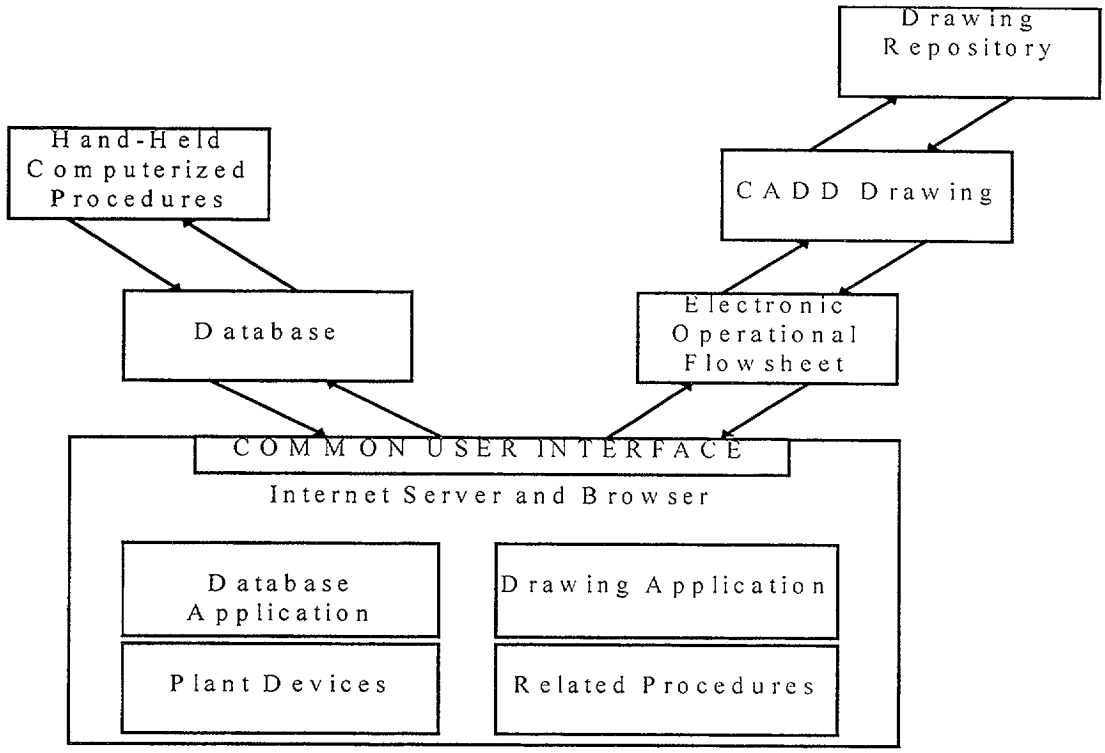


Figure 2: ESM Concept Block Diagram.

The ESM concept design incorporates a number of basic components and information flows as shown in Figure 2. The equipment database provides up-to-date equipment and system status information with cross-references to related procedures and drawings. An electronic drawing system is used to support the creation and display of electronic operational flowsheets, equipment status, jumpers, and work protection tag information. The object-orientated electronic drawing system supports programmable drawing objects that can be rendered using different colours or other attributes to indicate equipment status as extracted from the database, thereby mimicking the manual pinboard. Hand-held computer technology is used to support procedure execution. The hand-held computer technology also supports data collection and incorporates features to ensure procedural compliance and field safety. Lastly, a common user interface is utilized which is capable of supporting drawings, database queries, object linking and embedding, and external interfaces.

An important aspect of the ESM design concept is that the presentation of data and the integration of the database and drawing system components lends itself quite readily to current Internet technology. This technology provides standard interfaces supported by all major drawing system corporations, such as AutoCAD and Intergraph, and database solutions using current standards such as ODBC (Open Data Base Connectivity) and SQL (Standard Query Language). In addition, this methodology can support links to many other relational database systems including historical data systems such as PI-3 (OSI Inc.), condition based maintenance systems such as MAINSTAY (GasTops Inc.), and work management systems such as Indus Passport (Indus Group Inc.) and SAP (SAP GA). This ensures that the ESM can be fully integrated with other plant data systems supporting technical surveillance and analysis, maintenance management, and work management.

ESM DESIGN AND OPERATION

To facilitate system maintenance and a cost-effective implementation process, the ESM prototype design incorporates of a number of third-party off-the-shelf products including:

- an ESM database centered around the use of Microsoft Access,
- the use of InterCap Graphic Systems ActiveCGM as the ESM interactive drawing tool supporting electronic flowsheets,
- standard Microsoft Internet browser technology (NT Internet Server, Microsoft Internet Explorer, and Front Page HyperText Markup Language (HTML) Editor) to serve as the medium to integrate and exchange data between the other ESM components, and
- a hand-held computerized procedure system developed by AECL to facilitate the field execution of operating orders and other procedures.

The ESM uses an ODBC compliant database designed around the need to gather, present, report, and query information specific to the plant operational devices. Each device can be uniquely identified by a device name and associated with engineering documentation, CADD drawings, work procedures, work orders and work permits, work schedules, historical and real-time data, and other data. The database design is best illustrated in Figure 3 where the

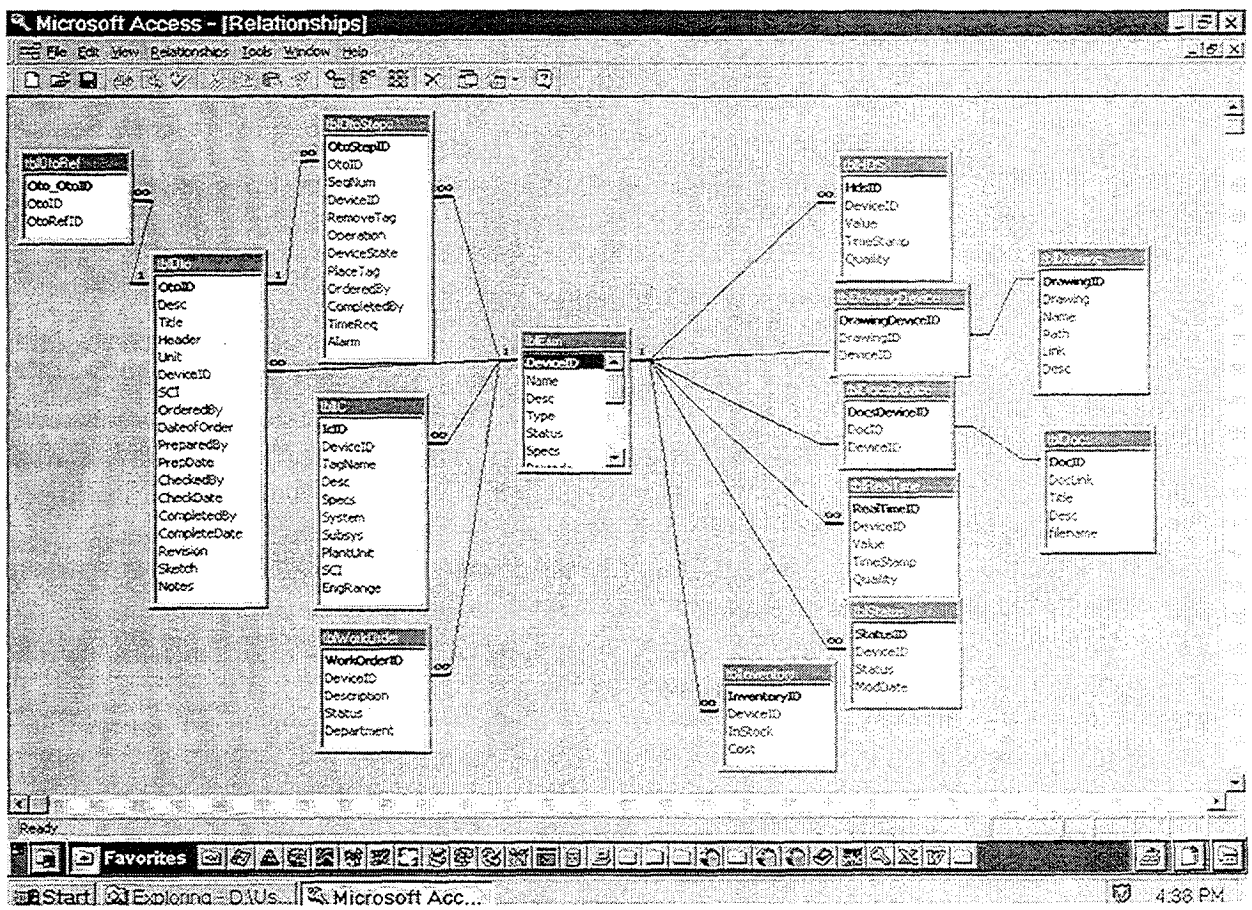


Figure 3: ESM Prototype Database Design and Relationships.

relationships between the unique device identifiers (DeviceID) and the other database components are shown. Each one to 'infinity' symbol represents a one-to-many relationship that allows a single DeviceID to be used in an 'infinite' number of OOs. Although each of the database tables are shown as part of the ESM database design, they could just as easily reside in other databases linked to the ESM through ODBC interfaces.

The drawing component of the ESM prototype provides the ability to dynamically interconnect the database and user interface through the association of drawing objects and equipment names. To achieve this both an authoring process and a display process were used. The authoring process allows drawings and their internal objects (equipment symbols) to be configured to provide interactive and animated behaviors while the display process executes the rendering, interaction, and animation of the drawing objects. The ActiveCGM product provides this functionality with its authoring tool for configuring drawing objects, and its embedded ActiveX component for displaying active drawings, interacting with users and external data. The configuration is, in fact, completed through 'point-and-click' operations using the ActiveCGM authoring interfaces.

Each of the tools previously described (Microsoft Access and ActiveCGM) have their own user interfaces and displays. However, the ESM relies on the integration and connectivity of a number of components, and therefore, these tools were integrated into a single operator interface through the use of an Internet browser based on standard Microsoft products such as NT Workstation Peer Web Server, Internet Explorer 3.01 and Front Page HTML Editor. These tools provided the data transfer mechanism between the user, ActiveCGM, and the ODBC-enabled database. The Internet server/browser tools were used to create 5 interactive HTML pages, each providing an interface to a component of the ESM. The first page serves as a container for the other four, and therefore, is transparent to the operator. The remaining four pages comprise the visible operator interface, as shown in Figure 4.

The user can individually size each of the four HTML frames. For example, if the drawing is the primary object of interest, the user can click and drag the frame separators to re-size the window.

The upper left frame is constructed from three ODBC database queries that are executed when equipment is selected on the drawing in the upper right frame, or by selecting a device name in the lower left frame. The first query captures the ESM related data, including the tag name, description, current state, latest work order and tagging information. The colour of the 'Current State' entry is dynamic depending on the current equipment status, with 'Closed' displayed in green and 'Open' in red. In a production ESM system, much more information would be included such as additional condition-based colour and text. The second query in this frame displays an active list of all drawings associated with the selected device including electrical and instrument air systems that may be used to drive the device. If a database does not already exist with these relationships, one could easily be generated using the CADD tools available at the plants. Clicking on the drawing title causes the drawing to appear in the upper right frame, and the lower left frame is refreshed to show all devices in the current drawing. The third query in the frame displays all associated procedures that reference the selected device. This may include references to other OOs (current or historic) or may extend to any category of plant procedure. For all electronic documentation, a simple search routine can be used to build this set of relationships. Selecting the document title displays the document in the lower right frame.

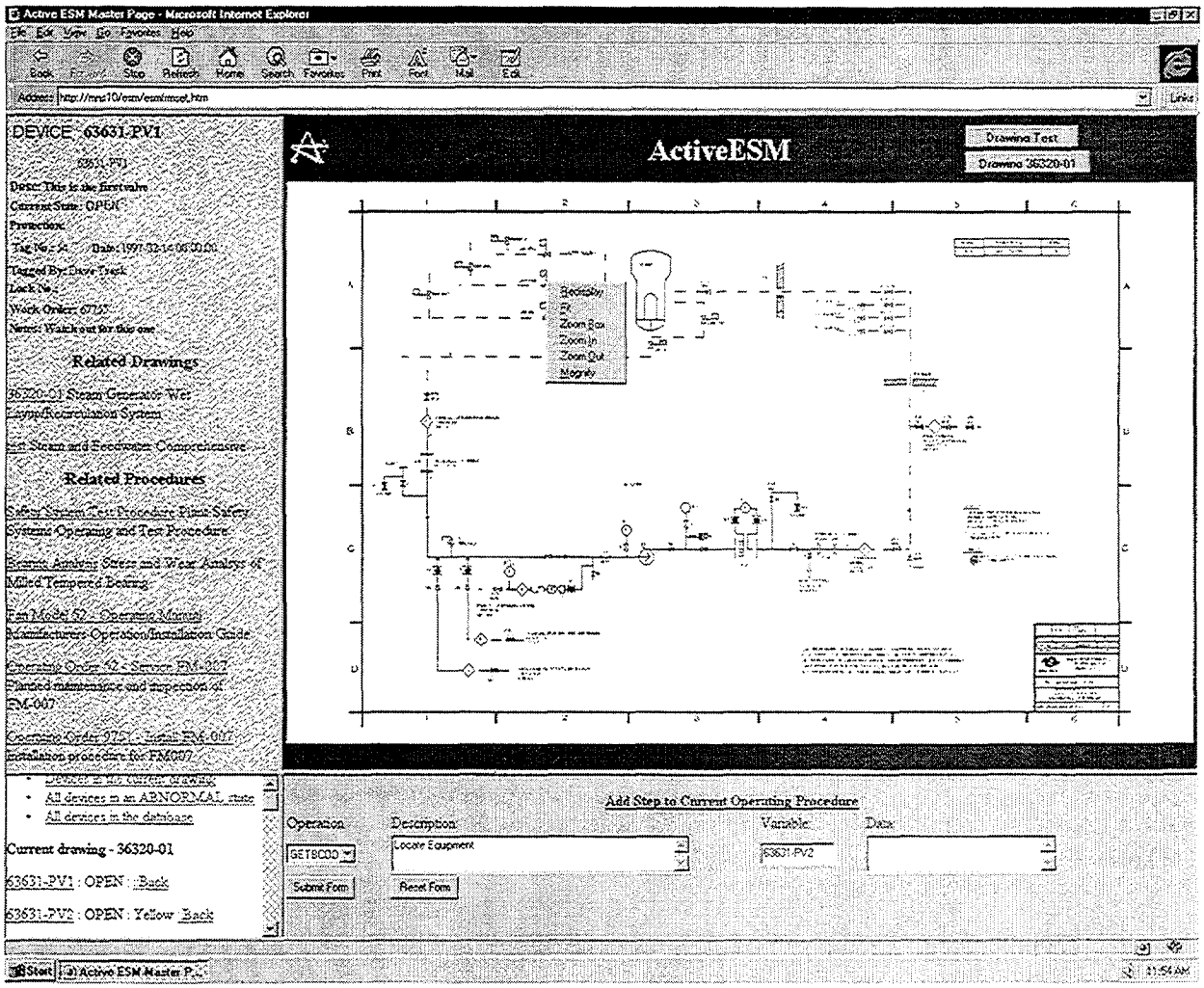


Figure 4: ESM User Interface using Internet Browser Technology.

The lower left frame also performs three ODBC queries, but displays only the device names, current state, and current protection level. The first query displays all of the devices on the current drawing, the second query displays all of the devices in the plant that are not in their pre-defined or normal state, and the third query shows all devices in the plant. Clicking on any device name will update the data in the upper left frame for the selected device. Selecting 'Back' returns the user to the top of the frame page. Searches can also be performed using the Edit/Search tool within the Edit pull-down menu and by then typing in the device name.

The lower right frame is intended to serve two purposes, the first is to display the related plant procedures when requested from the data frame in the upper right, and the second purpose of the frame is to provide a data entry form for creating and editing OOs.

The ActiveESM frame in the upper right displays animated CADD drawings. Within this frame the user can right click anywhere on the drawing to display a pop-up menu. This menu, provided as part of the ActiveX component of ActiveCGM, requires no additional programming. It features Redisplay, Fit, Zoom Box, Zoom In, Zoom Out, and Magnify. Redisplay, Zoom In, and Zoom Out are self-explanatory. Fit re-sizes the drawing such that the entire drawing is displayed within the frame. Magnify invokes a pop-up window and a

magnification frame to provide a birds-eye view of the drawing. Zoom Box allows the user to select any area of the display, which will magnify the selected area to fill the entire frame. Active elements on each drawing can be identified using one of two methods. As the cursor is moved over any active equipment symbol, the symbol colour changes to blue and the cursor changes from an arrow symbol to a hand. Secondly, if the status of any active element is not in the 'as-drawn' state, the element will appear in a colour other than black. Clicking the left mouse button on any of these active elements causes the data for the selected equipment to be queried in the upper left frame, and a pop-up menu to appear. This menu has been programmed to provide selections including 'Open', 'Close', and 'More'. These selections can be used to manually change the current operational status of any device on the drawing, or could be used as part of the process to change the operational configuration of the plant through the creation of OOs to be executed on the hand-held computerized procedure system.

OOs are created, stored, and edited within the Microsoft Access database. Each operating order is stored using a standard template (Figure 5) which includes the procedure title, revision number, author, work order information, and one or more steps, each of which includes the device name, operation, lock or tag information, and any other relevant information. The database facilitates the ability to track, edit, compare and search operating orders, by enforcing data integrity through structured data entry forms, which differ little from the standard operating order forms used today. As devices and operations are added to the procedure, the device names are validated and are then automatically added to a cross-reference table with the procedure identifier. Any queries on the device for related procedures automatically shows this relationship. In addition, other equipment data such as limits or barcodes are automatically included into the procedure to eliminate errors in transcribing and to simplify the entry process. The forms are presented, as they would appear on printed copies. Creating OOs can also be performed through the common user interface. By adding control commands to the descriptive titles in the data frame, the user can point-and-click to add the selected device and associated control to an open procedure located in the lower right frame of the display. For instance, clicking on the tag name, would add the step "Locate

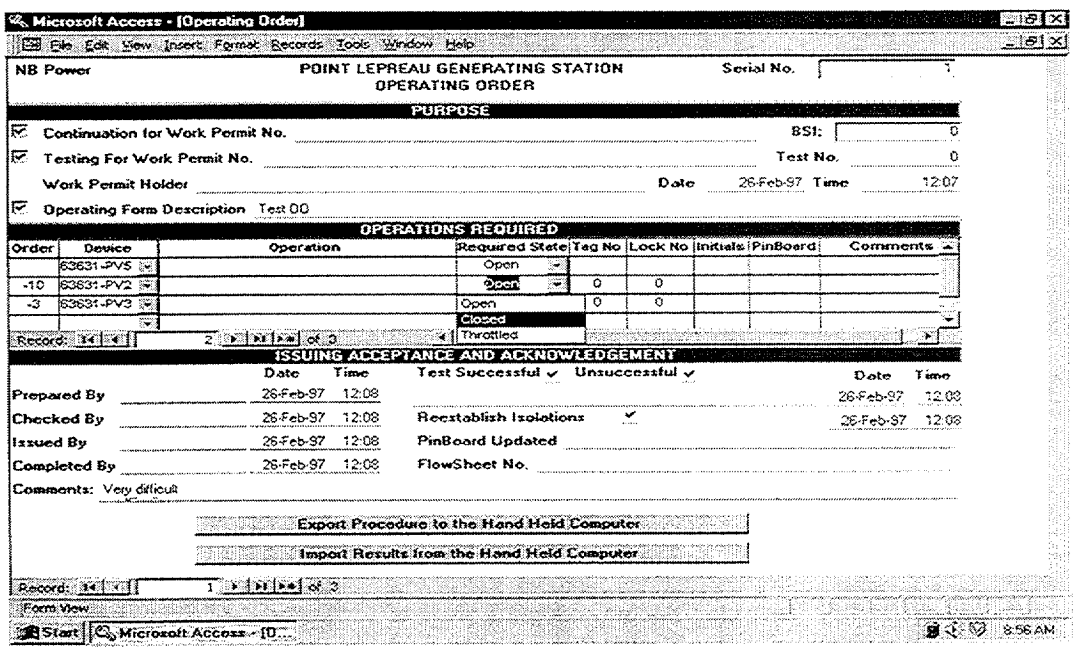


Figure 5: Database Template for Creating an OO.

device" to the procedure, and clicking on the current state would add the step "Operate device Open/Close". Once a procedure has been created, the steps can be reordered and edited through the common interface by modifying the step numbers and descriptions. In generating the steps of the OO, the system will also facilitate the generation of the necessary Standard Graphic Mark-up Language (SGML) tags interpreted by the Computerized Procedure Engine (CPE) software on the hand-held computer system to control the execution of the OO [4,5]. These tags appear in the procedure editing form as a drop-down list displaying the action identifier with a brief description of its use.

The execution of OOs takes place through the use of the hand-held computerized procedure system developed by the Canadian CANDU utilities and AECL as part of a cooperative CANDU Owner's Group project [4,5]. The heart of the system is the CPE software which interprets SGML tags embedded within standard text documents to control the execution of many types of nuclear procedures. SGML technology was the original standard of which HTML is a subset. HTML is a key technology used to navigate and display information on Internet web pages and within the ESM prototype.

The hand-held computerized procedure system offers many features and advantages. The hand-held is a light-weight tablet computer (1 kg) with a standard Intel processor, memory, and hard disk storage. The computer includes a 12x16 cm display with a standard 640 by 480 resolution. The computer can also be purchased with infrared and spread-spectrum radio frequency interfaces for wireless communications, as well as interfaces to barcode readers. A summary of the operational features of the CPE software are presented below.

1. The CPE assists in the navigation through the OO by highlighting the current step, and providing a table of contents and navigation buttons that allow hyperlinking to specific sections and pages. In addition, the CPE embeds the procedural workflow applicable to the procedure.

2. The CPE includes equipment verification through the use of a barcode scanner, which through the use of a fuzzy-logic interface can read partially damaged or obstructed barcodes.

3. Occasionally, steps may not be applicable based on the outcome of a previous step. In this case, the CPE uses a *strike out font* to indicate steps that are not to be performed.

4. Tag names, which may have had wild card designations in a paper-based procedure, are automatically filled in based on operator response. Data normally resident in the computer, such as the time and date, are automatically filled in to minimize operator entries and data entered in one step can be used throughout. This minimizes transcription errors.

5. When applicable, warnings and cautions are displayed in pop-up windows that require operator acknowledgment before the procedure proceeds. In addition, limits can be used to alert the operator to values that are out-of-range.

6. Calculations can be embedded in the procedure and automatically executed by the computer once all of the necessary data has been acquired.

7. The CPE can access and display engineering drawings, operational flowsheets, and other technical information associated with the procedure being executed.

8. The CPE provides a checking feature to ensure that all steps of the procedure have been completed. The CPE also provides a time-stamped list of all completed actions and results, which assist in ascertaining procedural compliance, but are also used to upload information to other systems such as the ESM for updating the equipment status.

After creating the OO using the ESM user interface, the procedure is downloaded into the portable hand-held tablet computer. This tablet computer is analogous to the standard clipboard normally used in the field. The operator interfaces to the computer using a stylus, which is a special pen which functions both as a mouse and as a writing tool. The operator performs each of the steps presented in the OO in the order provided, as controlled by the CPE software. The current step to be completed is always highlighted within a box. A sample OO created using the ESM prototype and loaded into the hand-held computer is shown in Figure 6. The steps within this OO include operator and work order identification, equipment verification at each step of the procedure, and the appropriate operating action to be performed. In addition, the OO includes the ability to write notes, add sketches, and reference engineering drawings relevant to the procedure.

One of the fundamental requirements of the ESM is to maintain an accurate, up-to-date status of the plant's operational configuration. The ability to modify the existing plant configuration is a critical element of the ESM. Two methods are available to update the operational status of any device listed within the ESM database and shown on the electronic

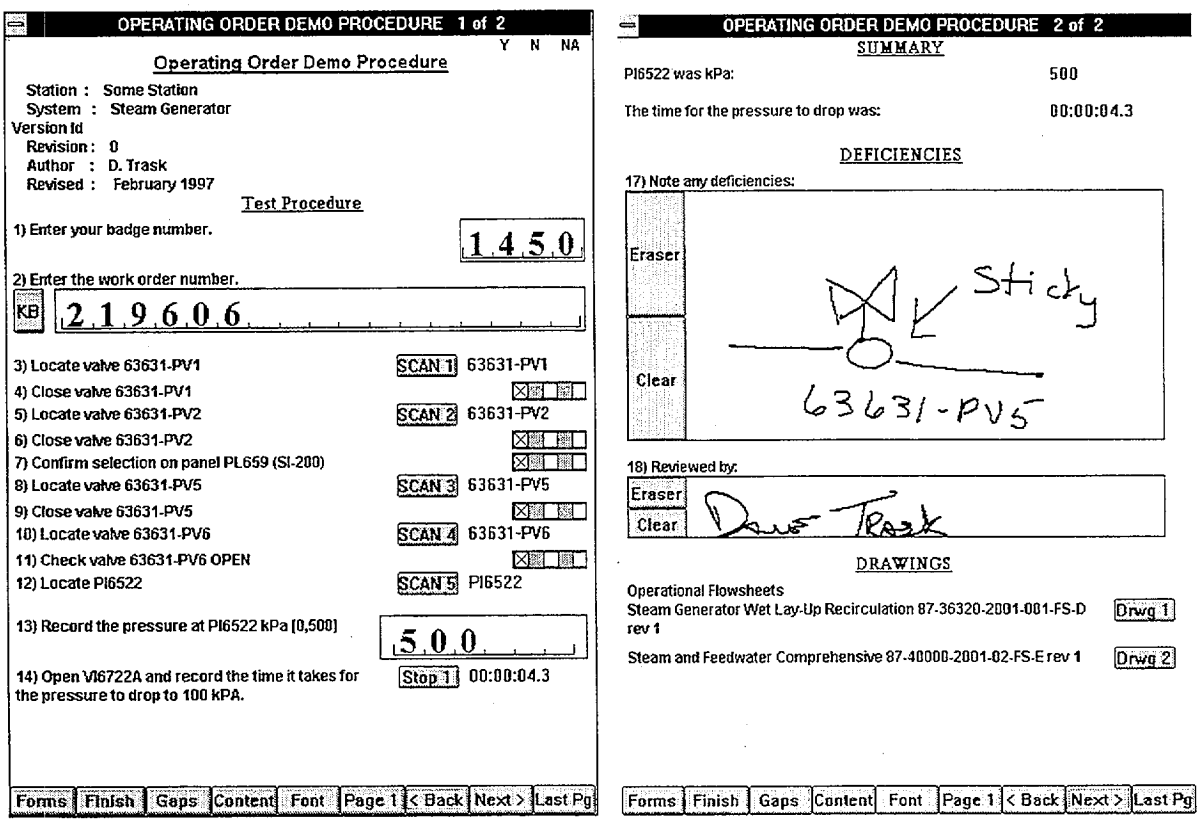


Figure 6: A Typical Example of a Computerized OO Using the CPE Software.

operational flowsheets. The first method is to manually change the status of any device through the ESM common user interface. The operator can manually change the status of any device on the electronic flowsheet by selecting the object and picking the appropriate status from within the pop-up menu. In the final ESM implementation, this action would incorporate the appropriate controls and security to ensure that the plant status was legitimately being updated by authorized users of the ESM. In the second method, the plant operational status can be updated as the final step in completing an OO using the hand-held computerized procedure system. Upon completion of the OO in the field including the completion of the appropriate review and approvals steps as required by the work control process, the information contained within the hand-held computer can be uploaded into the ESM database. This action will automatically update the ESM equipment status and the operator will instantly see the updated information in the electronic flowsheets and database as presented in the four frames of the ESM common user interface.

BENEFITS

The ESM has been designed to facilitate efficient plant operational configuration management. Some of the direct benefits of ESM include:

- reduced operational complexity,
- easier and faster access to plant device status information,
- better visualization of the plant configuration and the status of all operable devices,
- higher legibility of plant device data and records,
- semi-automated and electronic record keeping which minimizes the more boring manual tasks and reduces the risk of losing or misplacing information,
- easier and faster access to other plant data pertinent to operational configuration management,
- enhanced processes to link the design and operational configurations,
- easy access to historic OOs facilitating the creation of new OOs faster and with fewer errors,
- improved consistency in the preparation and content of OO procedures,
- enhanced tracking and execution of OOs with built-in procedural compliance and equipment verification resulting in fewer field errors and better safety to personnel, and
- faster turn-around time in updating the operational flowsheets leading to more up-to-date and consistent information supporting other operational decisions and future operational changes.

In addition, there are other benefits that can be captured as the ESM evolves within the nuclear environment. In the future, these benefits may include:

- verification that inter-linked procedures use common descriptions of equipment, instrumentation, and expected operational response,
- computer generated annunciation when equipment as-left configurations do not comply with design basis requirements, and
- the opportunity to compare actual achieved equipment performance against previous performance, targets, and expectations.

The more efficient, up-to-date, and error-free the operational configuration management process, the greater the benefit is to plant availability and reliability. Improvements to information flow and content lead directly to more accurate operational assessments of plant status, fewer operational errors, and better decision analysis. This in turn benefits plant reliability and availability.

CONCLUSIONS

Computer technology has significantly progressed over the last few years. The advent of new information technologies has made possible the integration of diverse information sources in ways not conceivable only a short time ago. The ability to hyperlink between databases and drawing objects, the integration of information via user interfaces provided by Internet browser systems, and new pen-based hand-held tablet computers makes advances in the design of operational systems realistic and achievable.

These new technologies have been integrated into the design of a generic CANDU Equipment Status Monitor system supporting plant configuration management. The improvements that can be achieved have a number of direct benefits to storing, visualizing, retrieving, changing, and overall management of the plant's operational status. These improvements can result in higher plant reliability and availability supporting higher plant capacity and capability factors.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the contribution by the Ontario Hydro Nuclear Technology Division to the design and development of the initial ESM system currently in use at the Darlington NGS. In addition, the authors would like to acknowledge the funding provided by the CANDU Owner's Group for the research and development of the next generation ESM under project WPIR 1687.

REFERENCES

[1] ONTARIO HYDRO, "Equipment Status Monitoring System Design Requirements", Revision 3 (1990 December).

[2] DEVERNO, M.T. , DE GROSBOIS, J., BOSNICH, M., POTHIER, H., XIAN, C., "Canadian CANDU Plant Data Systems For Technical Surveillance and Analysis", IAEA Specialists' Meeting on Monitoring and Diagnosis Systems to Improve Nuclear Plant Safety and Reliability, Gloucester, U.K (1996 May).

[3] DEVERNO, M.T. , DE GROSBOIS, J. , BOSNICH, M., POTHIER, H., XIAN, C., GILKS, G., "Canadian CANDU Plant Historical Data Systems: A Review and Look to the Future", Canadian Nuclear Association/Canadian Nuclear Society (CNA/CNS) Annual Conference, Fredericton, NB (1996 June).

[4] KENNEDY, E., DONIZ, K., "Hand-Held Data Collection and Procedure Environment", CNA/CNS Annual Conference, Fredericton, NB (1996 June).

[5] KENNEDY, E., "A Hand-Held Computer System to Support System Surveillance Programs", CANDU Owner's Group System Surveillance Workshop, Toronto, Ontario (1996 November).

NEXT PAGE(S) left BLANK

POWER PLANT SURVEILLANCE AND FAULT DETECTION: APPLICATIONS TO A COMMERCIAL PWR*



R.M. SINGER, K.C. GROSS, J.P. HERZOG, S. WEGERICH
Argonne National Laboratory,
Argonne, Illinois

R. VAN ALSTINE**, F.K. BOCKHORST
Florida Power Corporation,
Crystal River, Florida

United States of America

Abstract

The theoretical basis and validation studies of a real-time, model-based process monitoring and fault detection system (MSET, multivariate state estimation technique) is presented. Through use of a non-linear state estimation technique coupled with a probabilistically-based statistical hypothesis test, it is possible to detect and identify sensor, component and process faults at extremely early times from changes in the stochastic characteristics of measured signals. Data from an experimental fast reactor and a commercial LWR are used to demonstrate functional capabilities of the monitoring system. In addition, operational data from the Crystal River-3 (CR-3) nuclear power plant are used to illustrate the high sensitivity, accuracy, and the rapid response time of MSET for annunciation of variety signal disturbances. The types of faults detected and identified included the gradual degradation of a venturi flowmeter, rapidly failing flow sensor and the loss-of-time-response of a pressure transmitter.

1. INTRODUCTION AND BACKGROUND

From their earliest conception, nuclear power plants have included monitoring and fault detection systems as part of their basic design. However, in many cases these systems were of fairly elementary character and usually consisted of nothing more than upper and lower limits placed upon important sensor measurements that when exceeded would alert plant operators. Although this approach has proved to be reasonably successful, considerable advances in methods of signal and information processing have permitted the development of new techniques that not only are much more reliable and real-time operable, but also provide additional functional capabilities such as on-line sensor validation, extremely early fault detection and identification, provision of "virtual" sensors for replacement of failed sensors, diagnosis and prognosis of disturbances, fault-tolerant component operation, insight into the plant operational state, etc. At Argonne National Laboratory, such methods were initially developed to address critical operational issues at the Experimental Breeder Reactor No. 2 Power Plant (such as loss of irreplaceable sensors and forced shutdowns due to increased pump friction) [1] and then expanded for use in commercial power plants as well as many industrial processes. This paper will describe the theoretical basis of the resulting monitoring and fault detection system, summarize the supporting validation studies, and present results obtained from an experimental monitoring program performed at a commercial nuclear power station.

*Work supported by the US Department of Energy, Nuclear Energy Programs, under contract W-31-109-ENG-38.

**Presently with the ECAD Corporation.

2. OVERVIEW OF APPROACH

Numerous objectives can be ascribed to a modern process monitoring system, but perhaps one of the most important ones, at least in terms of reducing operational and maintenance costs is the following: to detect and identify incipient disturbances sufficiently early to avoid forced shutdowns and physical damage. In other words, it would be highly desirable to be able to detect disturbances so that necessary repairs can be scheduled and performed at a time convenient to plant operational requirements. This objective immediately leads to the following two needs: the detection of disturbances prior to changes in signal mean values (when mean values change, physical damage has likely occurred and shutdown may not be far off) and the minimization of both false and missed alarms (false alarms ultimately result in operator indifference and missed alarms can permit continued damage and probable shutdown). Accordingly, since the initial indication of abnormal operation of a piece of equipment usually appears as changes in the characteristics of the noise on sensors associated with this equipment, the monitoring method must utilize such information to detect and identify disturbances. To achieve this functionality, a model-based monitoring method must utilize a technique that not only has a high precision (to minimize error rates) but also be easily adaptable to the inevitable configuration and operational changes in the plant. In addition, the fault detection portion of the method must identify disturbances based upon changes in statistical characteristics of the signals as well as the mean values with prescribable missed and false alarm probabilities. These are challenging requirements.

First principal analytical models were immediately rejected as candidates because of large predictive uncertainties (perhaps 5 to 15%) which eliminate the possibility of detecting and identifying disturbances within these deadbands. The use of autoassociative artificial neural networks as a modeling technique was also considered, but extensive studies both at Argonne [2] as well as other laboratories [3] indicated that predictive uncertainties could not be consistently reduced below about 2 to 5%. However, some recent work performed by Uhrig and his students [4] have indicated that uncertainties in the range of 0.5% can be achieved. The modeling method that was found to most closely meet the requirements posed was that of state estimation using optimally nonlinearly filtered pattern recognition. This method will be described in a subsequent section.

During monitoring, this modeling technique was used to estimate the state of the reactor system which was then compared to the current measured state. The difference between the estimated and measured states was then analyzed using an extremely sensitive statistical hypothesis test (the sequential probability ratio test or SPRT) to determine if the system is in a "normal" or "abnormal" state. The extended SPRT as developed by ANL [5,6] can detect changes in the statistical characteristics of a monitored signal with prescribed probabilities of missed and false alarms. The basis of this test will also be described in a subsequent section.

3. DESCRIPTION OF MONITORING AND DIAGNOSTIC SYSTEM

As implied above, the monitoring and diagnostic system presented in this paper is based upon the use of a model of the process to estimate its operational state, make a measurement of the current operational state, and to analyze the difference between the estimate and measurement to determine if such differences are due to normal statistical fluctuations or if a real disturbance is manifesting itself. Since the model that is being used is empirically based and must have actual process data for training to recognize the interrelationships between plant variables needed for state estimation, the selection of data for training is an important issue. Since it is desired to detect and identify faults, one may decide to train the model using data obtained during specific faulted operational states of the process. However, this leads to the effectively impossible task of not only identifying all possible failure modes, but also of collecting data from each of these modes. Perhaps such data could be generated from a process simulator, but the critical information contained in sensor noise and needed for early fault detection cannot be so obtained. Accordingly, the path chosen here was to train the model using data obtained from the domain of expected normal operation so that any non-random modeling errors (i.e., differences between model estimates and measurements) could be attributed to process disturbances [7].

3.1 State Estimation Technique

The state estimation technique uses examples of the normal operating states of a system from which to learn the relationships that exist between the parameters used to define the state, make a single new observation of the system, and then use the patterns developed from the learned states to estimate the current "true" state of the system. System states are represented by vectors whose elements are chosen by the user and can range from direct values of signals from the sensors to the result of any scalar transformation of the signals. Although the state vector elements do not have to be linearly independent, they do have to represent the physical and/or chemical processes that are occurring and have some level of inter-correlation. The estimated state is calculated using a weighted combination of learned states, the weighting value being determined by the degree of pattern overlap with each learned state. The estimated state contains new estimated values for every parameter being monitored, including estimated values for sensors that have degraded or failed. Because the estimated states are based on actual established relationships with the values of all sensor signals representing the modeled system, the failure or degradation of any sensor has an insignificant effect on the estimated value for that sensor signal.

If data are collected from some process over a range of operating states, these data can be arranged in matrix form, where each column vector (a total of **m**) in the matrix represents the measurements made at a particular state. Thus, this matrix will have the number of columns equal to the number of states at which observations were made and the number of rows equal to the number of measurements (a total of **n** sensors) that were available at each observation. Defining the set of measurements taken at a given time t_j as an observation vector $\vec{\mathbf{X}}(t_j)$,

$$\vec{\mathbf{X}}(t_j) = \left[x_1(t_j), x_2(t_j), \ldots, x_n(t_j) \right]^T,$$

where $x_i(t_j)$ is the measurement from sensor i at time t_j, then we can define the data collection matrix as the process "memory" $\vec{\mathbf{D}}$:

$$\vec{\mathbf{D}} = \begin{bmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,m} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,m} \\ \vdots & \vdots & \vdots & \\ d_{n,1} & d_{n,2} & \cdots & d_{n,m} \end{bmatrix} \equiv \left[\vec{\mathbf{X}}(t_1), \vec{\mathbf{X}}(t_2), \cdots, \vec{\mathbf{X}}(t_m) \right].$$

Now, if a new observation is made and the sensor measurements from this process represent correlated phenomena, then one can assume an estimate of this vector of measurements can be represented by a linear combination of the column vectors in the data collection matrix. By minimizing the Euclidean norm between the estimated and measured data vectors, it is possible to obtain the following linearly optimal estimate of $\vec{\mathbf{X}}$:

$$\vec{\mathbf{X}}_{est} = \vec{\mathbf{D}} \cdot \left(\vec{\mathbf{D}}^T \cdot \vec{\mathbf{D}} \right)^{-1} \cdot \vec{\mathbf{D}}^T \cdot \vec{\mathbf{X}}_{obs} .$$

However, this result has numerous limitations, including but not restricted to the requirement that $[\vec{\mathbf{D}}^T \cdot \vec{\mathbf{D}}]$ be non-singular, an inability to accommodate random uncertainties, non-random defects, and very large databases. These characteristics of real data strongly diminish the range of applicability of this classical (linear) estimation technique.

Due to these limitations, it is necessary to examine alternative approaches that can be used in non-linear systems as well have robust properties in terms of handling all types of data characteristics. However, the formalism of the linear approach lead to a relationship between an estimate of the system state, a current measurement and the system history that has several very useful features. For example, the model "memory" can be easily expanded by simply adding new observation column vectors to the matrix $\vec{\mathbf{D}}$ $\vec{\mathbf{D}}$ and the only aspect of the relationship that might be computational intensive, the matrix inversion, can be performed "off-line" prior to repeated or

on-line estimations. These features are of sufficient value and utility that, if possible, they should be retained in any new non-linear approach. With this in mind, one can assume that the form of the linear estimation equation derived earlier can be used, but with a modification of the linear matrix operators to a non-linear form:

$$\vec{X}_{est} = \vec{D} \cdot \left(\vec{D}^T \circledast \vec{D} \right)^{-1} \cdot \left(\vec{D}^T \circledast \vec{X}_{obs} \right)$$

Here, the non-linear operator $\circledast$ is at present unknown and must be chosen so as to preserve the desirable features of the linear operator and in addition to have the following properties:

(1) The matrix $[\vec{D}^T \circledast \vec{D}]$ must be non-singular;
(2) If some elements in the observation vector are not within the ranges of the same elements of the column vectors in the memory matrix $\vec{D}$, the estimation vector must still represent an optimum estimation;
(3) If the observation vector is identical to one of the column vectors in $\vec{D}$, then the estimation vector must be identical to the observation vector;
(4) The error vector (difference between the observation and estimation vectors) must be minimized.

Two such operators that fulfill these conditions have been found, but cannot be presented here due to patent and proprietary issues.

3.2 Sequential Probability Ratio Test (SPRT)

The sequential probability ratio test [5] is a statistical hypothesis test that differs from the standard fixed sample test in the way in which statistical observations are employed. In the fixed sample test, a given number of observations are used to select one hypothesis from two or more alternatives. The SPRT, however, sequentially examines one observation at a time, and at some point makes a decision and selects a hypothesis.

The basic approach taken by the SPRT technique is to analyze successive observations of a discrete physical process by a comparison (difference) of the stochastic components of signals generated by two redundant sensors monitoring the process, or of signals generated by an actual and simulated sensor monitoring the process. Details of the use of SPRT in fault detection were provided in [6] and are briefly summarized here. SPRT solves the problem of deciding between two possible hypotheses: H_1, where the difference set forms a Gaussian probability density function with mean M (a system disturbance magnitude) and variance σ^2; or H_0, where the difference set from a Gaussian probability density function with mean 0 and variance σ^2. If the SPRT accepts H_1, then we declare that one of the two signals is degraded. Additional SPRT testing on other pairs of signals provides the information needed to logically deduce the specific sensor failure. The index and logic used for deciding upon hypothesis H_1 or H_2 is

$$L = \frac{M}{\sigma^2} \sum_{k=1}^{n} \left(y_k - \frac{M}{2} \right),$$

If $L \le \beta/(1-\alpha)$ then accept hypothesis $\mathbf{H_0}$ as true,
If $\beta/(1-\alpha) \le L \le (1-\beta)/\alpha$, then continue sampling,
If $L \ge (1-\beta)/\alpha$, then accept hypothesis $\mathbf{H_1}$ as true.

where α is the probability of accepting $\mathbf{H_1}$ when $\mathbf{H_0}$ is true (i.e., the false alarm probability) and β is the probability of accepting $\mathbf{H_0}$ when $\mathbf{H_1}$ is true (i.e., the missed alarm probability).

A second sequential probability ratio test for normal distributions examines the variance of the sequence. In the variance test, the system is degraded if the sequence exhibits a change in

variance by a factor of **V**, where **V**, the preassigned system disturbance magnitude for the variance test, is a positive number. The problem is to decide between two hypotheses: $\mathbf{H_2}$, where the difference set forms a Gaussian probability density function with mean **0** and variance $\mathbf{V}\sigma^2$; or H_0, where the difference set form a Gaussian probability density function with mean **0** and variance σ^2.

In this case, the index to be used is

$$L = \frac{1}{2\sigma^2}\left(\frac{V-1}{V}\right)\sum_{k=1}^{n} y_k^2 - \frac{1}{2}\ln V .$$

and the same threshold limits are used for the variance test as those used in the mean test.

A primary limitation of the applicability of SPRT statistical tests for sensor and equipment surveillance strategies lies in the primary assumption that the difference sequence is independently-distributed random data with strictly "white" noise. In most cases residual signals from a redundant sensor pair or from an actual and simulated sensor pair are normally distributed even though the raw signals may have some other distribution. It is, however, rare to find physical process variables associated with operating machinery that are not contaminated with serially-correlated, deterministic noise components.

A tool box of preprocessing methods have been developed at ANL, e.g. [8, 9], that convert a signal with any type of statistical idiosyncracies into a Gaussian signal that can be used directly with SPRT. If this was not performed, in many cases the hypothesis test would be invalid and large rates of missed and false alarms would result.

4. VALIDATION STUDIES OF THE MONITORING AND DIAGNOSTIC SYSTEM

Although an extensive validation program has been performed, only three studies can be presented here. The first examined the accuracy of the state estimation algorithm, i.e., the error in the estimate of a signal. A typical result is shown in Figure 1 where an estimate of a thermocouple signal from EBR-II is compared to the measured value. In this case, data were collected from 18 subassembly outlet thermocouples at 50 different times and used to "train" the model, i.e., to construct the memory matrix $\overline{\mathbf{D}}$. This model was then used in a monitoring mode for 50 minutes in which a measurement and estimate was made each minute. As can be seen by the comparison in Figure 1, the estimate for this signal is quite accurate, even following the small scale fluctuations of about +/-0.2 F. Although the average estimation error for all 18 signals computed in this test was about 0.004%, the general experience covering a wide range of operating conditions indicates that estimation errors of 0.1% to 0.2% can be expected. However, this accuracy appears to be much better than other methods that were evaluated and considered acceptable for use in fault detection.

The second test was an evaluation of the fault tolerance of the state estimation technique, i.e., can accurate signal estimates be made in the presence of multiple sensor faults. Again, extensive testing of this feature was performed and only one example can be presented. In this case, the entire heat transport circuit of the EBR-II reactor was modeled with 115 sensors. Readings from these sensors were taken at 11 separate operating states of the plant to construct the memory matrix $\overline{\mathbf{D}}$ and then monitoring was initiated. Sensor failures were simulated with the plant data acquisition system (without affecting actual plant operation) and included many failure modes (e.g., sudden shifts, gradual drifting, total loss, etc.). Under the worst conditions, 15 sensors were failed with another 5 being adversely impacted due to interrelationships; thus, a total of 20 sensors or 17% were providing erroneous information. In spite of this, as can be seen in Figure 2 where the reactor temperature rise is shown, the estimated value of this signal did not change as there were no actual changes in the plant. In other words, although over 17% of the plant sensors had "failed", the plant state had not changed and the estimation method recognized this from the information obtained from the 83% of the sensors that were correctly operating. In addition to this capability to predict the correct value of a failed sensor, although not shown here, correct values of signals from unfailed sensors were also

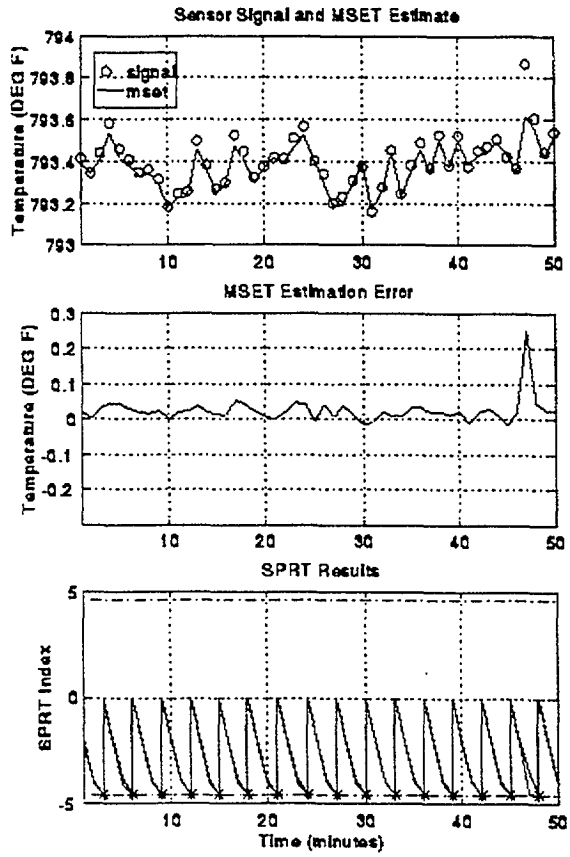


FIG 1. Evaluation of Accuracy of State Estimation Method

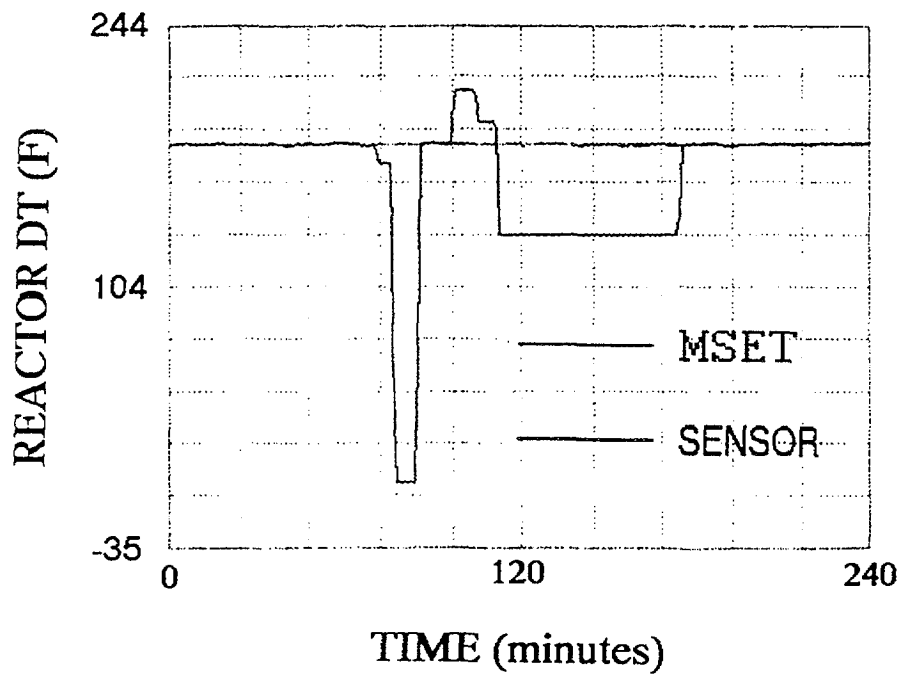


FIG. 2. Demonstration of Method's Capability to Operate with Multiple Failures

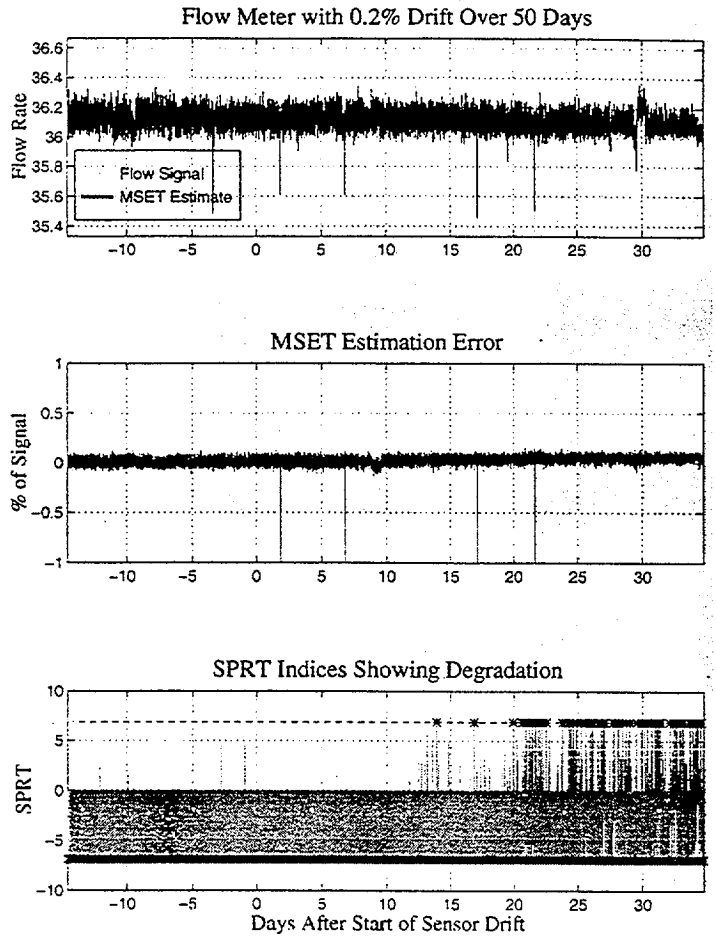


FIG. 3. Sensitivity of Fault Detection Method to Subtle Disturbances

made. This is an important characteristic for fault detection since it reduces the possibility of false alarms.

The third type of validation test involved studies of the sensitivity of the overall method (state estimation coupled with the SPRT hypothesis test) to detect faults; this is necessary if sufficient warning time can be provided to permit non-forced corrective action. Again, numerous tests were performed, but a typical result is shown in Figure 3 where data from a commercial PWR feedwater flowmeter is shown. A total of 60 sensors, all physically associated in some way with the feedwater flow, were measured at 13 times and used to construct the memory matrix. These 60 signals were then monitored over a period of 45 days during which no actual failures occurred; the test was performed by superimposing an artificial drift in only the feedwater flow sensor starting at time zero. The rate of drift was 0.2% over 50 days which would result in just a 1.0% change in sensor output after 250 days had passed, a degradation that would just possibly show up in a trending analysis and certainly not exceed operational limits. However, the monitoring code detected this drift initially at 13 days after its start and clearly confirmed the fault after about 3 weeks. At this time, the signal had degraded just 0.084%. Accordingly, if this had been a real fault, the operators would have had many months to perform any additional hands-on diagnostics and repairs and almost certainly not interfered with plant operation.

5. APPLICATION TO PWR PLANT SIGNALS

Argonne National Laboratory (ANL) and the Florida Power Corporation (FPC) have been engaged in a collaborative study since 1992 to configure and test ANL's MSET system using signals

from Florida Power's Crystal River-3 (CR-3) pressurized water reactor power plant for a variety of surveillance applications that include signal validation, instrument calibration monitoring, and early detection of component operability degradation. For the examples reported here, actual plant signals were taken from archive optical disks from the 18 month operating cycle spanning from June of 1992 through Dec. of 1993.

5.1 Venturi Flowmeter Surveillance with MSET

One of the primary objectives of nuclear power plants is the efficient operation of plant systems, thereby reducing the cost of electricity. Accurate determination of the thermal power of the plant is required to minimize the cost per unit of energy produced. The feedwater flow rate to the steam generators is one of the primary quantities used for the thermal power calculation [10]. However, the accuracy of the flow meters that measure the feedwater flow rate deteriorates over time resulting in flow rate measurements that are higher than their actual values, thus yielding artificially high thermal powers [11]. U.S. NRC licensing rules require that a reactor be operated at or below the rated power for the reactor. Since these rules also require that the calculated thermal power be used when setting the operating conditions of the plant, the real power produced by a reactor hampered by inaccurate feedwater flow measurements will be less than the power rating for the reactor. A 2% power derating costs a utility about $20,000 per day, or 7.3$M per yr, in lost revenue for an 800 MWe unit at an energy cost of $0.05 per kW-hr [11].

Venturi flow meters are commonly used to measure the feedwater flow rate in nuclear power plants. The flow meters consist of a short section of constricted flow area piping (the venturi surface) that is inserted between two flanges in the feedwater pipe. The constriction accelerates the fluid and temporarily lowers its static pressure. Pressure gauges are used for measuring the pressure drop between the inlet and constricted regions of the flow meter. Fluid flow rate is directly related to the pressure drop. The accuracy of venturi flow meter measurements decreases with time though, due to a chemical reaction between the surface coating of the flow meter and the feedwater. The fouling of the venturi surface with reaction products results in flow measurements becoming 1 % - 2% higher than the actual flow [12]. The fouling problem has been observed to develop rapidly, after as little as 2 months of operation with a clean venturi flow meter. During long shutdown periods of the reactor, the feedwater flow meters are cleaned and recalibrated. But since the long shutdown periods occur at the end of a reactor operating cycle, which typically lasts for 18-24 months, reactors can spend most of their normal operating time with fouled feedwater flow meters.

We have used the MSET system to model the feedwater flow meter as a function of dissimilar process variables dynamically related to the feedwater flowrate. When trained with reliable data, the MSET model can estimate the correct flowrate regardless of the changes in the physical state of the flow meter, since the model's estimates are based on the behavior of the system as a whole.

The MSET system is used to model one of the two feedwater flow meters in Florida Power's CR-3 two feedwater flow meters in Florida Power's CR-3 power plant. The two feedwater flow meters are located in the piping that supplies condensate water to the loop A and B steam generators. Because the two loops contain identical components, only the feedwater flow meter in loop A has been modeled by MSET for the present investigation. The MSET model utilizes data from 15 diagnostic sensors in loop A. In addition to the flowrate data from feedwater flow meter A, the model utilizes signals from other loop A sensors including steam generator level indicators, steam line thermocouples, feedwater thermocouples, and the feedwater pump tachometer. The signals that are included in the model are those that are most highly correlated with the feedwater flow meter signal. For this analysis, only every 10^{th} point recorded during the reactor cycle was used (i.e., one point every 10 minutes). But since the reactor run lasted 476 days, the total number of data points used in the analysis is over 68,000.

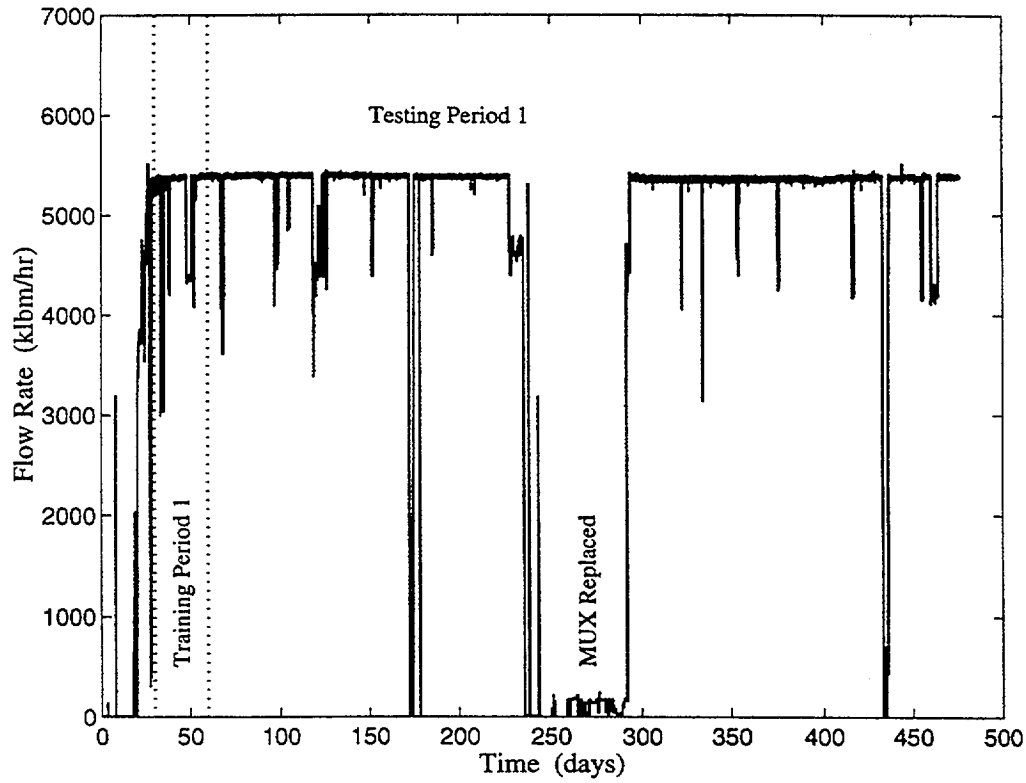


FIG. 4. Measured Flow Rate for the Loop A Venturi Flow Meter (lst Calculation)

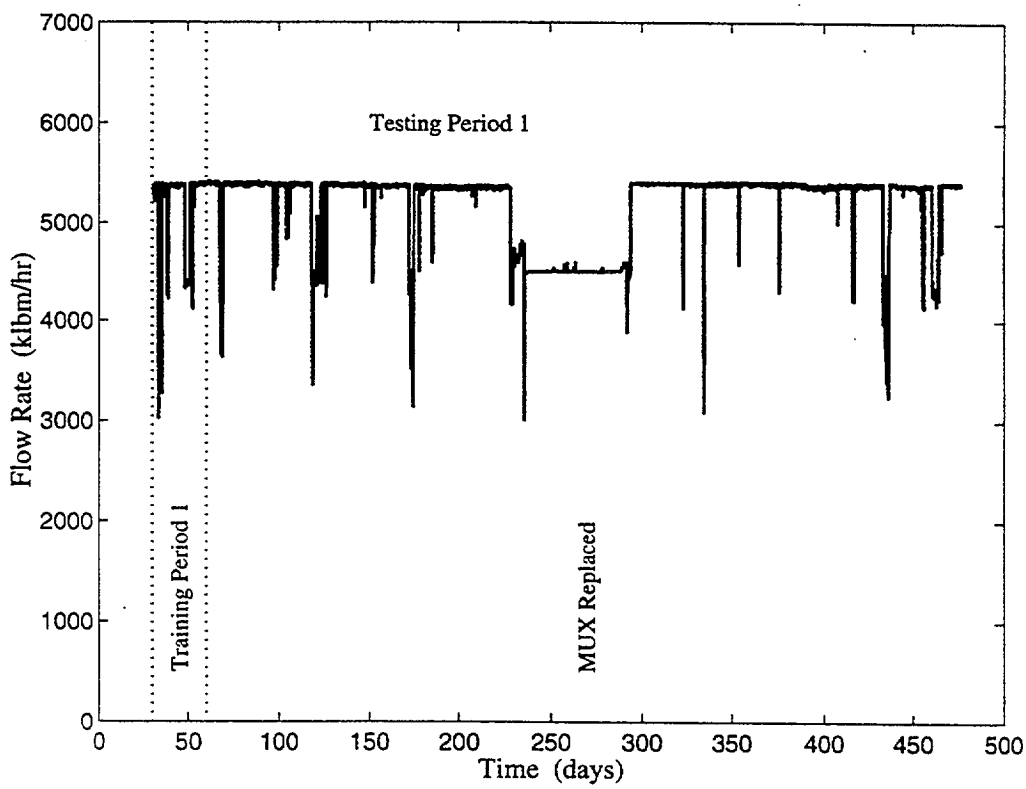


FIG. 5. Calculated Flow Rate for the Loop A Venturi Flow Meter (lst Calculation)

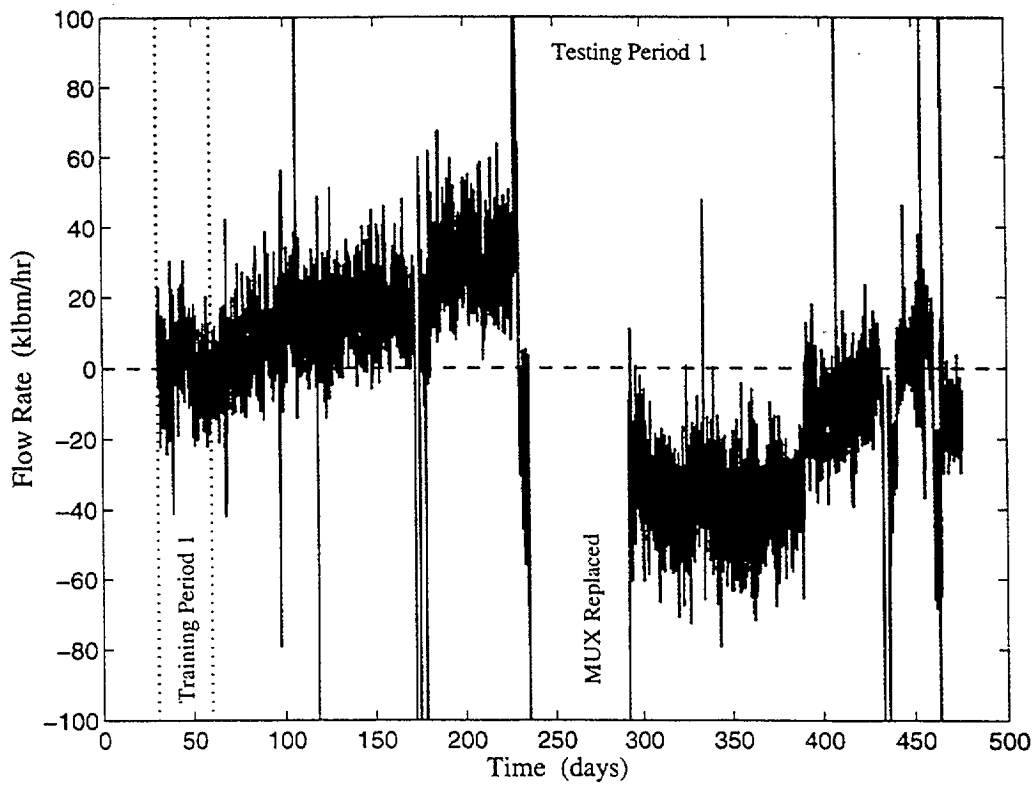


FIG. 6. Difference between Measured and Calculated Flow Rates (lst Calculation)

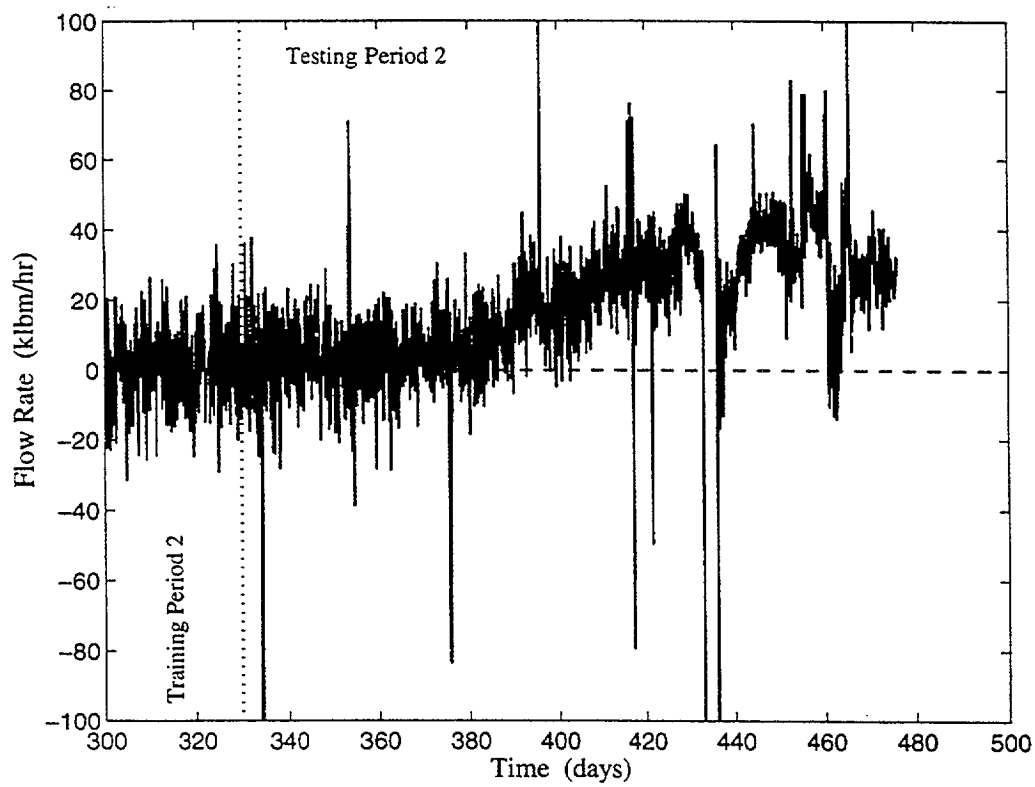


FIG. 7. Difference between Measured and Calculated Flow Rates (2^{nd} Calculation)

The MSET model was trained using data from the second month of the operating cycle (i.e., days 30 through 60). Fig. 4 shows the signal from the loop A feedwater flow meter for the whole of the operating cycle. The figure indicates which period of the reactor cycle was used to train the model and which period was used to test the model. Also indicated in Fig. 4 is a roughly 2 month period at the middle of the reactor run during which the feedwater signal was not archived. During this period, the reactor's data acquisition system was off-line due to the replacement of a multiplexor (MUX).

In Fig. 5, the MSET calculation for the feedwater flow is shown. The calculated flowrate compares well with the flow meter measurements. In Fig. 6, the difference between the measured and calculated flowrates is shown. Note that the calculated and measured flowrates drift apart during the first 6 months of the testing period 9 days 60 to 220). This drift is due to the fouling of the flow meter, which causes it to report flowrates that are higher than the calculated flowrates.

By the end of the first 6 months of the testing period, the measured flowrate is about 0.5% larger than the calculated flowrate. A discontinuity is evident between the response of the difference signal from before the period when the data archival system was taken off-line and the response from after the period. Immediately before the MUX was replaced, the measured flowrate is about 30klbm/hr greater than the calculated flowrate, the measured flowrate is about 40 klbm/hr less than the calculated flowrate. The discontinuity is due to the recalibration of some of the sensors in the feedwater system. When the sensors used as inputs to the model are recalibrated, the model must be retrained since the earlier training patterns are no longer valid. To illustrate this point, a second calculation was performed in which only data recorded after the MUX replacement were used. Data from the eleventh month of operation (i.e., days 300 through 330) were used to train the model in the second calculation. In Fig. 7, the difference between the measured and calculated flowrates for the second calculation is shown. The second calculation reveals an additional drift of about 0.7% in the flow meter measurements during the later half of the operating cycle.

The MSET analysis has shown that the degradation of venturi flow meter measurements due to fouling of the venturi surface can be detected. The analysis of the Crystal River-3 data revealed a slow and steady degradation of the flow meter measurements during the 1992/1993 cycle.

5.2 Failure of a Flow Sensor

This second example is of a rapidly failing flow sensor in CR-3 that was taken from signal archives. The upper subplot in Fig. 8 shows data from sensor R237, the primary loop B flowrate, superimposed upon the MSET estimate for that signal. This flow sensor failed (i.e., its output dropped by about 5% in a several hour period) on day 167 in the reactor cycle. MSET was trained to recognize the normal behavior of the system in which this flow sensor was located and then used to monitor the system. It can be seen in Fig. 8 that the actual flow signal and the MSET estimate agreed quite well during the initial portion of the monitoring period. This is also indicated by the middle subplot, which shows the estimate error--or the difference between the measured and estimated flowrates. As observed in the upper subplot, the measured and estimated flow values clearly diverge after about 167.5 days (a few percent difference). Indeed, if this signal was being closely watched, this failure would likely be detected by visual observation at this point. However, at 167.5 days, a full 9 hours before the fault would become evident to visual observation, MSET starts to alarm (the lower subplot in Fig. 8), indicating that sufficient information has been obtained to confirm that a malfunction also occurred. A short time later, the fault is obvious where the measured signal decreases from its initial value of about 72 to about 70 while the estimated signal remains at it's initial value. The significance of the estimated value remaining where it does is quite important; this directly implies that despite the large change in the signal form the pressure sensor, the model has determined from the total collection of sensor data available that the system state has not changed and this sensor similarly should not change. Thus, it can be concluded that the fault is isolated to this particular sensor and that the process has not been affected. If this had been a safety critical sensor, the process could have been shut down prior to the loss of this sensor. However, it

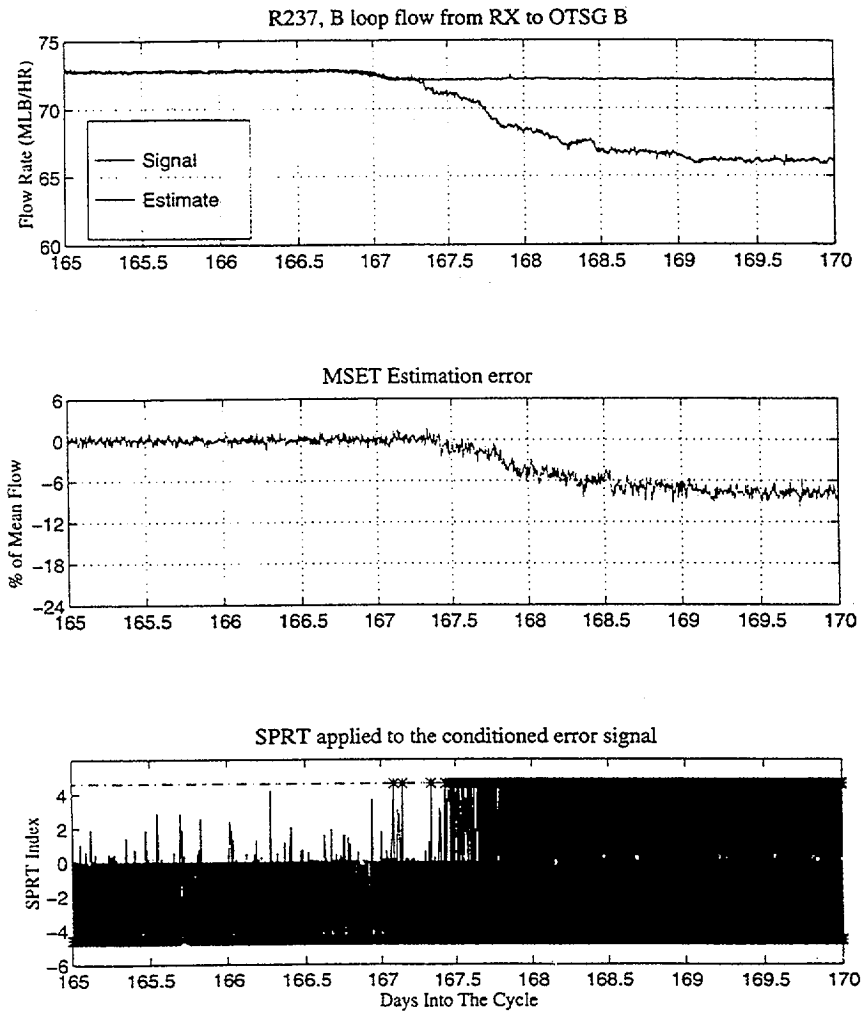


FIG. 8. Failure of R237, detected using MSET on day 167 of the cycle

would also have been possible to utilize the estimated sensor reading from MSET to replace this faulted sensor and to continue operation of the process.

5.3 Loss-of-Time Response Failure

A loss-of-time-response failure in an instrument is one of the most difficult modes of failure to identify with conventional surveillance schemes during steady-state operation. In this mode of failure, which has been known to occur particularly with oil-filled pressure transmitters, the mean value of the signal may remain unchanged. The disturbance may show up only as a change in the dynamic response of the transmitter. Conventional trending programs that use simple threshold limits, and even parity-space methods that rely on the mean values of signals, may fail to identify this mode of failure.

One such failure was identified in CR-3 in January, 1993. The failed sensor was one of three redundant sensors. To illustrate the very high sensitivity of the SPRT method for identifying extremely subtle disturbances in sensors with incipient faults, Fig. 9 shows signal segments from two of the redundant sensors, R200 and R201. The data shown in these figures were taken from mid-mid-December 1992, before the instrument degradation was observable to operations personnel. The middle subplot shows the residual function, which exhibits small fluctuations about a zero mean. The bottom subplot shows continuous SPRT alarms--even though no discrepancy is at all apparent to a visual inspection of the raw signals.

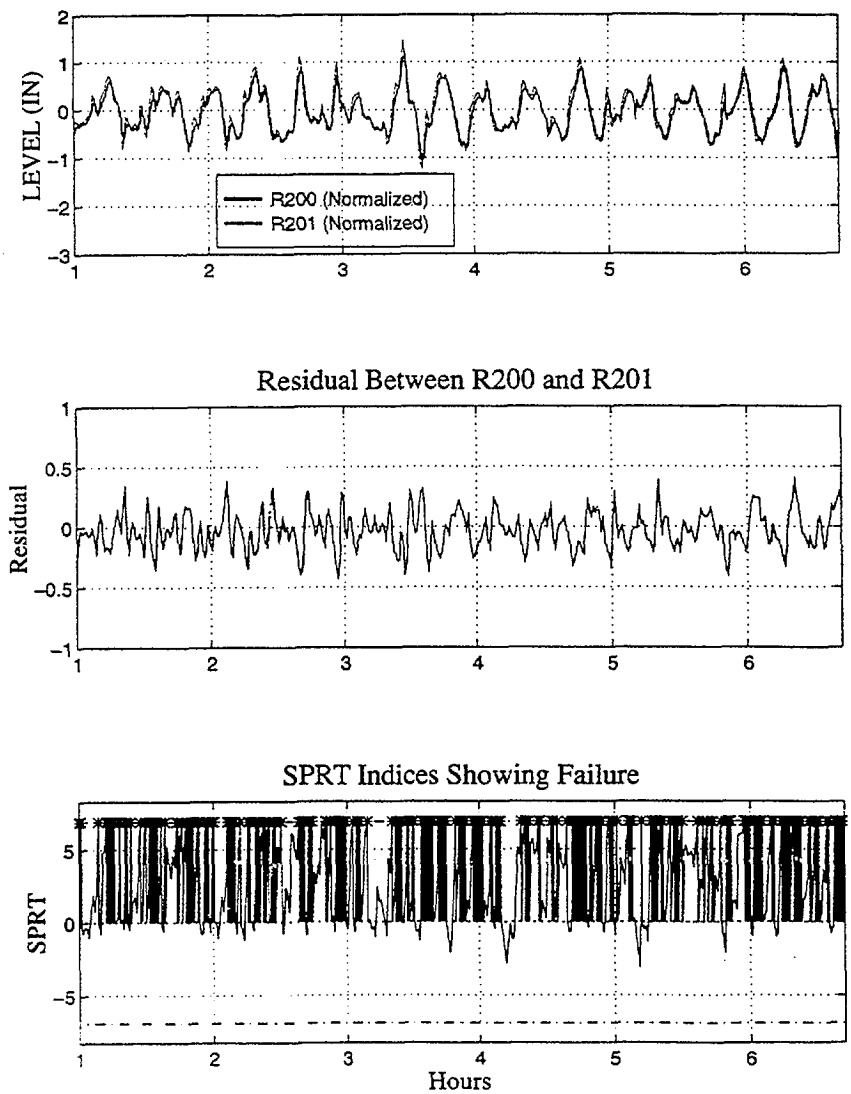


FIG. 9 (I) RPS--ES Rosemount Transmitter Time Constant Failure

Fig. 10 shows the raw signals for redundant sensors R200 and R202 (upper subplot), the residual function (middle subplot), and the SPRT index (bottom subplot). Once again, SPRT alarms tripped continuously, indicating a sensor disturbance in R200 or in R202. Finally, Fig. 11 shows the same corresponding information for redundant sensors R201 and R202. Note that there are no SPRT alarms in the lower subplot of Fig. 11. The conclusion that can be drawn from the SPRT results in these three figures is that sensor R200 is failing.

To learn how much earlier degrading sensor R200 could have been identified by the SPRT method, archive signals were processed from several weeks before the sensor was confirmed to have failed. Fig. 12 summarizes the results from the SPRT calculations for the three redundant signal pairs. Note that for both signal pairs involving pressure transmitter R200, SPRT "signal degradation" alarms started tripping at a high frequency early in the figure. The SPRT for sensors R200 and R202 started to alarm on day 119 in the operating cycle, and for sensors R200 and R201 on day 120. These SPRT annunciation times corresponded to 10/19/92 and 10/20/92, respectively. This is a full three months before the degradation became observable to operations personnel

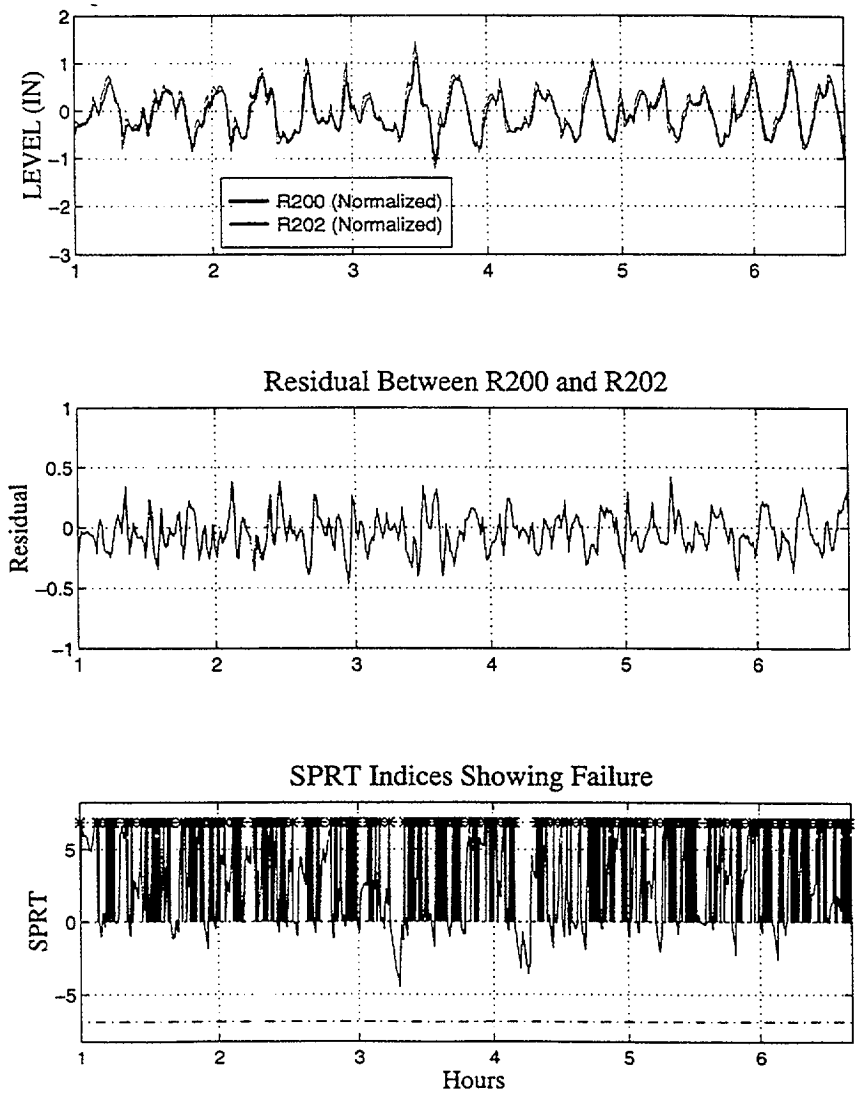


FIG. 10. (II) RPS--ES Rosemount Transmitter Time Constant Failure

6. SUMMARY AND CONCLUSIONS

A highly accurate and sensitive model-based monitoring and fault detection system (MSET) has been developed and validated with data from an operating sodium-cooled fast reactor and a commercial PWR. The model is based upon a state estimation technique that utilizes nonlinear optimal filtering pattern recognition and an extended version of the sequential probability ratio test. Extensive validation tests were performed in which the prediction accuracy, tolerance of multiple faults and fault detection sensitivity were demonstrated; selected results from these tests were reported here. In addition this paper has presented a demonstration of the complete MSET method to detect and identify both sudden and subtle malfunctions in sensors from an operating nuclear plant.

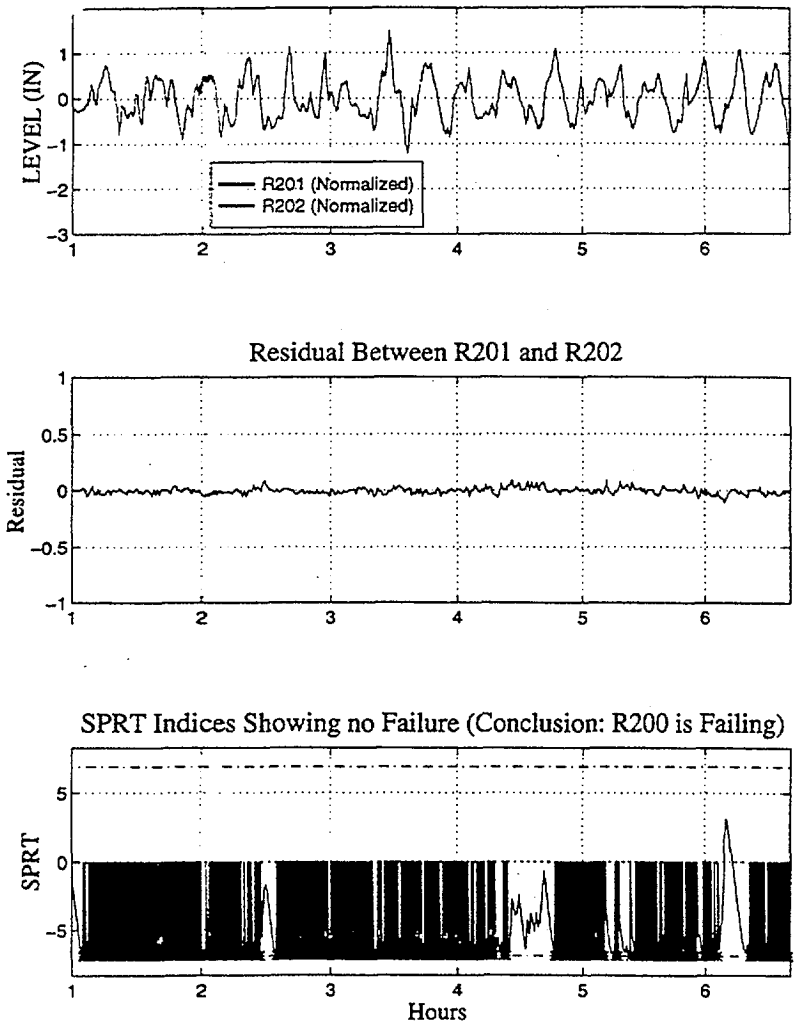


FIG. 11. (III) RPS--ES Rosemount Transmitter Time Constant Failure

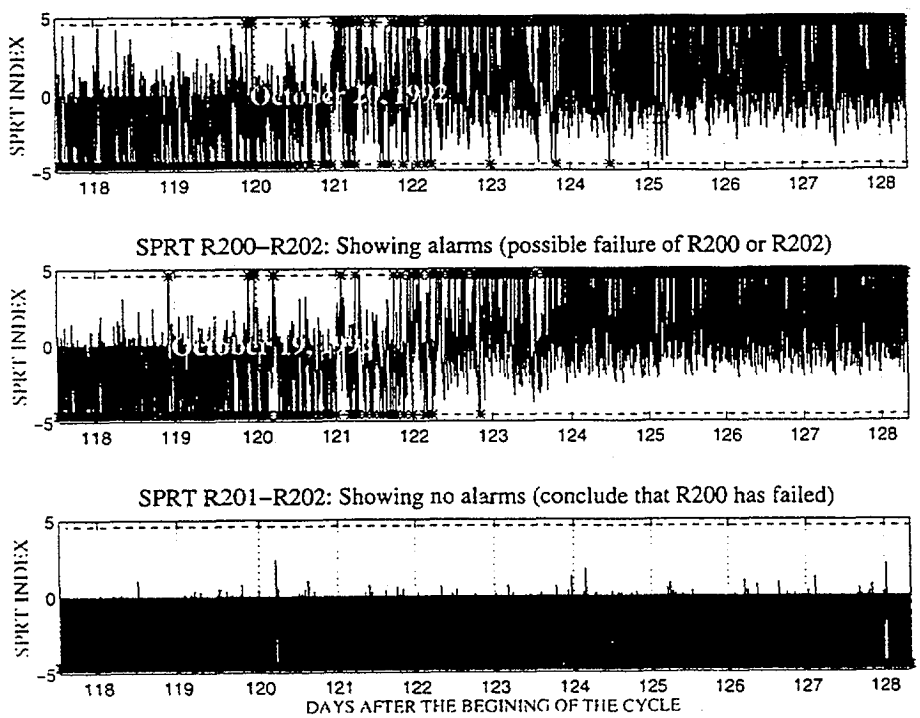


FIG. 12 SPRT R200-R201: Showing alarms (possible failure of R200 or R202)

REFERENCES

[1] R. M. Singer, K. C. Gross and R. W. King, "Applications of Pattern Recognition Techniques to Online Fault Detection," Proc. First Intl. Machinery Monitoring and Diagnostics Conf., Las Vegas (11-14 Sept 1989) 853-868

[2] J. P. Herzog, personal communication (Jan. 1995).

[3] E. Türkcan and Ö. Ciftcioglu, "Neural Network Benchmark for SMORN-VII," Overview Proc. 7th Symp. Reactor Surveillance and Diagnostics (SMORN-VII), NEA/MSC/DOC96 (17 May, 1996) 39-54.

[4] R. E. Uhrig, University of Tennessee (Knoxville), personal communication, (July 1997).

[5] A. Wald, "Sequential Analysis," John Wiley & Sons, New York (1947).

[6] K. C. Gross and K. E. Humenik, "Sequential Probability Ratio Test for Nuclear Plant Component Surveillance," Nucl. Technol., Vol. 93 (Feb. 1991) 131-137.

[7] R. M. Singer, K. C. Gross, R. W. King and S. Wegerich, "A Pattern-recognition-based, Fault-tolerant Monitoring and Diagnostic Technique." Proc., Symp. Nuclear Reactor Surveillance and Diagnostics (SMORN VII), Avignon, France Vol. 2 (June 19-23, 1995) Vol. 2 13-4.

[8] K. C. Gross and K. K. Hoyer, "Spectrum-Transformed Sequential Testing Method for Signal Validation Applications." 8th Power Plant Dynamics, Control & Testing Symp., Knoxville, Tenn., Vol. I (May 1992) pp. 36.01-36.12.

[9] K. E. Humenik and K. C. Gross, "Using Fourier Series Methods to Reduce Correlation of Nuclear Power Reactor Data," Nucl. Sci. and Eng. Vol. 112 (Oct. 1992) 127-135.

[10] K. Kavakliogul and B. R.Upadhyaya, "Monitoring Feedwater Flowrate and Component Thermal Performance of Pressurized Water Reactors by Means of Artificial neural Networks," Nuclear Technology, Vol. 107, July 1994, pp. 112-123.

[11] "Feedwater Flow Measurements in U.S. Nuclear Power Generation Stations," TR-101388, Electric Power Research Institute, Nov. 1992.

[12] "Flowrate Mismeasurement Causes Unneeded Derating," Nuclear News, Feb. 1993, pp. 39-40.

COMPUTER-GENERATED DIRECT PERCEPTION DISPLAYS FOR SUPPORTING PWR FEEDWATER SYSTEM START-UP AND FAULT MANAGEMENT: A PROOF-OF-PRINCIPLE IN DESIGN

D.V.C. REISING*, B.G. JONES**, N. MORAY***, S. SHAHEEN**,
P.M. SANDERSON+, J. RASMUSSEN++



*Department of Mechanical and Industrial Engineering,
University of Illinois at Urbana-Champaign,
Urbana, Illinois, United States of America

**Department of Nuclear Engineering,
University of Illinois at Urbana-Champaign,
Urbana, Illinois, United States of America

***Department of Psychology,
University of Surrey,
Guildford, United Kingdom

+Swinburne University of Technology,
Victoria, Australia

++HURECON
Denmark

Abstract

Traditional Single-Sensor, Single-Indicator displays are poorly matched to the cognitive abilities of operators, especially for large and complex systems. It is difficult for operators to monitor very large arrays of displays and controls as well as to integrate the data displayed into the meaningful information needed to complete tasks. Research over the last decade on interface design has suggested that computer generated graphical or "configural" displays are better designed to support these complex tasks. Moreover, a theoretical framework for designing such graphical interfaces known as Ecological Interface Design is becoming more widely accepted as the basis for designing control interfaces for continuous process control systems. If the start-up sequence of a plant can be thought of as constructing that plant from its components, then the level at which operators think about the plant becomes progressively more global and abstract during the start-up procedure. As operators construct the plant, they climb the "abstraction hierarchy" in terms of their cognitive reasoning. Standard operating procedures (SOPs) do not support this intellectual effort or change of strategy for thinking more globally about the plant. SOPs run to many hundreds of pages, are difficult to use, and require multiple operators. The manuals do not in themselves provide indications that steps have been omitted, performed in the wrong order, performed at the wrong time, or that inappropriate actions have been performed – nor do they indicate what appropriate steps *have* been completed. A graphical interface is proposed which should enforce the correct sequence of behaviors, prevent incorrect sequences, and provide constant feedback as to the state of the plant as well as the location of the operator actions in the overall start-up sequence. More generally, we believe that such an approach can support normal operations and recovery from fault conditions, but, as shall be discussed, there are difficult problems which have not yet been investigated in extending the proposed approach to fault management. In the present research Rasmussen et al's framework was used for designing computer-generated graphical displays that support pressurized water reactor (PWR) start-up. Specifically, a suite of displays was developed to support a PWR's feedwater (FW) system start-up as a proof-of-principle. The suite of displays demonstrate the theoretical design approach and are not meant to represent a fully implementable interface for FW system control.

1. INTRODUCTION

The traditional Single-Sensor, Single-Indicator (SSSI) display is poorly matched to the cognitive abilities of operators, especially for large and complex systems [1]. With the increasing use of computing power, future displays will be computer-generated, "glass" displays presented on computer monitors. Taking advantage of the computing power means integrating the thousands of individual data points originally displayed with SSSIs into meaningful representations, or *information*. There is now increasing evidence that such computer supported "integrated", "direct perception", and "direct manipulation" displays can provide a very powerful method of reducing mental workload and supporting diagnosis [2], [3], [4], [5]. The strength of these configural displays is that they represent plant data at the appropriate level of abstraction so that this information matches the cognitive demands of the operators' tasks.

Ecological Interface Design (EID) is a recent theoretical design approach for rationally designing configural, computer-supported displays [6], [7]. A succinct description of the goal of EID is that an interface should support operator reasoning at different levels of abstraction by showing directly the system's governing constraints – both physics and physical – in a way that maps those constraints to geometries in the display. In so doing, the operator is better supported for dealing with both routine and non-routine events, including unanticipated system states [7].

EID typically involves integrated, direct perception, and direct manipulation displays. An integrated display is one where the values of several SSSI inputs are shown in a single display in such a way as to show their mutual interrelations [8]. Direct perception displays (e.g., ecological) allow operators to perceive the locus of the plant in state-space, without the use of complex calculations, steam table(s), etc., substituting pictorial displays for numerical displays [6], [9], [10]. Direct manipulation interfaces provide icons that represent controls, which can be manipulated by a cursor, mouse, or other input device. Such action results in direct acts on the actual physical components represented by the icons by means of the computer-plant hardware interface.

We believe that displays that represent the plant's various levels of abstraction, from physical components available for use to high level state-space relationships that govern the plant's dynamics, will greatly reduce the cognitive load on the operator and allow the use of perceptual rather than cognitive mechanisms to support monitoring and diagnosis, as well as fault management. In addition to providing a more direct perception of plant state, the use of carefully designed graphical displays can better support the correct use of standard operating procedures (SOPs). Instead of the enormous burden which text-based SOPs impose, a well-designed direct manipulation graphical interface can allow the operator to navigate through a sequence of operations with a greatly reduced attention load. Such an interface should greatly reduce the probability of i) misreading or misinterpreting written SOPs, and ii) losing one's place during navigation through the many tens or hundreds of pages required.

This paper presents an integrated suite of displays that adheres to the EID principles to support the start-up of a pressurized water reactor's (PWR) feedwater (FW) system from cold shutdown. Specifically, the displays are intended as a proof-of-principle to show that meaningful, complex displays can be designed based on the task requirements as outlined in SOPs, and that such displays support the cognitive demands of the operator's tasks better than written SOPs. The displays herein demonstrate the design approach and are not meant to represent a fully implementable interface for FW system control.

The suite of displays will not only support improved control rooms for NPPs, but will also have relevance to all large and complex industrial systems. In so far as these displays offer improved operator support, they will reduce human error and its consequences, lead to better fault management and hence greater safety, and promote greater productivity by increasing the efficiency of normal operation. The work is thus relevant to power generation, the management of chemical plants, nuclear waste processing, and the management of all large industrial systems whether hazardous or not.

2. A PHILOSOPHY OF DISPLAY DESIGN

Our philosophy is to integrate the information from SSSI sources so as to provide a coherent picture of system state that does not require the operator to perform elaborate cognitive operations on the data to determine what the state of the plant is. Rather than displaying SSSI information, a suite of displays directly reveals the plant's state in terms of the system and physics constraints that govern it. The operator should be able to perceive even the most complex relationships between variables because they are directly displayed on the screen. Furthermore, when operators must perform a sequence of operations over a period of minutes or hours, involving the manipulation and monitoring of many variables, the form of the display should lead the operator through the sequence without having to consult complex written operating procedures.

An obvious example of such a sequence is the start-up from cold shutdown procedure for a NPP. In this case hundreds of variables must be controlled and monitored over many hours. Control actions must be taken at appropriate moments. The plant must be continuously monitored to ensure that critical variables follow an appropriate trajectory towards the normal operating state, and above all that the values of the variables do not approach boundaries which are associated with hazardous plant states. The written SOPs for start-up run to several hundred pages, and require the operator to move backwards and forwards through different sections. The manuals do not in themselves provide a checklist facility for tracking progress, nor do they indicate that steps have been omitted, performed in the wrong order or at the wrong time, that wrong actions have been performed, *or* that the correct actions *have* been done. SOPs also do not incorporate system alarms. The proposed display architecture is an attempt towards achieving all of these features.

2.1. SOPs as a "Grammar" for Correct Behavior

We can conceive a computerized SOP design which is embodied in the plant interface. We can think of the entire sequence of operations as resembling a sentence, not of words but of behavior. Speaking grammatically requires one to place words in a correct sequence according to rules, so that the sequence of spoken words results in a sentence which can be understood by a listener. Similarly the performance of any long rule-governed sequence of actions results in a series of commands which can be understood by a plant where the architecture embodies the same rules. This is particularly true for PWR start-up procedures where systems must be brought together with tight tolerances on their own parameters and with respect to time. SOPs are an attempt to ensure correct rule-governed sequences of behavior. Similarly, a graphical interface should not only reinforce the correct sequence of behaviors, but should also prevent incorrect sequences, and provide constant feedback as to the state of the plant, and the operator's location in the overall start-up sequence. More generally, such an approach can also support normal operations and recovery from fault conditions.

2.2. Plant Start-up as the Construction of the Plant

If the start-up sequence can be thought of as constructing the plant from its components [2], then the level at which operators think about the plant becomes progressively more global and more abstract as start-up progresses. Operators simultaneously construct the plant and climb the "abstraction hierarchy" from the point of view of cognition [2], [11]. During start-up operators bring components to a state of readiness by switching them on, providing power, pre-heating them, bringing them up to speed, etc. Once the components of a subsystem have been appropriately configured, in general the operators no longer think of the components, but of the subsystem as a single unit [11]. Thus after closing a circuit breaker, operating a switch, and checking lubricating oil pressure and speed of rotation, an operator no longer thinks of those as individual parts or variables, but rather of "pump #123" as a single entity. A group of pumps, condensers, valves and heaters which have been all brought up to operating condition is thought of as "Feedwater System B", and so on. As the process of start-up continues, the operators' level of attention should switch appropriately, so that where details are no longer needed, attention is switched to the global properties of the system as a whole. The displays in a graphical direct manipulation interface should support the shift in thinking between levels of abstraction and aggregation as they occur.

Usually SOPs do not support this economy of intellectual effort and change in strategy. However, given the power of computer graphic interfaces, we believe that it can be done and at the same time will better support decision making by operators.

2.3. Construction of the Plant as a "Lattice" Diagram

The process of start-up can be represented conceptually by the inverted tree diagram (possibly better described as a "root" diagram) in Fig. 1. Although this representation is technically not a lattice, for the sake of brevity we will use the term lattice to describe it. The term "bird's foot" lattice [12] has been proposed for it from the obvious resemblance of the parts of the diagram to the feet, ankle and legs of a bird, with the structure being repeated at each level of abstraction.

At the bottom of the lattice is a row of inverted branches (or "toes"), each of which corresponds to a simple, single component of the plant (see "Parts" in Fig. 1). During plant start-up these parts are "aggregated" into subsystems by activating and connecting them, either physically or functionally. In the lattice representation, each joint (or "ankle") thus represents the fact that a subsystem has been configured and is beginning to run up towards its set point(s) as a result of the start-up procedure (e.g., "Processes"). When several such processes are running, and when required checks have been made to ensure that all is normal, they must be "aligned" with each other (to ensure synchronization, mass/energy balance, etc.). When several toes are collectively active, the ankle represents a complete functional unit, and the operator can now think in terms of connecting that functional unit to other completed units and details of the sub-units can be ignored. These functional units are now the toes of a higher level synthesis, and the process proceeds up and to the right towards the fully synthesized and fully functional normal operating conditions.

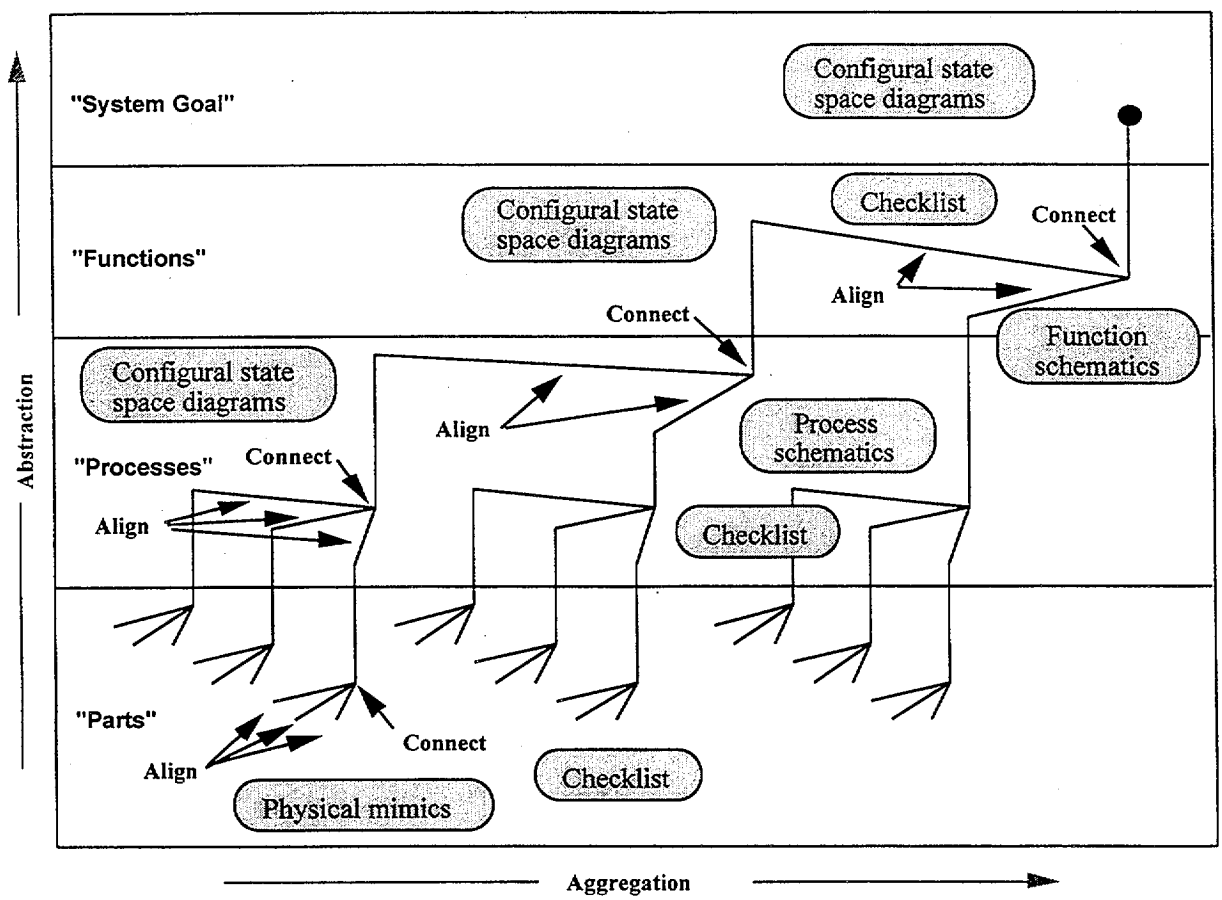


FIG. 1. The "lattice" that represents plant start up as aligning and connecting plant components and sub-systems. The types of displays that could be used to support the start-up procedure at the appropriate level of abstraction are indicated by the gray background.

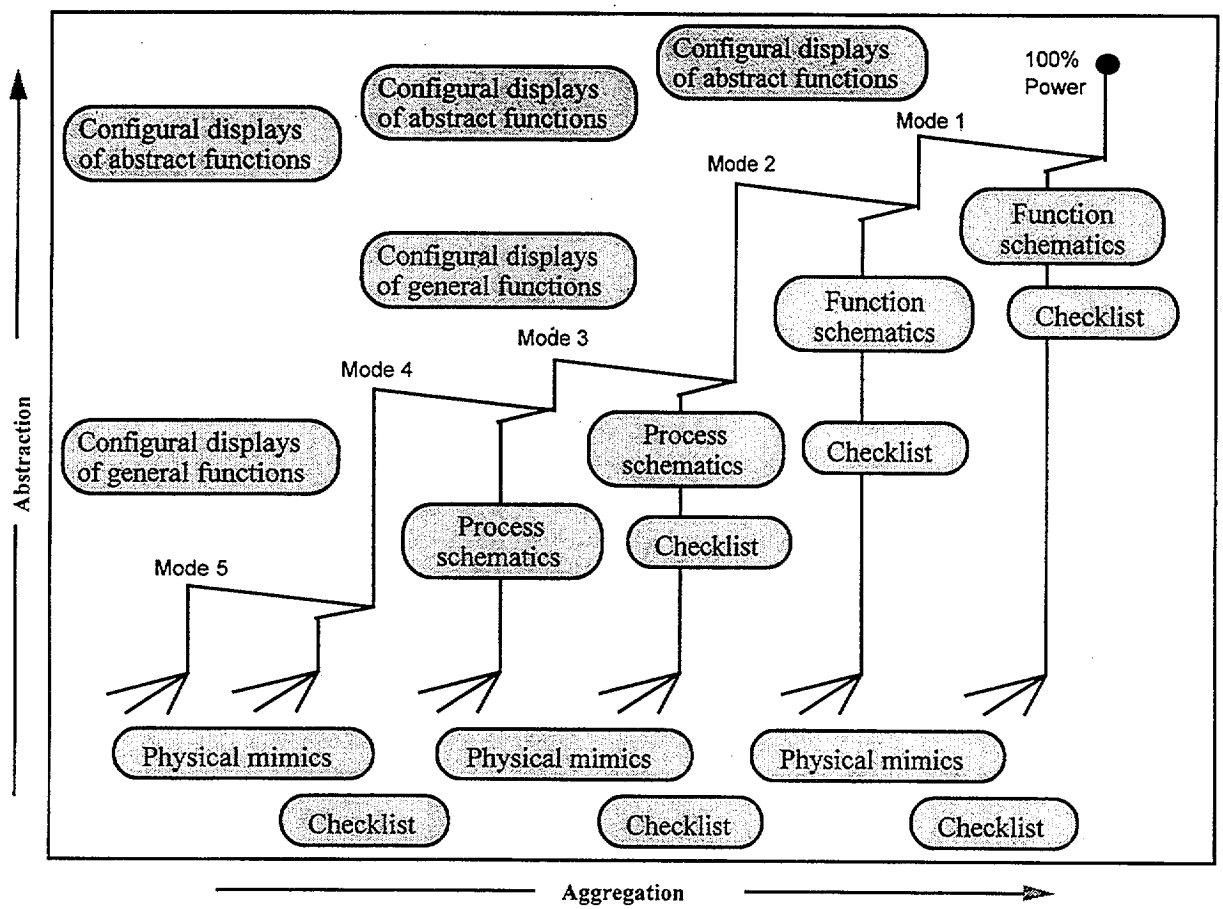


FIG. 2. A high level lattice representing the entire PWR start-up procedure.

3. GRAPHICAL SOPs WITHIN THE LATTICE ARCHITECTURE

This section starts by discussing PWR start-up in terms of the lattice structure just described. A proof-of-principle example on how the architecture was applied to PWR FW system start-up is then presented. The section concludes with a discussion of how the architecture may support fault management.

3.1. Overview of PWR Start-up with the Lattice Architecture

In terms of PWR start-up, the entire process can be summarized in lattice form. In Fig. 2 the lattice defines plant processes, functions, and states according to the industry-defined stable plant configurations, Modes 5 through 1. To develop the grammar for the behavioral sequence represented by a lattice, we note that the typical start-up flow charts accompanying the SOPs can be re-drawn so as to support a hierarchical representation of the task. The contents of operating procedures can be represented as a lattice in which the lowest branches are the names of the simplest components, and the top node is the plant running under normal conditions (see Fig. 2).The reader can imagine how the toes at the bottom of the lattice could represent the various steps required to move the plant from Mode 5 to Mode 4 to Mode 3 etc. Jones et al [13] present all start-up steps in a complete lattice.

The operator's task is to activate components and guide these components to their normal operating state by moving through the lattice, instead of having to read many pages of operating procedures. An operator will always be acting on individual components such as pumps, valves, switches, etc. Therefore, they need to be shown physical mimics of these components. In a direct manipulation display, actions on an icon on the screen result in changes in the object or process

represented by that icon. Hence, moving a control on the screen by means of a mouse replaces the use of a manual switch on a traditional control panel. The operator also requires configural state-space diagrams that show how the operator's action on a specific component is changing the new subassembly's or the whole system's performance in terms of their boundary constraints.

As a subassembly or process is completed (e.g., an ankle is formed), the mimics of the low level components and configural displays for lower level functions can be replayed by more global state-space diagrams. These higher level state-space displays redescribe the subassembly or process at its new functional level instead of in terms of the component settings, alignments, etc. Configural displays may be needed for both the generalized functions (i.e., pressure vs. temperature limits for the reactor coolant system) and the abstract functions (i.e., mass-energy balances on the PWR's secondary side [4], [14]). As the start-up procedure evolves, the displays for representing the procedures to the left of where the operator is in Fig. 2 will tend to be more configural and oriented towards functions and processes. Displays for procedures to the right of where the operator is in Fig. 2 will show component and subsystem mimics as well as configural displays showing the results of actions taken on the components or subsystems. However, the graphics should still allow operators to call up relevant mimics or functional schematics at each ankle to let operators use their expertise if unusual configurations are required to handle conditions not included in SOPs, thus coupling the intelligence of operators to the standard SOP and emergency operating procedure (EOP) designs. For example, if two out of four redundant pumps are required, and one does not start, the mimic diagram helps the operators to decide what steps to take to work around the problem. The lattice representation allows the operator to retrace a path from the current state down to the components which are connected to that state, so as to support manual intervention when required.

3.2. Example of the Lattice Displays for FW System Start-up

As a proof-of-principle we will describe a prototype interface for a PWR FW system start-up sequence that was the lattice diagram introduced above. Operators see a progressively integrated and abstract representation of the plant as they configure the plant for normal operation, but the computer system preserves information about a route back to detailed subsystem operation in order to support fault

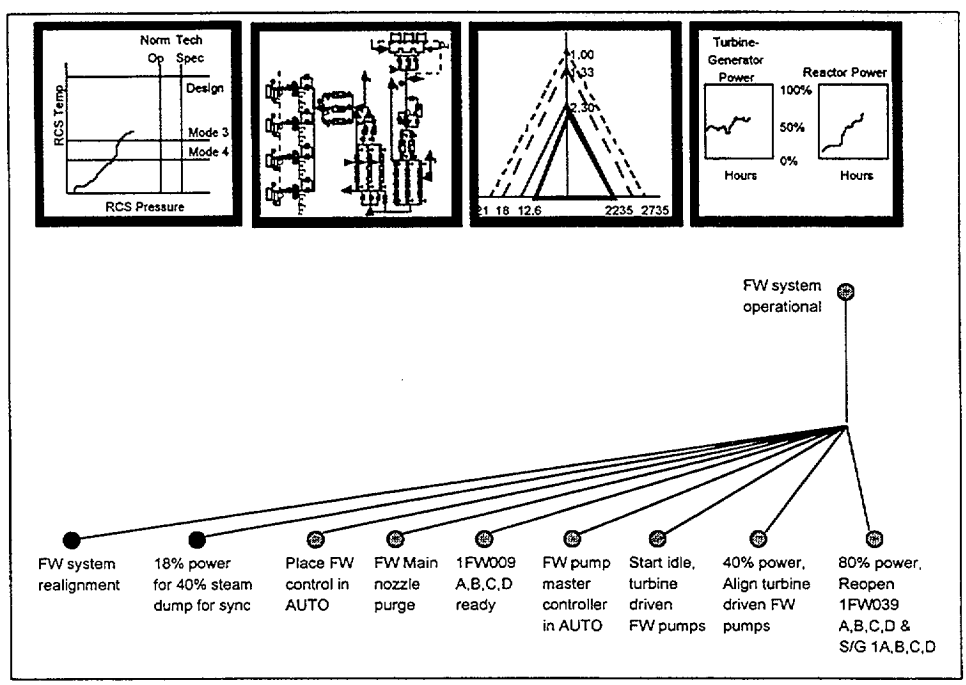


FIG. 3. A proof-of-principle overview display for FW system start-up, presenting the steps to be executed, in order from left-to-right, as well as configural state-space displays at the top.

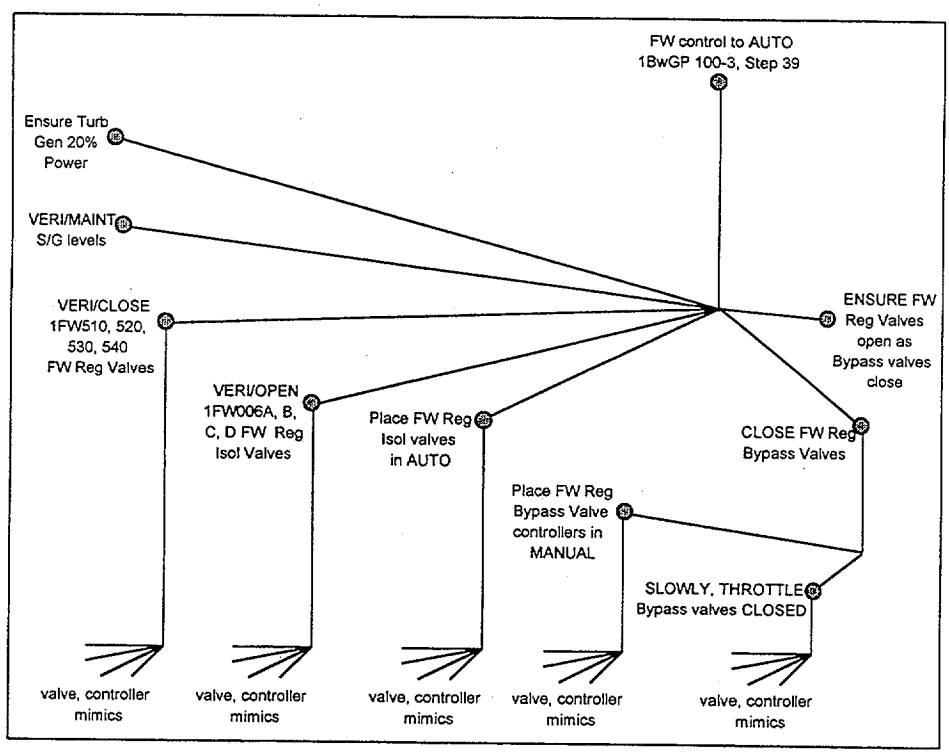


FIG. 4. The display for the "Place FW control in AUTO" node in Fig. 3.

1BwGP 100-3
Revision 6

FOR INFORMATION ONLY

```
**********************************************************
*                          NOTE                          *
*   FW pressure can be maintained greater than Steam     *
*   pressure by control of FW Pump Master Controller     *
*   in MANUAL.                                           *
**********************************************************
**********************************************************
*                          NOTE                          *
*   Step F.39. can be repeated as necessary to line      *
*   up flow to each loop.                                *
**********************************************************
```

F. 39. Placing Feedwater Control in Automatic:

a. ENSURE that the Turbine Generator is at approximately 20% power (235 MW).
b. VERIFY/MAINTAIN Steam Generator levels at or slightly above program level, by ADJUSTING the FW Reg Bypass Valve(s), as necessary.
c. VERIFY/CLOSE 1FW510, 520, 530, and 540, FW Reg Valves.
d. VERIFY/OPEN 1FW006A,B,C, and D, FW Reg Isol Valves.
e. With each Steam Generator's level at or slightly above the program level, PLACE the associated FW Reg Isol Valve in AUTO.
f. PLACE the FW Reg Bypass Valve controllers in MANUAL, and SLOWLY THROTTLE the Bypass Valves CLOSED.
g. ENSURE that the FW Reg Valves begin to open as the Bypass Valves are throttled closed.

FIG. 5. A illustration of a PWR's written start-up procedures for one step in bringing the FW system on-line.

management. The amount of detail displayed is always appropriate to the level of the current task because the display "knows" the causal path to the controls of relevant components at the physical level for both normal and abnormal operation. The suite of graphical direct manipulation displays developed here is an instantiation of the bird's foot lattice shown in Fig. 1, specialized for the FW system.

Figure 3 presents the highest level proof-of-principle interface for the FW system start-up. At the top of this interface, several configural state-space displays and a mimic (second from left) are presented to provide an overview of the system state. Start-up tasks are executed by clicking the mouse on the nodes in the display, from left to right following the standard English reading rule. Figure 3 indicates that the first two tasks, FW system realignment and 40% steam dump for synchronization, have been completed by the black nodes that would be colored green in the actual color display. This means that the next task to complete is to place the FW control in AUTO. An operator would click on the grayed node and be presented with Fig. 4. (Note: In terms of entire plant start-up, Fig. 4 shows what would be one "toe" in the Mode 1 alignment in Fig. 2.) Figure 4 corresponds to the portion of the written SOP presented in Fig. 5.

Figure 4 would then require the operator to click on the first gray node, Ensure Turb Gen 20% Power and view another display that would show turbine generator power in the form of a graph or trend chart. The operator would then be returned to the display in Fig. 4. The line and node for this step would now be colored green and the operator would click on the next gray node. A graphical display for the steam generator levels of all four steam generators would be presented, to which the operator may refer while completing the remaining steps. Next, the operator would click on the third node from the left and be shown the display in Fig. 6.

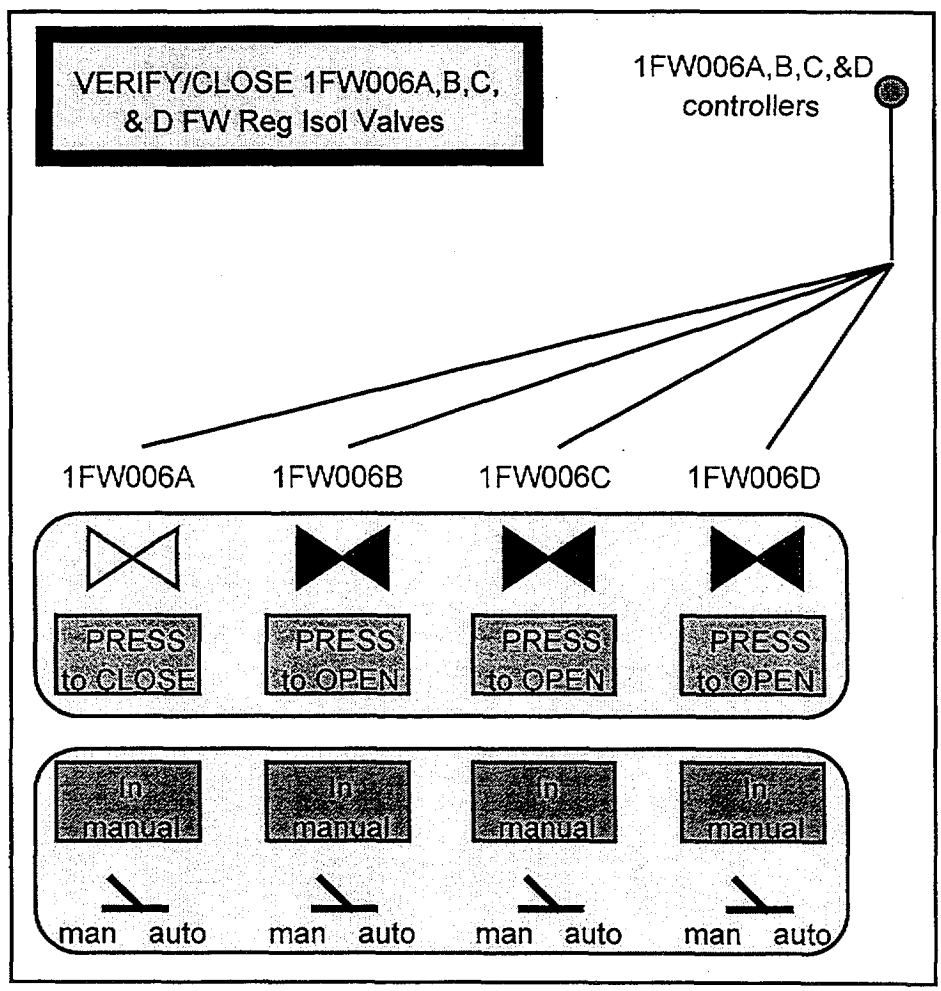


FIG. 6. The display for the "VERI/OPEN 1FW006A,B,C,D FW Reg Isol Valves" node in Fig. 4.

Figure 6 represents the lowest level information about the FW system, showing mimics of the valves and the "virtual" controllers. (Note: An alternative display could show these valves in relation to the rest of the FW system, in an expanded version of the mimic presented at the top of the display in Fig. 3.) The operator is presented with the display in Fig. 6 and reads the instructions in the highlighted box, and then directly clicks on the controller. In the present example, the operator has already opened

1FW0006A by clicking on the box that now says "PRESS to CLOSE". The operator can then see if this command has been executed by the valve icon above that box. This icon becomes outlined in green. Once all valves are open, all the valve icons are outlined in green, the lines leading to the top node are green, and the top node itself turns from gray to green. The operator is returned to the display in Fig. 4 where the "VERI/OPEN 1FW006A,B,C,D FW Reg Isol Valves" node is now colored in green. Once all tasks in Fig. 4 are completed, all nodes including the topmost node in Fig. 4 are colored in green and the operator is returned to Fig. 3, ready to move onto the next major FW system start-up task.

3.3. Supporting fault management

The lattice format can be used to support fault management during system start-up by using the nodes as alarms. For example, suppose that the operator is viewing Fig. 3, ready to start the step "FW pump master controller in AUTO," and an error arises with the 1FW006C FW Reg Isol Valve open/close setting. The "Place FW control in AUTO" node in Fig. 3 would turn red. The operator could then click on that node and be shown the display in Fig. 4. Figure 4 would have a red node at the "VERI/OPEN 1FW006A,B,C,D FW Reg Isol Valves" step. Clicking on this node would bring up Fig. 6 showing a red-filled 1FW006C valve, indicating that the valve has erroneously closed. The operator could then click the OPEN/CLOSE controller to reopen the valve.

4. CONCLUSION

There is widespread agreement among those working in high technology human factors engineering that displays using integrated information are more effective than SSSI displays, and empirical evidence is beginning to support this [2], [4], [15], [16]. On the other hand, there is a considerable art—despite the movement towards engineering approaches—in designing such integrated displays [17]. Therefore, before implementing a particular realization of these ideas, careful evaluation is needed, especially of failure modes. We believe that the notions of i) guiding the operator through SOPs by means of a graphical display rather than by means of vast, written text procedures, and ii) guiding the operators' thinking to the appropriate level of abstraction by means of the bird's-foot diagrams are both sound. However, to date this approach has not been realized in a real plant or a simulator. Furthermore, the ideas presented here are not meant to represent a fully implementable interface for FW system control but rather to demonstrate the theoretical design approach. More rigorous systems analyses need to be conducted, including field studies concentrating on how operators work together and adapt to the work environment and work artifacts.

The proposed set of graphics is particularly appropriate for the start-up sequence, passing from cold shutdown to full power. *It does not necessarily follow that the same set of graphics is appropriate for monitoring, detecting faults, diagnosing faults and managing faults once the plant is running.* Consider what the occurrence of a red node in the bird's foot diagram means. If it occurs in Fig. 4, then the natural thing to do is to click on it, back down to Fig. 6 and take appropriate action. It may be that one of the valves has failed into a different state, and this can then immediately be rectified—or at least the operator can go into manual mode to try to reset the valve and override the automatic controllers. But consider that will happen if a red node appears in the left-hand side of Fig. 2 under Mode 5, after Modes 5, 4, 3, and 2 are complete. Plant pressures and temperatures are now very high. It is not at all obvious that if we find a valve in an abnormal state upon following the trail of red nodes down the through lattice, all that is required is to immediately reset the valve. This might result in severe thermal or mechanical shock to some part of the system.

Two more major issues with the implementation of the lattice architecture that are related to each other are not addressed in this paper. The first issue is concerned with display "real estate." We believe that multiple computer monitors will be required to show the various mimics, configural displays, and overviews of the start-up procedure. We have not addressed how to arrange these various displays across the multiple monitors or how to assign priority to displays that could be replaced completely or partially covered in a multi-windowing environment. The second issue is that of visual momentum [18]. Visual momentum concerns how to make the transitions between displays in the lattice architecture seamless and still provide operators with the knowledge of where they are in the overall start-up procedure.

If the approach advocated here were to be developed, designers would have to take great care to ensure that only safe and appropriate routes are provided for operators to follow. This is possible if graphics are developed for all SOPs and EOPs, because plant designers and regulators believe that, by definition, the latter do provide appropriate paths for all situations. One approach is not to get rid of written SOPs and EOPs, but instead to make the SOPs available to the operators in a form which more effectively couples them to the psychological properties of the operators. The graphical displays would not only be as good as the written SOPs, but would also provide a broader envelope for the success of the SOPs because the displays show the connection between the activities and the system goals. The displays would go beyond the written procedures by not only preserving the integrity of the sequence of actions but by also showing the significance of those actions in relation to the system constraints and goals.

ACKNOWLEDGMENTS

Our thanks are due to personnel at the Commonwealth Edison Braidwood training facility for discussions and assistance.

REFERENCES

[1] WOODS, D. D., O'BRIEN, J. F., & HANES, L. F. (1987). Human factors challenges in process control: The case of nuclear power plants. In G. Salvendy (Ed.), *Handbook of human factors* (pp. 1724-1770). New York: Wiley & Sons.

[2] RASMUSSEN, J., PEJTERSEN, A. M., & GOODSTEIN, L. P. (1994). *Cognitive Systems Engineering*. New York: John Wiley & Sons.

[3] BENNETT, K. B., & FLACH, J. M. (1992). Graphical displays: Implications for divided attention, focused attention, and problem solving. *Human Factors, 34(5)*, 513-533.

[4] MORAY, N. P., JONES, B., RASMUSSEN, J., LEE, J., VICENTE, K., BROCK, R., & DJEMIL, T. (1993). *Development of a Performance Indicator for the Effectiveness of Human-Machine Interfaces for Nuclear Power Plants*. UILU-ENG-92-4007. Washington, D. C.: U.S. Nuclear Regulatory Commission. NUREG/CR-5977.

[5] VICENTE, K. J., CHRISTOFFERSEN, K., & PEREKLITA, A. (1995). Supporting operator problem solving through ecological interface design. *IEEE Transactions on Systems, Man, and Cybernetics, 25(4)*, 529-545.

[6] VICENTE, K. J., & RASMUSSEN, J. (1990). The ecology of human-machine systems II: Mediating "direct perception" in complex work domains. *Ecological Psychology, 2(3)*, 207-249.

[7] VICENTE, K. J., & RASMUSSEN, J. (1992). Ecological interface design: Theoretical foundations. *IEEE Transactions on Systems, Man, and Cybernetics, 22(4)*, 589-606.

[8] SANDERSON, P. M., FLACH, J. M., BUTTIGIEG, M. A., & CASEY, E. J. (1989). Object displays do not always support better integrated task performance. *Human Factors, 31(2)*, 183-198.

[9] FLACH, J. M. (1988). Direct manipulation, direct engagement, and direct perception: What's directing what? In *Proceedings of the Human Factors Society 32nd Annual Meeting* (pp. 1355-1358). Santa Monica, CA: Human Factors Society.

[10] FLACH, J. M., & BENNETT, K. B. (1992). Graphical interfaces to complex systems: Separating the wheat from the chaff. In *Proceedings of the Human Factors Society 36th Annual Meeting* (pp. 470-474). Santa Monica, CA: Human Factors Society.

[11] RASMUSSEN, J. (1986). *Information processing and human-machine interaction: An approach to cognitive engineering*. New York: North-Holland.

[12] MORAY, N., JONES, B., SANDERSON, P. M., REISING, D. C., SHAHEEN, S., & RASMUSSEN, J. (1995). The "bird's foot" integrated graphical interface for NPP operation. In Y. Anzai, K. Ogawa, & H. Mori, (Eds.), *Symbiosis of human and artifact* (pp. 995-998). Amsterdam: Elsevier. [*Proceedings of the Sixth International Conference on Human-Computer Interaction* (HCI International '95), Tokyo, Japan, 9-14 July.]

[13] JONES, B. G., SHAHEEN, S., MORAY, N., REISING, D. C., SANDERSON, P. M., & RASMUSSEN, J. (1996). *Development of advanced direct perception displays for nuclear power plants to enhance monitoring, control, and fault management*. Technical report submitted to the U.S. Department of Energy, Germantown, MD. Contract # DE-FG02-92ER75781.

[14] BELTRACCHI, L. (1987). A direct manipulation interface for water-based rankine cycle heat engines. *IEEE Transactions on Systems, Man, and Cybernetics*, *17(3)*, 478-487.

[15] VICENTE, K.J. , MORAY, N., LEE, J.D., RASMUSSEN, J., JONES, B.G., BROCK, R., & DJEMIL, T. (1996). Evaluation of a Rankine cycle display for nuclear power plant monitoring and diagnosis. *Human Factors*, *38(3)*, 506-521.

[16] WOODS, D. D., WISE, J. A., and HANES, L. F. (1982). Evaluation of safety parameter display concepts. *(EPRI NP-2239)*. Palo Alto, CA: EPRI.

[17] REISING, D. C. and SANDERSON, P. M. (1996). Work domain analysis of a pasteurisation plant: Building an abstraction hierarchy representation. In *Proceedings of the Human Factors and Ergonomics Society 40th Annual Meeting* (pp. 293-297). Santa Monica, CA: Human Factors and Ergonomics Society.

[18] WOODS, D. D. (1984). Visual momentum: A concept to improve the cognitive coupling of person and computer. *International Journal of Man-Machine Studies*, *21*, 229-244.

NEXT PAGE(S) left BLANK

XA9848578

IGENPRO KNOWLEDGE-BASED DIGITAL SYSTEM FOR PROCESS TRANSIENT DIAGNOSTICS AND MANAGEMENT*

J.A. MORMAN, J. REIFMAN, J.E. VITELA, T.Y.C. WEI
Argonne National Laboratory,
Argonne, Illinois

C.A. APPLEQUIST, P. HIPPELY, W. KUK
CRC/ComEd,
Chicago, Illinois

L.H. TSOUKALAS
Purdue University,
West Lafayette, Indiana

United States of America

Abstract

Verification and validation issues have been perceived as important factors in the large scale deployment of knowledge-based digital systems for plant transient diagnostics and management. Research and development (R&D) is being performed on the IGENPRO package to resolve knowledge base issues. The IGENPRO approach is to structure the knowledge bases on generic thermal-hydraulic (T-H) first principles and not use the conventional event-basis structure. This allows for generic comprehensive knowledge, relatively small knowledge bases and above all the possibility of T-H system/plant independence. To demonstrate concept feasibility the knowledge structure has been implemented in the diagnostic module PRODIAG. Promising laboratory testing results have been obtained using data from the full scope Braidwood PWR operator training simulator. This knowledge structure is now being implemented in the transient management module PROMANA to treat unanticipated events and the PROTREN module is being developed to process actual plant data. Achievement of the IGENPRO R&D goals should contribute to the acceptance of knowledge-based digital systems for transient diagnostics and management.

1. INTRODUCTION

Argonne National Laboratory (ANL), Commonwealth Research Corporation (CRC)/ComEd and Purdue University are collaborating together on a Joint Cooperative Research and Development Agreement Project [1] sponsored by the United States Department of Energy (US DOE). The focus of the project R&D is on the use of Artificial/Machine Intelligence (AI) techniques with on-line knowledge bases to provide real-time operator assistance during off-normal plant transient conditions. This advanced technology could improve the availability and reliability of water cooled nuclear power plants. The resultant knowledge-based digital system for process transient diagnostics and management is referred to as the IGENPRO package. Verification and Validation (V&V) goals [2,3] have been perceived as an important factor in the large scale deployment of such digital systems for plant transient diagnostics and management. Operator confidence in the V&V of such systems is crucial. The IGENPRO approach to this issue is to construct a generic plant- and thermal-hydraulic system-independent package. This would then, conceptually, limit the V&V requirements to a generic once-through qualification. This approach is analogous to that taken for the quantitative analysis thermal-hydraulic (T-H) codes such as RELAP-5 and TRAC where the generic Navier-Stokes equations are codified as a generic quantitative core knowledge base thus allowing a given T-H system from a given plant to be simulated as a configuration of generalized energy slabs/momentum junctions/mass volumes. The IGENPRO approach is to structure the knowledge database on the generic T-H first principles

*Work supported by the US Department of Energy, Office of Nuclear Energy, Science and Technology, under contract W-31-109-ENG-38.
**Instituto de Ciencias Nucleares, Mexico City, Mexico.

of mass, momentum and energy conservation and not use the conventional event-basis structure [1,4]. Thermal-hydraulic function and T-H component characteristics form the basis. This then allows for comprehensive generic knowledge, relatively small knowledge bases, and above all the possibility of T-H system/plant independence. The qualitative analysis IGENPRO T-H code would also have TRAC-like T-H system/plant independence. Universal V&V can then be performed on the core knowledge bases and application-specific V&V would only be required for the plant configuration database. All these attributes of the IGENPRO approach allow a simpler V&V effort.

The objective of the IGENPRO system is to diagnose on-line the onset of off-normal conditions, identify the component malfunction which caused the off-normal conditions and then recommend a sequence of operator actions which would best manage the off-normal conditions. However, the application of the package is not restricted to on-line usage. Given the novel non-event-based approach to the knowledge base structure, it could also be used off-line for root-cause analyses, the automated generation of procedures, the alignment design of thermal-hydraulic systems, operator training and perhaps predictive maintenance. In essence, off-line it could be utilized as an intelligent CAD tool to aid plant system engineers and design engineers. In the step-by-step phased approach to verification and validation (V&V) of this package it is envisioned that off-line usage would come first as a confidence building measure for ultimate on-line applications. Different parts of the package can be put to different usage thus implementing a phased approach to V&V. The next sections describe the general structure, approach and modules of the IGENPRO package.

2. IGENPRO APPROACH

Figure 1 shows the modular structure of the IGENPRO package. There are three modules in the Supervisory Module. The first module performs signal processing. Sensor/signal validation is performed before the plant instrument signals reach the IGENPRO package. The signal processing module PROTREN basically extracts signal trends from noisy signals. These signal trends are then used by the process diagnostics module PRODIAG to identify the malfunctioning component which initiated the transient off-normal conditions. Finally the last module, the process management module PROMANA, utilizes this diagnosis to recommend a sequence of operator actions which would best manage the off-normal conditions. The knowledge base structure shown in Fig. 1 is one where the "simpler" T-H knowledge is expressed in terms of IF-THEN rules encoded in an Expert System (ES); the more "complicated" T-H knowledge is encoded into a hierarchy of neural networks (ANNs) and finally the most "complex" T-H knowledge is encapsulated in a simulator code. We focus here on the ES and the ANNs. Interfacing will be developed in the future for the simulator. As mentioned in the introduction, the IGENPRO approach to the knowledge base

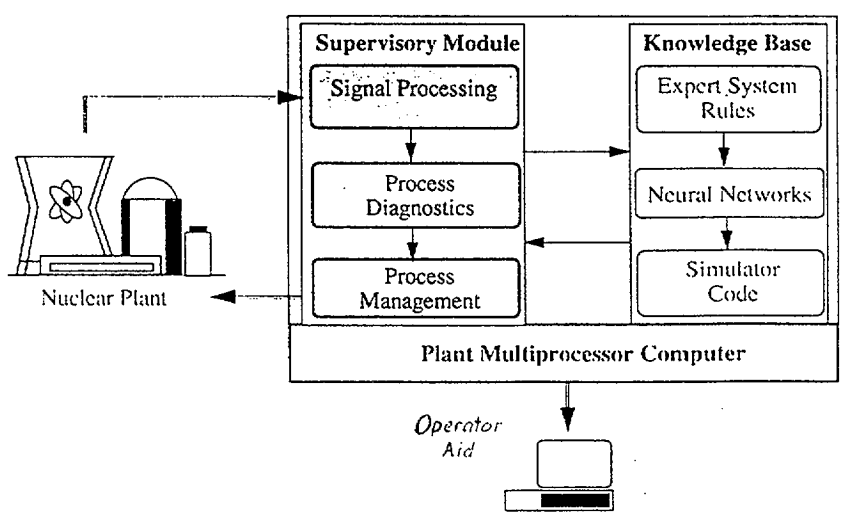


FIG. 1. IGENPRO Modular Structure.

structure is founded on generic first-principles T-H. Since the development of the PRODIAG diagnostics module is the most advanced of the three modules we discuss the approach in terms of the work on the diagnostics. But the same approach is also used for the PROMANA management module.

T-H phenomena play a major role with a wide range of behavior for many different fields of application. The physics of T-H is therefore a complex area. However there already exists a universal description of T-H regardless of the type of application. This is the mathematical description inscribed in the Navier-Stokes conservation equations with various equations of state and transport properties. This T-H knowledge base has to be translated into the language of AI using a few key general physical concepts if the generic T-H system independence is to be preserved. The mathematical description has to be transformed into the AI system of rules, representations and supervisory flow logic. If not, heuristics would inevitably creep in and render the concept of T-H system independence meaningless. This is a first-principles approach. To perform this transformation the IGENPRO approach is to translate the dynamic behavior first by decomposing the instrument signal history for each T-H variable into a first order trend and higher order frequencies. The three T-H conservation equations are then used, with qualitative analysis [1,5], in quasistatic form with the first order trends to compose spatial correlations across the T-H system. These spatial correlations are expressed in the form of IF-THEN rules and are therefore part of the ES shown in Fig. 1. They correlate changes in the three T-H functions of mass, momentum and energy to the signal trends and can be used in the localization of the component fault. Details are available in [6] and are summarized below in Section 2.1. Time windows [7] are used to broaden the validity of the use of the quasistatic conservation equations but in general the higher order frequency part of the signals is utilized in the hierarchy of ANNs shown in Fig. 1. This is where changes in component T-H characteristics, such as valve characteristics, are utilized to further sharpen the diagnostic focus. A method, denoted as the method of component characteristics [6], has been developed to help further localize the identification of the malfunctioning component. This is described in Section 2.2. Additional methods are being investigated to utilize other T-H component characteristics in this ANN part of the diagnostics. As one proceeds down the knowledge base shown in Fig. 1, invariably the diagnostic methods become more dependent on specific component data until the interfacing with the simulator is reached when T-H system dependent information such as volume sizes and tube heat transfer areas are crucial. But even so, in keeping with the non-event based approach the effort is focused at developing methods that do not require knowledge of the faulted component T-H characteristics. In summary the IGENPRO approach is a first-principles T-H function and T-H component-characteristics-based approach. The focus is to preserve the T-H system-independence by not requiring preknowledge of event-based signal data. While this discussion has focused on the PRODIAG diagnostics similar remarks can be made for the approach taken for the PROMANA transient management module.

2.1. T-H Function ES

Figure 2 illustrates the three types of knowledge of the proposed diagnostic ES and their corresponding usage, in a three-step mapping, that relates process symptoms into component faults [8]. When a process component fails, it causes the process T-H variables, e.g., pressure p, flow w, temperature T, and level L, to vary or trend from their expected values. The physical rules database (PRD) is used to map the trend in the T-H variables into imbalance trends in the three conservation types of mass, energy, and momentum, e.g., mass increase, momentum decrease. Then, the component classification dictionary (CCD) is applied to map the identified imbalance type and trend into generic faulty component types, e.g., pump, valve, heat exchanger, whose failure could have been responsible for the identified imbalance, i.e., the inadequate performance of one of the three T-H functions, mass transfer, energy transfer, or momentum transfer. Finally, the piping and instrumentation diagram (PID) containing the process schematics information, the only system-dependent portion of the knowledge base (KB), is applied to identify specific faulty components, e.g., pump A, valve CV-121, regenerative heat exchanger C, as the possible faulty component candidates.

This is a novel function-oriented first-principles-based concept for developing process diagnostic ESs that overcomes previous limitations of T-H system dependence. Except for the self-contained process schematics representation, the KB of the proposed system is process-independent, which allows for usage of the same diagnostic system with different processes and plants. This possibility not only decreases the effort involved in developing a new system, but it also eliminates the time-consuming process of KB

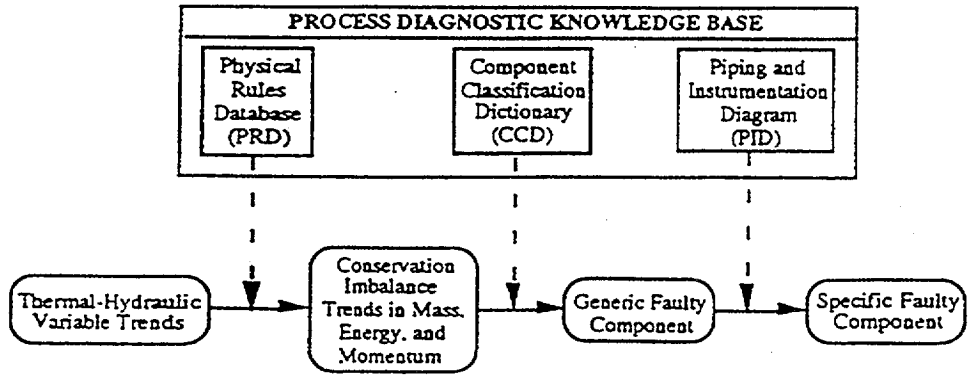


FIG. 2. Knowledge Base Structure of T-H Function ES.

verification and validation, which needs to be performed only once in the proposed approach. The process-independent diagnostic capability of the proposed ES is attained through the use of qualitative reasoning where a small number of values are taken to represent the values of continuous real-valued variables.

2.2. T-H Component Characteristics ANNs

We now turn to detailing the ANN implementation developed to this point for PRODIAG. It performs diagnostics at the plant level to supplement the ES diagnostics. The role of this plant-level ANN is to aid in the diagnosis of mass or momentum malfunctions through the use of component characteristics. We use here the momentum characteristics

$$\Delta p = f(w) = \text{pressure difference across component.} \tag{1}$$

We illustrate the use of the method of component characteristics for mass and momentum plant-level diagnostics with an open loop configuration [5]. For an open loop with two end conditions and no junctions, the quasistatic momentum equation is

$$p_1 - p_2 = f_1(w) + f_2(w). \tag{2}$$

The loop has been divided into two segments. Segment 1 has momentum characteristic $f_1(w)$ while segment 2 has momentum characteristic $f_2(w)$. Each segment's momentum characteristic is a combination of the component characteristics in the segment. The two end conditions are at pressures p_1 and p_2, respectively, and the flow is from p_1 to p_2. The flow w is measured in segment 1. Manipulating Eq. (2) gives us

$$(p_1 - p_2) - f_1(w) = f_2(w). \tag{3}$$

If there is a pressure transducer which measures the pressure p at the intersection of segments 1 and 2, then by Eq. (1) which is the definition of momentum characteristics, we have for segment 2

$$\Delta p = f_2(w) = p - p_2. \tag{4}$$

We also have from Eqs. (3) and (4)

$$\Delta p = (p_1 - p_2) - f_1(w). \tag{5}$$

If we plot Eq. (5) in Δp w space, we have a curve 1 which will intersect with a plot of Eq. (4) in Δp w space, denoted as curve 2. The intersection point is the operating point, as it gives the value of Δp and w in steady-state normal operation of the open loop. A momentum function malfunction in segment 1 alters the

momentum characteristic $f_1(w)$. This changes curve 1 in Δp w space. However, the momentum characteristic $f_2(w)$ does not change, so curve 2 remains the same. The operating point, therefore, moves along curve 2. If an ANN is trained to recognize curve 2, which is the component characteristic $f_2(w)$, then this ANN can be used to recognize momentum malfunctions in segment 1. However, mass malfunctions in segment 1 would also alter $f_1(w)$ so there would be an ambiguity in the diagnostic resolution. If the mass malfunction is in between the flow measurement and the pressure measurement, this would effectively also change $f_2(w)$, so the operating point would move off both curve 1 and curve 2. This type of diagnostic behavior in Δp w space allows the following conclusions to be drawn.

- No malfunctions → operating point does not move;
- Mass or momentum malfunctions in segment 2 → operating point traces out curve 1;
- Mass malfunction (upstream of w measurement) or momentum malfunction in segment 1 → operating point traces out curve 2; and
- Mass malfunction (downstream of w measurement) in segment 1 → operating point traces out neither curve 1 or curve 2.

With this representation of malfunctions, an ANN can be constructed to recognize the component characteristic combinations and, therefore, support the diagnosis of mass and momentum malfunctions at the plant level. No preknowledge of faulted component characteristics is required. This illustrates the PRODIAG ANN plant-level diagnostic technique for a model open loop configuration.

3. PROTREN MODULE

The primary function of the PROTREN module is to provide trending information to the diagnostic program PRODIAG. The module uses signal processing and fuzzy logic techniques for the purpose of classifying incoming signals into *increasing*, *decreasing* and *steady-state* categories which may subsequently be utilized by the diagnostic program PRODIAG. Usually, signal trending is performed in relation to the expected operating values of the signals monitored and with the use of various threshold parameters, such as, for example, thresholds for determining the onset of a transient or thresholds for obtaining a trend. In PROTREN, the signals are preprocessed and features signifying broad, but system-specific, fuzzy classes indicating signal direction are extracted. It is desirable, and certainly advantageous from the point of view of trend management, to obtain accurate trending information before the onset of various plant automatic control actions, which may mask the phenomena involved and somewhat complicate the successful realization of diagnostic tasks. Hence, successful trending is expected to be performed within appropriate time constraints and in a computational framework where reliability and accuracy objectives are balanced by speed and efficiency requirements; a situation that has called for the investigation and implementation of fuzzy techniques [9].

3.1. PROTREN's Overall Approach

Nuclear power plants are complex systems with numerous variations in the design and operation of their components and subsystems. They typically operate about a *steady-state*, such as full power, with any substantial deviation from such a state constituting a *transient*. Trending of plant signals helps to identify transients in a timely and reliable manner particularly if both general and specific characteristics of various signals can be captured in the right mixture and in a way that satisfies the overall computational economy of the problem. Flow and pressure signals, for example, tend to indicate plant trends in a much faster manner (since incompressible fluids are present); while temperatures and levels reflect processes with greater inertia and hence may indicate plant trends with considerable delay. On the other hand, flow and pressure signals tend to be noisier and hence may require more preprocessing to be performed for extracting significant features. Thus, trending tasks require taking into account the general nature of the signals under consideration as well as specific issues including, but not limited to, sampling rates, location of sensors, and steady state signal statistics.

For the purpose of correctly identifying transients via trends of relevant plant signals, the PROTREN module receives individual signals and processes them through three subsystems: *feature extraction*,

determination of expected values, fuzzification of trend. In feature extraction, a signal may be filtered or averaged in a moving-average sense to remove high frequency noise. From past data a detailed understanding of signal spectra is obtained and after determining expected values, error terms are formed by comparing expected with measured values. The fuzzification of trends calls for fuzzy rules (whose principal advantage is computing speed) for determining if there is a transient and if a trend is in the *upward, downward* or *about the same direction.*

3.2. Feature Extraction

The main purpose of feature extraction is to remove high frequency noise from the data and produce the most important features of the signal. It is assumed that the useful transient information is found in the low-frequency components of the signals [10]. Having built a detailed understanding of the nature of plant signals under consideration through off-line analysis, a filtering mechanism somewhat similar to that of an RC integrator which averages the data in a moving-average sense is used for removing the high frequency noise in online analyses. This simple approach is intended to facilitate meeting the overall diagnostic time requirements (e.g., less than 5s in the diagnostic system PRODIAG).

From historical data, the probability distribution functions (PDFs) or histograms of signals are obtained. The PDFs contain prototypical information about the nature of a signal which can be used as a reference during the online analysis. When new data arrives from the data acquisition system two features have been found to be significant: a *threshold* below which a transient may be likely and *how* the data clusters in certain regions of the PDF. For example, if the data is below the 0.1 level of the PDF or if it clusters around the 0.02 area, we have a situation possibly indicating the presence of an upward trend. At present we seek to automatically set the size of the appropriate time window for on-line filtering and feature extraction depending upon past experience and time constraints imposed by the larger time window within which transient identification decisions need to be made.

3.3. Determining Expected Values

For each signal, an error $e(t)$ can be formed by comparing *expected* with *measured* signal values. A quantitative measure of the error uncertainty (an error bar, $\Delta e(t)$) can also be obtained where an increasing error bar provides a strong indication that the observed signal is related to a transient with an upward direction. A stable error and an error bar criterion (e.g., $\Delta e(t)$ crosses the 0-axis at least 4 out of 6 times in the last six measurements) may be used to reliably identify *steady state*. In addition, a decreasing error may indicate a transient where the signal is going down. Thus trends of expected and measured values for a certain number of past time steps (e.g., the last six) can be compared and a decision can be made as to the direction of a transient, should one be present.

Currently an investigation is underway to reveal if there is any useful reliable relation between error bars and plant transients. An important question in this regard concerns the length of time for which historical data may be used, in other words, how many past values do we really need to use, e.g., 100 points or 5 points and with what type of weighting function to include them in trending calculations.

3.4. Fuzzification of Trends

The purpose of the fuzzification subsystem is to categorize a signal by placing it in one of the following signal classes: *increasing*, *decreasing* or *steady-state*. Several approaches are under investigation regarding this objective, including neural networks, fuzzy IF-THEN rules and sequential probability ratio testing (SPRT). Feedforward neural networks may be used to output the membership functions of the *increasing*, *decreasing* or *steady-state* classes directly through mapping incoming signals to membership function parameters. Determining the appropriate shape of membership functions for a number of important plant (or simulator) signals relies heavily on off-line analysis of historical data and the nature of the PDFs as described in Section 3.2. A self-organizing neural network may also be used for clustering errors and producing membership functions for the trend categories.

PROTREN's identification of trends requires quantified probabilistic uncertainty estimates and significant efforts to verify and validate its workings under all possible conditions. An advantage of fuzzy rules in this regard may be that no single item is used for making a decision, but rather there is built-in methodological redundancy that enhances the reliability of the overall system.

4. PRODIAG MODULE

The knowledge based structuring concepts have been implemented in the current laboratory-scale version of PRODIAG using Quintus Prolog for the following range of applicability: single-phase liquid plus noncondensible gas T-H systems; non-neutronic heat sources; coolants with bulk moduli and thermal expansion coefficients similar to water; single fault initiated transient scenarios; transient severity should be sufficient for instrumentation in single-phase liquid components to respond; use of instrumentation signal data which has been filtered for noise; and diagnostic window closure upon initiation of control action. To demonstrate the scale-up feasibility of the proposed diagnostic system it was developed for use with the Chemical Volume Control System (CVCS) of the Braidwood pressurized water reactor (PWR) plant. A full-scope operator training simulator representing the Braidwood nuclear power plant is being used both as the source of development data and as the means to evaluate the advantages of the proposed diagnostic system. One particular CVCS configuration for one specific operating mode was selected. This configuration is normal charging/letdown mode at 100% power. Simplifications were therefore made in the CVCS layout [6]. Only T-H signals, excluding the external systems measurements, are utilized and it should be adequate to treat a smaller set of local controllers. The full-scope Braidwood simulator malfunctions for CVCS operator training are used as the basis for the selection of the test matrix of transients. Each single-fault transient event was simulated for 40s, including 3s of null transient, starting from a steady-state normal mode of the CVCS operation. Initial results obtained by using the initial "first-principles ES" portion of the PRODIAG module to diagnose transient events were summarized in [1]. Additional ES validation results are reported here. The validation matrix consists of both semi-blind and blind testing. Some testing of the ANN representations was also performed.

A total of ninety-seven transients corresponding to twenty distinct single-component malfunctions have been simulated and used for testing. Thirty-nine out of the 97 transients were used to blind test the diagnostic system where the identity of the transient was not provided until after the analysis. Table 1 shows that, out of the 39 transients, 95% were correctly identified within the first 40 seconds into the transient with graded degree of accuracy, i.e., uniquely identified, identified as one of two candidates, etc. The remaining transients, with very mild severity levels, were not identified. Forty-nine % of the simulated transients are uniquely identified, 8% are identified as one out of two possibilities, 33% are identified as one out of three, 5% are identified as one out of four possibilities, and 5% are not identified. As discussed in Section 2, instrumentation failure should be detected by the classical techniques of signal validation. The two unidentified simulations refer to pressure transmitter failure which cannot be diagnosed. Overall, PRODIAG correctly diagnosed 95% of the transients with varying precision and did not identify 5% of the transients. No transients were misclassified. These results indicate that the PRODIAG system is a significant step in the direction of addressing the major limitations of existing AI-based advisory systems.

Testing of the component characteristics approach using ANNs developed for PRODIAG is shown in Fig 3. These results were obtained for the CVCS configuration discussed previously. The ANN representation is designed to address the plant-level diagnostics question of whether the malfunction is a mass or a momentum imbalance. The method of component characteristics discussed in Section 2.2 is used to give

TABLE 1. SUMMARY OF PRODIAG BLIND TEST PERFORMANCE

Uniquely Identified	2 Possible Candidates	3 Possible Candidates	4 or more Candidates	Incorrect Diagnostics	No Diagnostics
49%	8%	33%	5%	-	5%

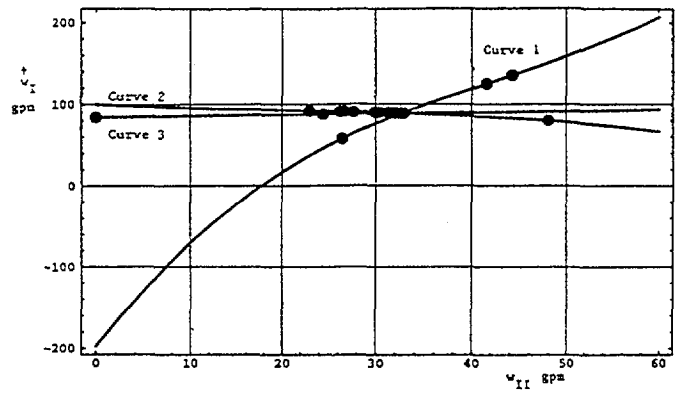


FIG. 3. Test of ANN Representations for CVCS Seal Loop Malfunctions.

curves 1-3 in w_I w_{II} space with each curve corresponding to a certain set of malfunctions. Details are available in [6]. The w_I flow is the charging pump discharge header flow and the flow w_{II} is the pump seal injection flow. Figure 3 shows the actual data from the set of testing transients as dots. It can be seen that the group of dots do actually congregate around the set of three curves in w_I w_{II} space. The fact that the transient data does group around the predicted three curves shows that the method of component characteristics is a valid one. ANNs trained to associate particular mass or momentum failures in various flow segments with curves 1-3 were tested for various transients. In every case, the correct diagnosis was provided.

5. PROMANA MODULE

PROMANA, the transient management module within the IGENPRO system, is a logical extension of the PRODIAG module. Once PRODIAG has identified a fault in a process system, the same first-principles approach is applied to that process system to identify corrective actions that will mitigate the fault situation. Most, if not all, advisory systems that have been developed, or are under development, are designed for a specific plant system. PROMANA is intended to be a generic code that can be applied to many different plants without the need for major revisions of the computer code and the associated requirements for verification and validation of the modified code. Specific plant operating parameters and configurations are contained in a separate database that is linked to the main body of the code.

To determine the set of operator actions needed for T-H system realignment in response to a component malfunction requires an alternate flow-path search through the T-H system loops. A primary goal of the PROMANA module is to not restrict the solution to a predefined set of alternate flow paths which is based on an assumed fault. The PROMANA approach is to consider all possible ways to interconnect various segments of a system or even multiple, connected systems. After studying representative system flow diagrams, it became clear that the only approach consistent with this goal was to base the solution on a junction-segment description of the system. PROMANA thus assumes that any system can be described by a series of interconnected flow segments, each defined by one inlet and one outlet junction. Each junction can have a number of segments attached to it (a current limit of three is imposed for development purposes). The relationships between the junctions and segments are stored in one of several database files used by the program.

The following steps outline the general solution approach taken in the PROMANA module after a failed component is identified.

- identify all safety-related components affected by the failure (forward search);
- develop a list of possible replacement flow paths made up of flow segments containing the replacement components (reverse search);
- search for replacement components (mass, momentum, energy function) that can provide the required source or sink of mass, momentum or energy to the safety-related components within the possible replacement paths;

- prioritize the possible replacement options based on calculated thermal-hydraulic parameters for these solutions; and
- verify that all high-level safety function requirements are met by the new configuration.

When a given component is identified as faulted, the segment containing that component is identified from the database. The search program is invoked in a forward-search mode, starting at the outlet junction of the failed segment. Following normal flow paths, all segments that are serviced (i.e., receive flow from) by the failed segment are located and stored in a table. Each of these loops is examined to see if it contains any safety-related components. These components are defined as those whose function is critical and must be maintained if the process or plant is to remain on-line, or whose function is necessary for the safety of the system. Starting from the inlet junction of any segment containing a safety-related component, PROMANA is then run in reverse-search mode to construct either (a) all loops than can deliver flow to the important component or (b) all loops that can function as a bypass around the failed segment. During this search, normally closed valves may be opened and segments whose flow may be reversed are included in potential paths. These are examples of the first-principles PRD rules and CCD T-H component generic attributes which are used in PROMANA. The same first-principles approach to the knowledge base structuring is taken in PROMANA as in PRODIAG but there are differences in the knowledge. The thermal-hydraulic parameters associated with each segment of the constructed paths are examined to see if they match or exceed those necessary to meet the requirements of the safety-related components. If the new path meets those requirements, it is added to a table of recommended alternate paths. Thermal-hydraulic calculations based on first-principle rules are used to prioritize the list of solutions, which is presented to the system operator as a guide to corrective actions.

6. CONCLUSIONS/SUMMARY

A knowledge base structure for the IGENPRO approach to knowledge-based digital systems for process transient diagnostics and management has been developed with the potential for generic T-H system independence. It is first-principles T-H function and T-H component-characteristics based and does not require preknowledge of the faulted event data. It is therefore not event based. Analogous to the approach taken for the numerical simulator codes such as RELAP and TRAC, the only plant and T-H system specific knowledge that is required is the connectivity information of the PID and the normal operating component characteristics. In this manner, V&V should become simpler with comprehensive generic knowledge and relatively small knowledge bases. On an application dependent basis, V&V should only be required for code input and not for the code itself.

This knowledge structure based on the combined use of a first-principles T-H function ES and T-H component-characteristic ANNs has been constructed for the PRODIAG diagnostic module. Implementation in the PRODIAG code has been completed for a laboratory proof-of-concept system. A set of first-principles qualitative physics-based ES rules and a supervisory flow logic which are plant and T-H system independent have been developed. While ANN training has to be T-H system specific, a set of ANN representations which could be derived by a plant- and T-H system-independent automated reasoning program, has also been developed. ES diagnostics proceed through a three-step mapping process, where trends in T-H variables are mapped into trends in imbalances of mass, energy, and momentum, which are then mapped into generic faulty components and next mapped into specific faulty components. The mapping from T-H variables to imbalances in the conservation equations is performed through qualitative physics-based rules. Unlike prior work describing the use of qualitative physics-based rules, the approach here is generic, with no need to customize the rules as a function of the process to be diagnosed. The proposed approach is T-H system-independent and can be applied to different processes and plants, with the provision of the appropriate process-specific piping and instrumentation diagram. Promising proof-of-concept testing results have been obtained with PRODIAG using CVCS transient test data provided by the Braidwood PWR full scope operator training simulator. The objective of generic portability appears to be feasible.

Given the progress made with PRODIAG diagnostics module, development of the knowledge base structure for the transient management module PROMANA has proceeded along similar lines. The three ES databases, the PRD, CCD and PID utilized by PRODIAG, are also used by PROMANA but there are

differences in the knowledge which is required. To determine the set of operator actions needed for T-H system realignment in response to a component malfunction requires an alternate pathway search through the T-H system loops. This is the basic goal of the PROMANA module. To perform this search with a generic T-H system independent method requires that the PROMANA knowledge-base structuring be at a very basic level, component-level structuring and not at a higher level, system-level structuring. This necessitates the usage of the generic component-level classification dictionary, the CCD and obviates the usage of a generic system-level classification dictionary, the SCD. This basic level classification is required because a system could simultaneously have any of the three T-H functions, mass, momentum or energy. In contrast it is simpler to classify the T-H function on a component level. Using the CCD structure puts the PROMANA on the same footing as PRODIAG. As with PRODIAG, in addition to T-H function, PROMANA also uses T-H characteristics (attributes both qualitative and quantitative). There are, however, differences in that the T-H attributes useful for transient management are not exactly the same as those useful for T-H diagnostics. There are also differences in the PRD rules. But in general, both PROMANA and PRODIAG use the first-principles IGENPRO T-H function/T-H characteristics approach derived for the knowledge-base structuring. The PROMANA code system has been developed to the point where it is now possible to automatically construct all possible flow paths leading from a failed component, examine those paths for the presence of important components, then automatically search the system for all potential flow paths to restore the function of the failed component.

Work is continuing on performing a blind-blind test of PRODIAG with simulator data for the Braidwood Component Cooling Water System. Effort is proceeding on the PROMANA module with the focus also on the Braidwood CVCS. PROMANA will interface with a simulator code to meet quantitative limits from technical specifications and a probabilistic risk assessment code to provide risk and reliability screening criteria. Proof-of-concept-testing will involve comparisons with the CVCS Abnormal Operating Procedures. Braidwood CVCS operating plant data is being used to both develop and test the PROTREN module. Fuzzy logic will be used. Achievement of the IGENPRO R&D goals should contribute to the acceptance of knowledge-based digital systems for plant transient diagnostics and management. Since these goals include T-H system and plant independence this R&D effort would be ideally suited for international collaboration across national reactor plant lines. An international collaborative project à la the NRC ICAP program for RELAP-5 and TRAC, but at an earlier project stage than ICAP, would be promising if focused on the shared development of first-principles T-H knowledge bases using the unique experiences of the worldwide community of reactor safety analysts and engineers.

ACKNOWLEDGMENTS

We wish to thank Tom Chasensky and Mike Biegel of the Commonwealth Edison Braidwood Station for providing their full support. Acknowledgment is due to Judy Wozniak for her careful typing of this paper.

REFERENCES

[1] REIFMAN, J., WEI, T.Y.C., ABBOUD, R.G. and CHASENSKY, T.M., "Cooperative Research and Development for Artificial Intelligence Based Reactor Diagnostic System" (Proc. American Power Conf., Chicago, Illinois, April 25-27, 1994) 365-370.

[2] BERNARD, J.A. and WASHIO, T., *Expert Systems Applications Within the Nuclear Industry*, American Nuclear Society, Chicago (1989).

[3] KIRK, D.B. and MURRAY, A.E., "Verification and Validation of Expert System for Nuclear Power Plant Applications," Technical Report EPRI-NP-5978, Electric Power Research Institute, Palo Alto, California (1988).

[4] REIFMAN, J., BRIGGS, L.L. and WEI, T.Y.C., "Nuclear Power Plant Diagnostics Using Qualitative Analysis and Component Functional Classification" (Proc. Frontiers in Innovative Computing for Nuclear Industry, Jackson, Wyoming, September 15-18, 1991) 227-236.

[5] DE KLEER, J. and BROWN, J.S., "A Qualitative Physics Based on Confluences," *AI*, (1984) 24, 7.
[6] REIFMAN, J., WEI, T.Y.C., VITELA, J.E., APPLEQUIST, C.A. and CHASENSKY, T.M., "A Hybrid Artificial Intelligence Based Reactor Diagnostic System for Process Faults" (Proc. 6th International Conf. on Nuclear Engineering, New Orleans, Louisiana, March 10-16, 1996) 885-891.
[7] REIFMAN, J. and WEI, T.Y.C., "PRODIAG - Dynamic Qualitative Analysis for Process Fault Diagnosis" (Proc. 9th Power Plant Dynamics, Control and Testing Symp., Knoxville, Tennessee, May 24-26, 1995) 40.01-40.15.
[8] REIFMAN, J. and WEI, T.Y.C., "Systematic Construction of Qualitative Physics-Based Rules for Process Diagnostics" (Proc. 7th Portuguese Conf. on Artificial Intelligence, Funchal, Madeira Island, Portugal) (1995a) 311-322.
[9] TSOUKALAS, L.H., UHRIG, R.E., *Fuzzy and Neural Approaches in Engineering*, John Wiley & Sons, New York (1997).
[10] UHRIG, R.E., *Random Noise Techniques in Nuclear Reactor Systems*, Ronald Press (now McGraw Hill), New York (1970).

NEXT PAGE(S) left BLANK

XA9848579

THE PASSIVE AUTOCATALYTIC RECOMBINER TEST PROGRAM AT SANDIA NATIONAL LABORATORIES*

T.K. BLANCHAT
Reactor Safety Experiments,
Sandia National Laboratories,
Albuquerque, New Mexico

A. MALLIAKOS
US Nuclear Regulatory Commission,
Washington, D.C.

United States of America

Abstract

Sandia National Laboratories (SNL) has developed systems and methodologies to measure the amount of hydrogen that can be depleted in a containment by a passive autocatalytic recombiner (PAR). Experiments were performed that determined the hydrogen depletion rate of a PAR in the presence of steam and also evaluated the effect of scale (number of cartridges) on the PAR performance at both low and high hydrogen concentrations.

Introduction

PARs are being considered by the nuclear power industry as a combustible gas control system in operating plants and advanced light water reactor (ALWR) containments for design basis events. PARs do not require a source of power; instead, they use a catalyst to recombine hydrogen and oxygen gases into water vapor upon contact with the catalyst. At low hydrogen concentrations, energy from the recombination of hydrogen with oxygen is released at a relatively slow (but continuous) rate into the containment. The heat produced creates strong buoyancy effects which increases the influx of the surrounding gases to the recombiner. These natural convective flow currents promote mixing of combustible gases in the containment.

SNL, under the sponsorship and direction of the U. S. Nuclear Regulatory Commission (USNRC), has conducted an experimental program to evaluate the performance of PARs. A PAR was tested at the Surtsey experimental test facility at SNL. The following describes the configuration of the PAR, the test facility, the instrumentation, the control and data acquisition system, the test conditions, and the test results and analyses.

PAR and Test Facility Description

The PAR test module was a scaled version of the prototype PAR that was developed and fabricated by NIS INGENIEURGESELLSCHAFT MBH (Hanau, Germany). Detailed tests and analyses were made in cooperation with the Battelle Institute, Frankfurt, and the Technical University, Munich [1]. Its development has been sponsored by the German utility, RWE Energie. The NIS/RWE PAR device contains flat rectangular cartridges filled with porous spherical ceramic pellets, which are coated with palladium. The large surface area of the palladium layer of the pellets acts on diffused gas molecules to recombine hydrogen with oxygen. Between the cartridges, the PAR device has open flow channels to allow heavier particles or aerosols in the atmosphere to flow through with little plugging of the cartridge and little fouling of the pellet surface.

*Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

The prototype PAR contained two rows of standard catalytic cartridges (44 cartridges per row) and had dimensions of 1 m by 1 m. The PAR test module (also manufactured by NIS) contained only one row of standard catalytic cartridges and could be assembled as either a 1/2 scale (44 cartridges), 1/4 scale (22 cartridges), or 1/8 scale (11 cartridges) PAR by removing cartridges and using smaller (length) front and back panels. Note that the 1/2 scale PAR test module configuration has dimensions of ~0.5 m by ~1.0 m.

Figures 1 and 2 show that the PAR test module housing holds the catalyst cartridges in a vertical direction and guides the air flow. A vertical flow channel of about 1-cm spacing is formed between the cartridges. These flow channels (along with the PAR body or housing) define the flow area for convection of the heat generated by the heat of reaction. The PAR exit has a chimney with a free cross-sectional area equal to the cross-sectional area through the cartridges.

The catalyst material is inserted into rectangular cartridges (0.45 m length, 0.01 m wide, 0.20 m tall). The cartridges are filled with the catalyst pellets. The steel sides of the cartridges are perforated with many slot-like openings that allow gases to enter the cartridge and steam to exit. The catalyst is a palladium-coated (0.5 w/o) aluminum oxide pellet with a diameter of about 4-6 mm and a bulk density of ~0.5 g/cc. The porous oxide pellet provides a large inside surface area (~100 m^2/g) of palladium that allows a high conversion. A hydrophobic coating is placed on each pellet to minimize startup delays due to water, either from steam condensation or from containment sprays, on the catalyst surface.

Figure 3 shows the location of the PAR test module in the Surtsey vessel. The PAR was located at the vessel centerline, ~1 m above the midline elevation in the Surtsey vessel. Horizontal and vertical I-beams exist in the lower half of the Surtsey vessel but there are no I-beams located directly below the PAR. The Surtsey vessel is an insulated ASME-approved steel pressure vessel with a current working internal volume of 99 m^3. It has a cylindrical shape with removable, dished heads attached to both ends, and is 3.6 m in diameter by 10.3 m high.

Instrumentation, Control, and Data Acquisition

The most significant variables measured in the PAR experiments were: (1) the pressure and temperature in the Surtsey vessel, (2) the gas constituents and steam concentrations, (3) the PAR pellet and channel gap temperatures, (4) the flow velocity through the PAR, and (5) the amounts of hydrogen and oxygen injected into the Surtsey vessel. A personal computer (PC)-based data acquisition system (DAS) was designed to control and monitor the course of the test in real-time. The DAS provided instantaneous readouts of the temperatures of the cartridge pellets and corresponding cartridge air gaps, Surtsey vessel pressure, temperatures, and gas concentrations, and valve positions for steam, hydrogen, and oxygen additions. In addition, the DAS controlled the hydrogen target concentration and gas addition interval. This allowed changing the test conditions (during the course of a test) based on real-time test results.

Four pressure transducers were used to measure the pressure in the Surtsey vessel. The gas temperature in the Surtsey vessel was measured with twenty thermocouples installed in two rakes. The two thermocouple rakes (10 thermocouples each, 1-m spacing) were installed vertically in the vessel; one rake at the vessel centerline (array A) and one rake (array B) located about 0.32 m from the vessel wall. In addition, thermocouples measured the Surtsey wall temperature and the injected oxygen, hydrogen, and steam temperatures. Steam was mixed with the oxygen and/or hydrogen during each gas injection to minimize steam condensation.

A real-time gas mass spectroscopy (GMS) system was used to determine the concentrations of nitrogen, oxygen, and hydrogen in the vessel at four sample points. The four sample points were

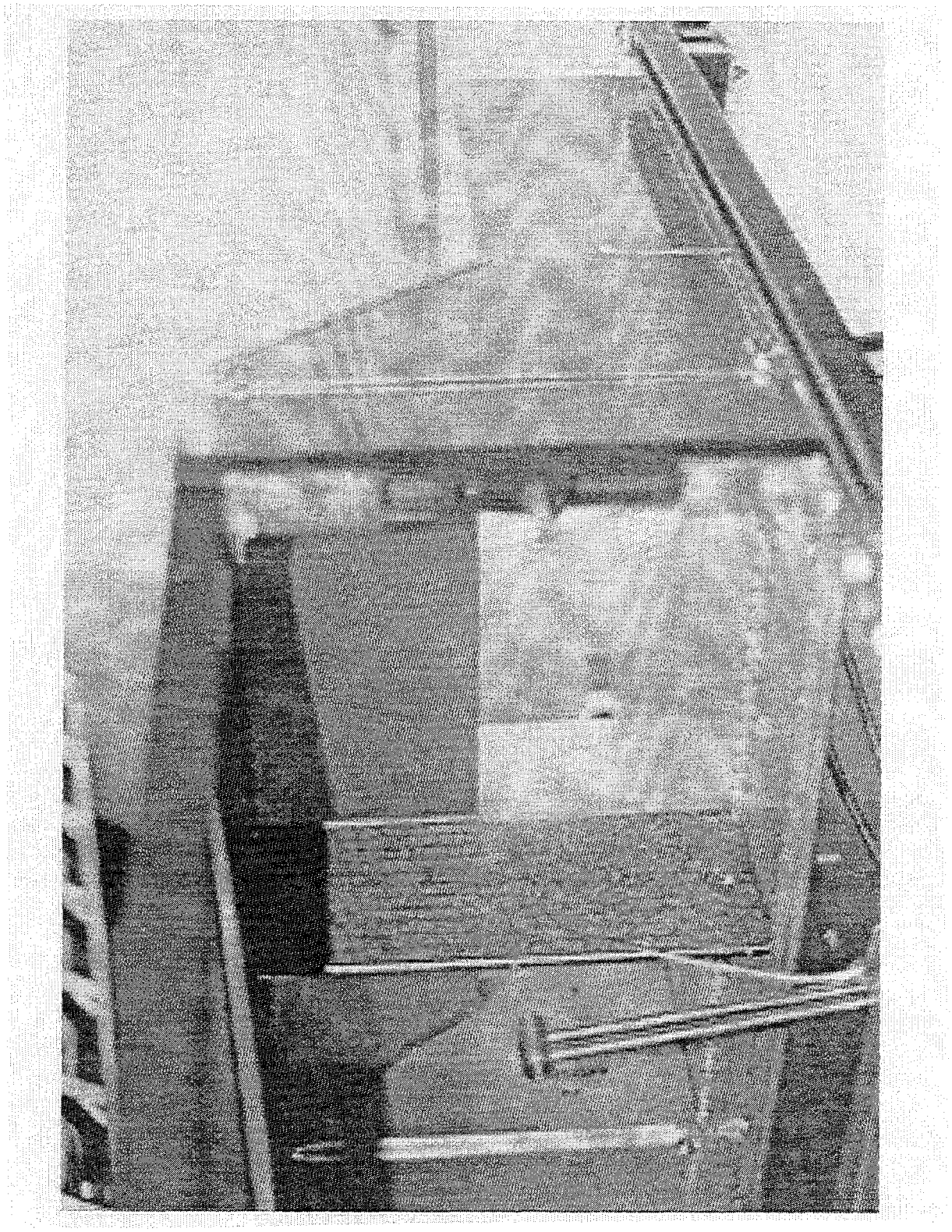


Figure 1 Bottom view of the PAR housing and chimney with one cartridge

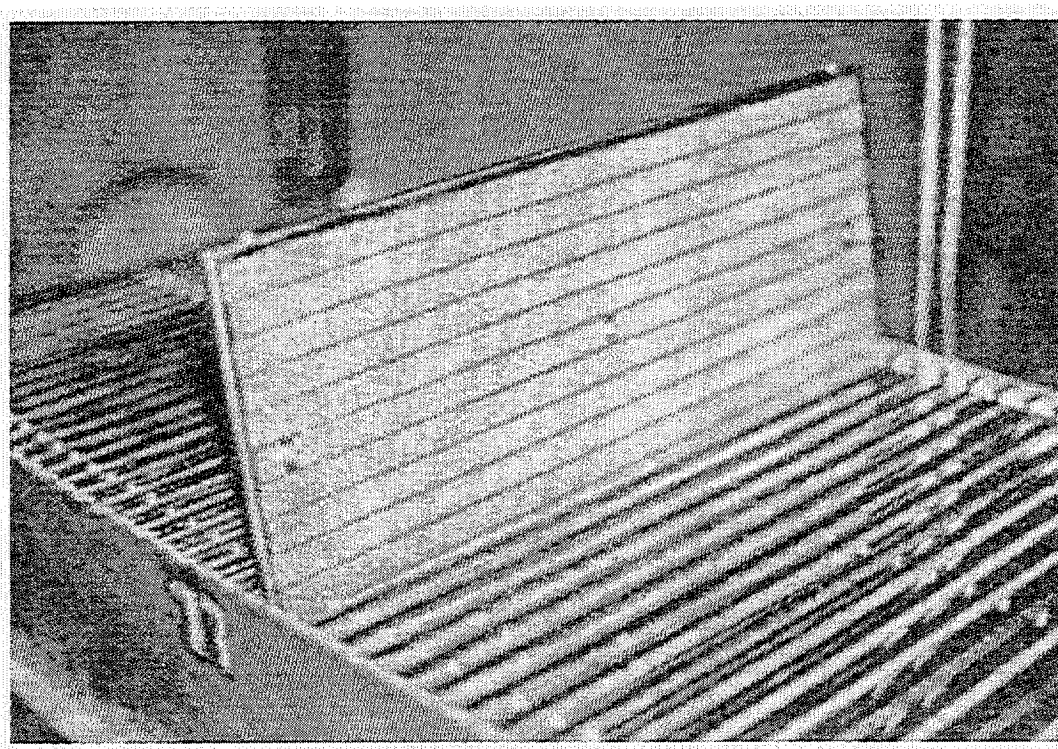


Figure 2 Cartridge held in a vertical configuration by the PAR housing

at the PAR inlet, the PAR outlet, high in the vessel near the dome, and low in the vessel near the floor. Gas grab samples were used as an independent verification of the gas composition.

A color camera and an infrared (IR) camera were mounted on Surtsey ports and viewed the PAR through tempered glass windows. In addition to the digital camera, an infrared camera also viewed the PAR through a different level 5 port. The cameras could see the PAR exit (top of the chimney) and provide visual evidence in the event of a deflagration event. Other instrumentation included a hygrometer to measure relative humidity and pitot-tube differential pressure transducers and a hot-wire anemometer to measure the velocity of the gas at the PAR inlet and outlet.

Twelve thermocouples monitored the catalyst temperature at three cartridge locations; PAR middle (and a PAR middle backup), PAR edge, and PAR corner. Three vertical positions for temperature measurement were monitored at each location (2-cm from the bottom, middle, and 2-cm from the top). These thermocouples were inserted into the cartridges and surrounded by the catalyst pellets. Twelve thermocouples monitored the temperature of the gas in the gap between the cartridges and were located opposite of the catalyst thermocouples. Four thermocouples monitored the PAR inlet temperature. Two thermocouples were located at the centerline middle and two were located at the centerline edge (within 2-cm of the PAR bottom). Four thermocouples monitored the PAR outlet temperature. Two thermocouples were located at the centerline middle and two were located at the centerline edge (within 2-cm of the chimney exit).

The hydrogen and oxygen gas was supplied to the vessel from separate manifolds. Standard 44 liter compressed gas cylinders were installed on the manifolds. In the tests that involve a prototypic air/steam atmosphere, the cold gas entering the vessel was mixed with an appropriate amount of steam (capable of heating the cold gas to saturation temperature) using a diffuser/mixer pipe that was located near the floor of the vessel. This was necessary to prevent

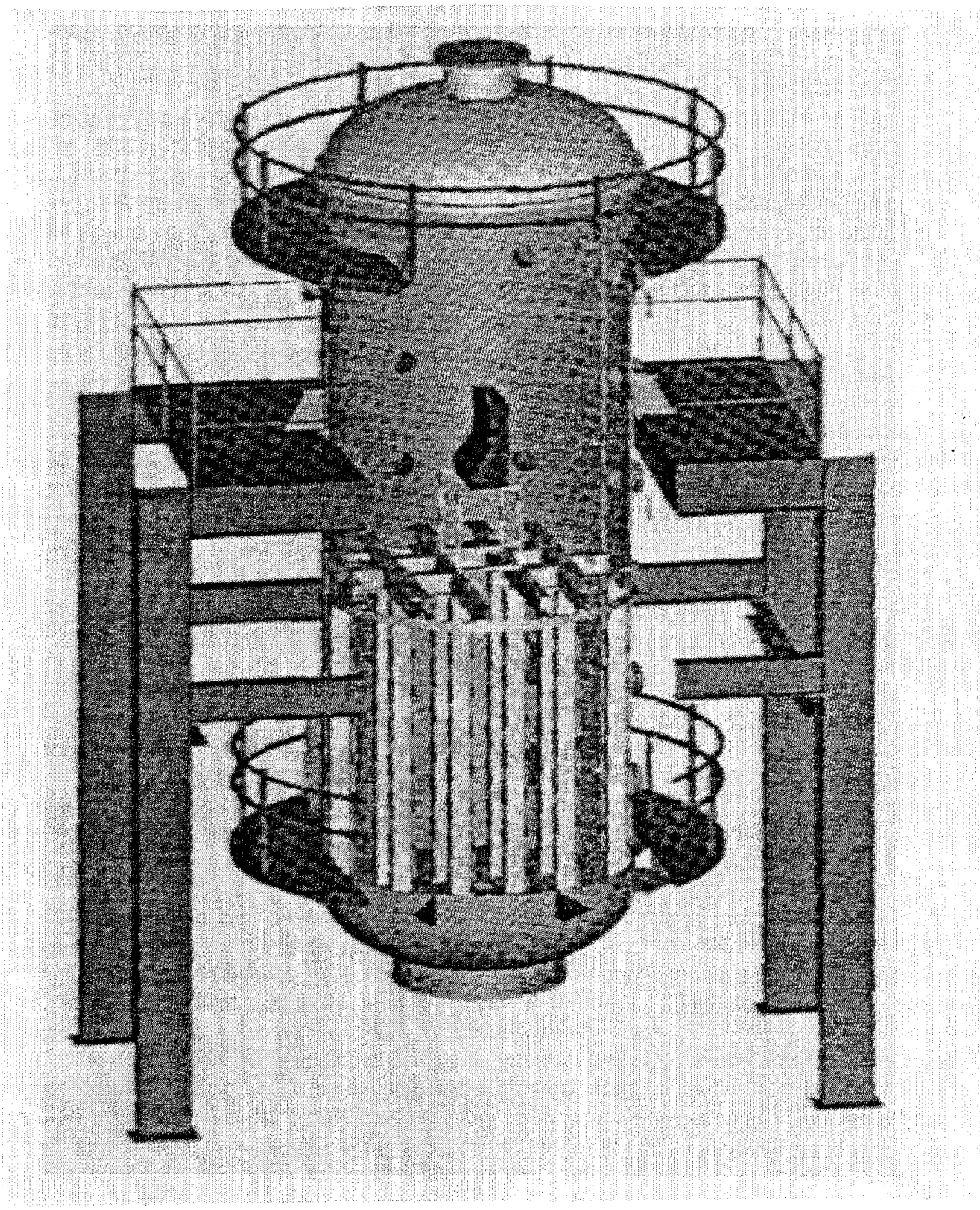


Figure 3 PAR location in the Surtsey vessel

condensation of the steam. Mass flow controllers were used to provide precise metering of the hydrogen and oxygen into the vessel. Two mixing fans were installed in the vessel. They were located on opposite sides of the PAR at the openings of the I-beam lattice; one pointed upward and one pointed downward. The fans were usually operated when hydrogen was injected and prior to taking gas grab samples to ensure that the containment atmosphere was well mixed.

Gas Composition Measurements and Analyses

The GMS system cannot measure gas concentrations in the presence of steam; a dry sample must be presented. In order to achieve this, a condenser and condensate trap (and heated gas inlet lines) were installed on each gas measurement line. This yielded dry-basis gas concentrations; however, to determine wet-basis gas concentrations, the steam fraction must be known. A hygrometer was used to determine the relative humidity (RH). The steam concentration was then calculated from the ratio of saturation pressure to total pressure times the RH fraction. The saturation pressure of steam was determined from saturated steam tables using the vessel average gas temperature.

Test Matrix

Six depletion rate tests using a scaled PAR were conducted. PAR performance at low hydrogen concentrations was determined at 1/2 scale, at 1/4 scale, and at 1/8 scale. NIS states that the hydrophobic coating is probably destroyed when the PAR catalyst exceeds temperatures of about 473 K. The PAR catalyst would reach these temperatures at about 2% H_2 in cold dry air and about 1% H_2 in a 50 mole % air/50 mole % steam environment at 0.2 MPa. These tests were performed at hydrogen concentrations that would not destroy the hydrophobic coating.

Three repeat tests (at 1/2 scale, at 1/4 scale, and at 1/8 scale) were performed at relatively high hydrogen concentrations which yielded the scaled performance data and completed the scaled depletion rate test series.

Experimental Results

The scaled depletion rate tests started with a mixture of 0.107 MPa of air and 0.107 MPa of steam, for a total pressure of about 0.21 MPa. To achieve these conditions, the vessel was sealed with about 0.083 MPa of cold air inside (one Albuquerque atmosphere at about 293 K). The Surtsey vessel was then heated internally by adding steam to obtain a gas temperature of about 375 K. At a temperature of 375 K, the air and steam partial pressures become equal.

Two observations can be made regarding most of the PAR tests. An evident depletion rate (startup) was achieved by the PAR within 10 minutes in hot, steamy atmospheres when exposed to hydrogen concentrations in the range of 1 to 6 mole %. The second observation was that at steady-state operation the PAR appeared to generate a convective flow loop in the Surtsey vessel from the PAR outlet to the dome, down the Surtsey wall (until reaching the height of the PAR inlet), and then returning to the PAR inlet; as indicated by both the hydrogen concentration and the vessel gas temperature measurements. Since the convection flow pattern did not extend to the lower half of Surtsey vessel, the vessel was not completely well-mixed by the PAR during steady-state operation. The hydrogen concentration from the sample point located near the floor always showed a higher concentration when measurements were taken after the last addition, as compared to the other sample points. This indicated that the depletion below the PAR near the floor was lower than that in the upper half of the Surtsey vessel. Also, the convective loop appeared to be driven further downward into the lower half of the Surtsey vessel in those tests with the higher hydrogen concentrations and hence higher PAR temperatures.

A test with the PAR configured at 1/8 scale provides an example of a PAR performance test. The Surtsey vessel was sealed and pressurized with steam to about 0.21 MPa. The initial gas

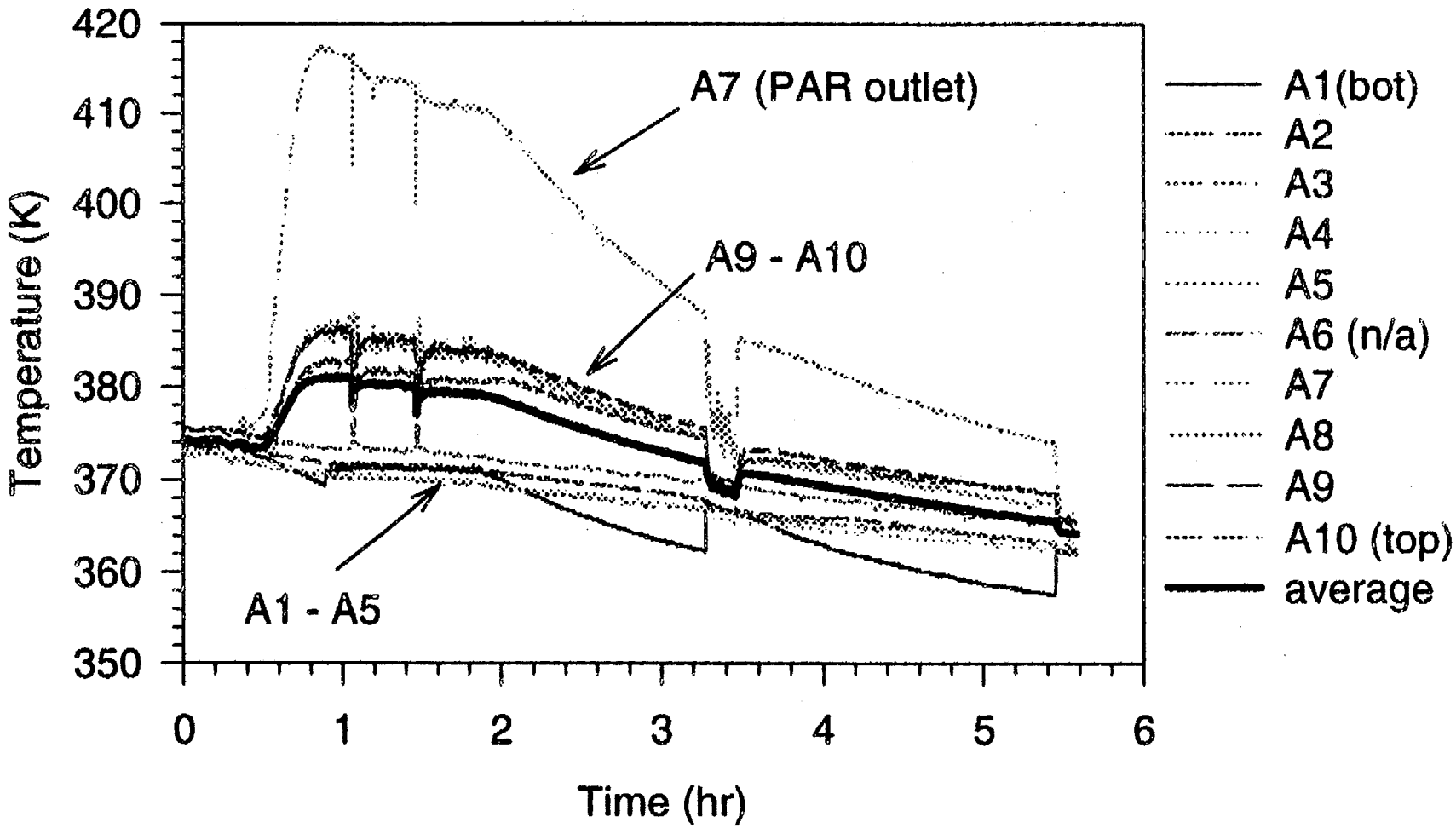


Figure 4 Centerline gas temperatures with 1/8 scale PAR

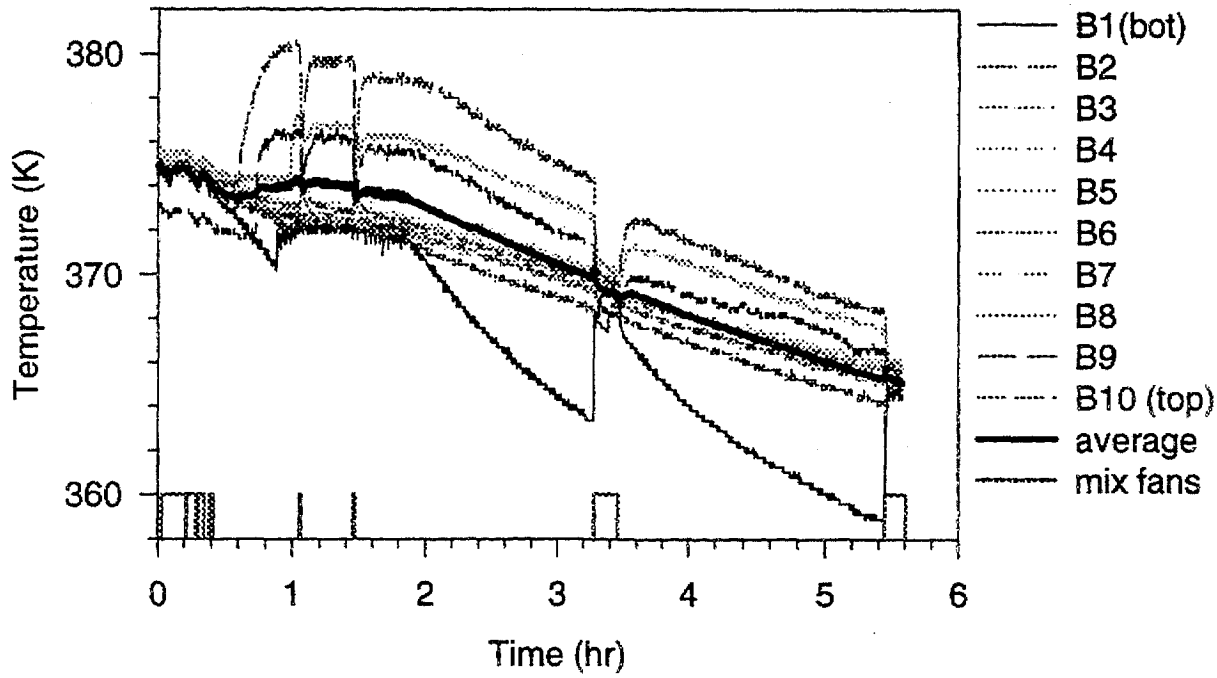


Figure 5 Wall gas temperatures with 1/8 scale PAR

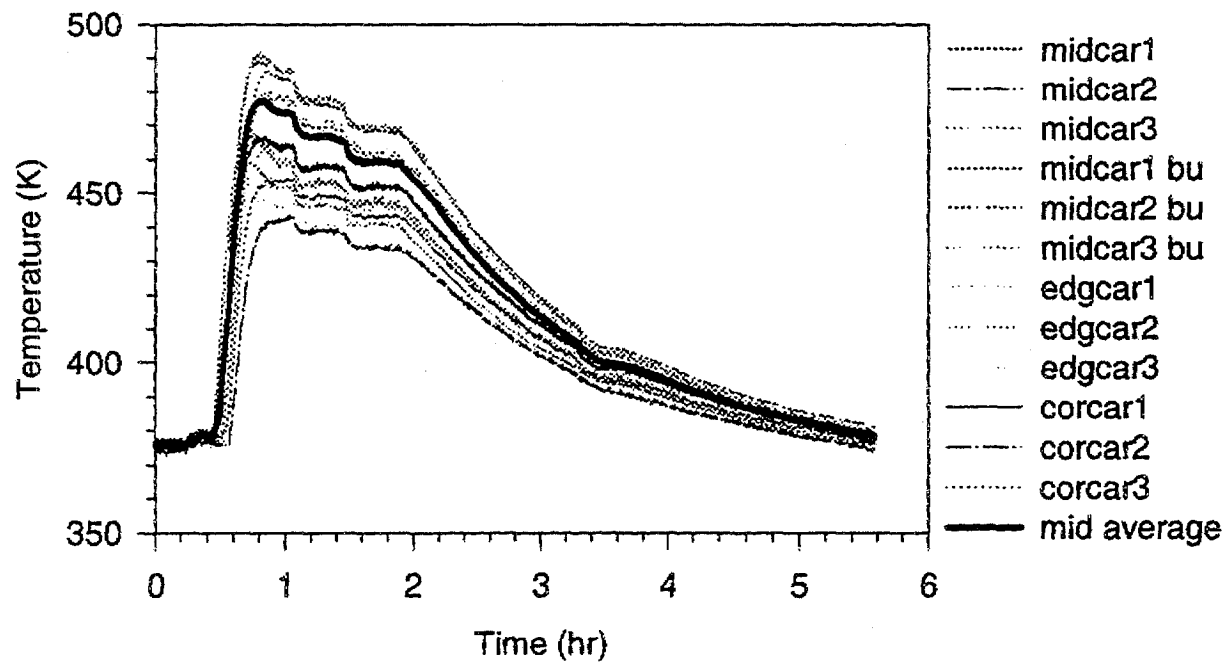


Figure 6 Catalyst cartridge temperatures with 1/8 scale PAR

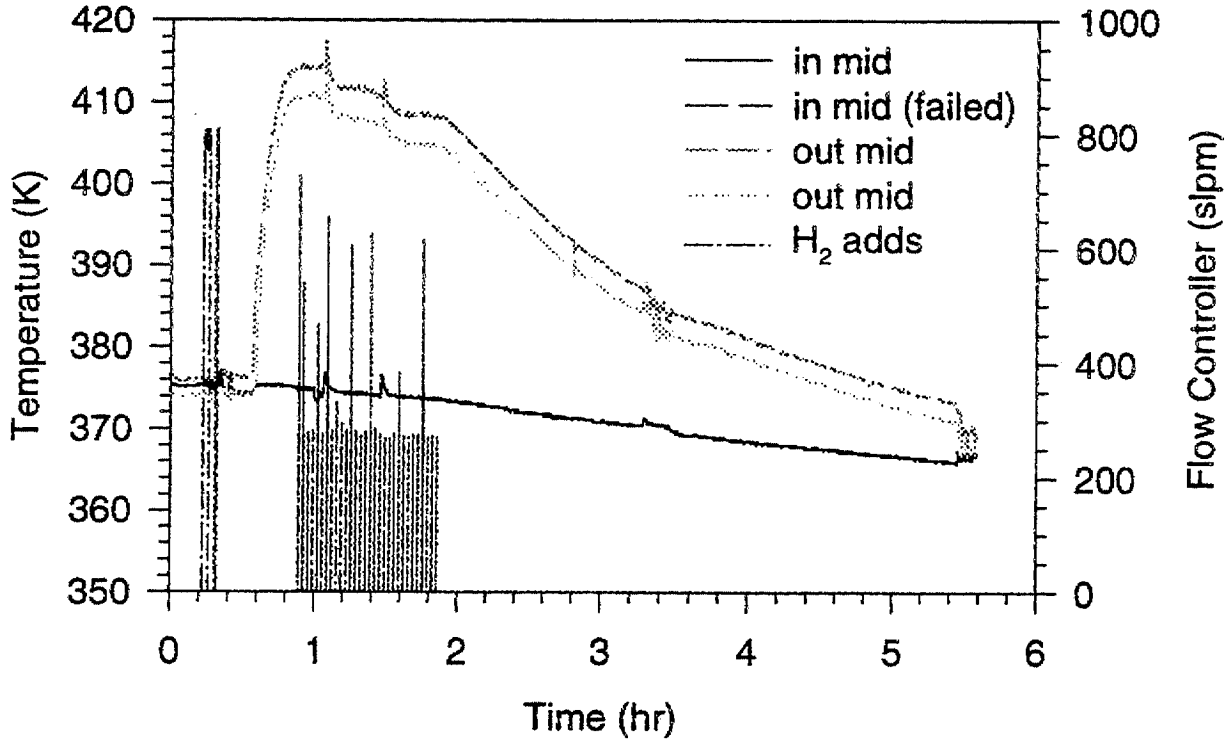


Figure 7 Inlet and outlet temperatures with 1/8 scale PAR

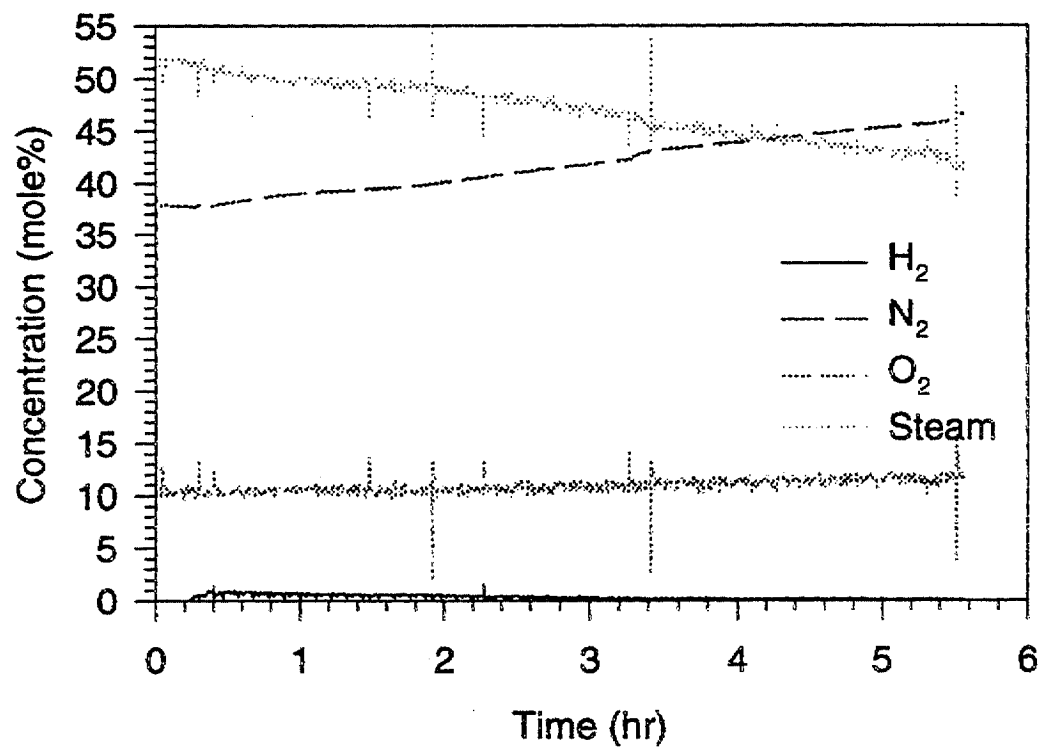


Figure 8 Gas concentrations (wet-basis) with 1/8 scale PAR

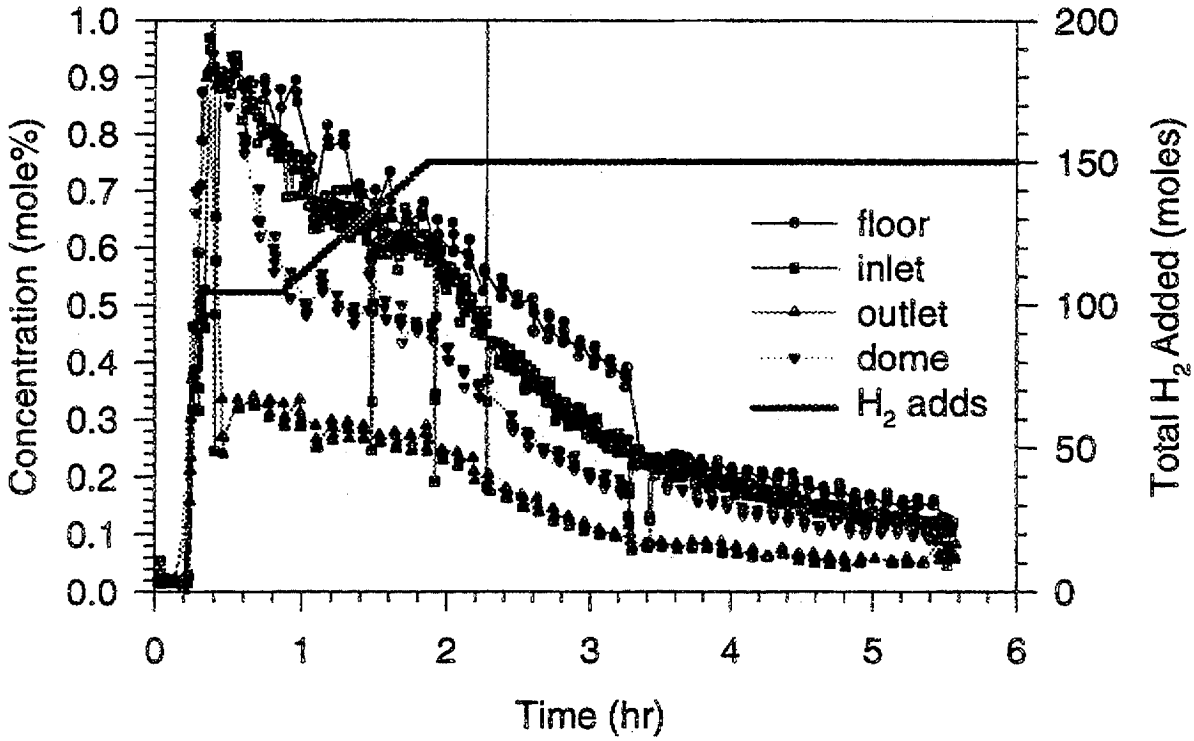


Figure 9 H_2 concentrations (wet-basis) with 1/8 scale PAR

temperature was about 374 K. The PAR started recombining after the first hydrogen addition to about 1.0 mole % which is indicated by the first small increase of the catalyst temperature (Figure 6). There was about a ten minute delay (from the time of first hydrogen injection) in PAR startup. The startup of the PAR is characterized by the establishment of natural convection, which is shown by the increase in the gas temperature at the PAR outlet (Figure 7), followed by the increase in the vessel gas temperature (Figures 4 and 5). Figure 5 also shows the times when the mixing fans were operating while Figure 7 shows the hydrogen additions using the mass flow controller. Figure 8 gives the wet-basis gas concentrations. The steam concentration ranged from about 50 mole % at the beginning of the test to about 40 mole % at the end. The oxygen concentration remained relatively constant at about 10 mole %. Figure 9 focuses on the hydrogen concentrations at the vessel floor, PAR inlet, PAR outlet, and vessel dome locations. This figure also shows the integrated hydrogen addition. The hydrogen concentration from the sample point located near the floor showed smaller decreases as time progressed after the last addition, compared to the other sample points. This indicated that a reduced depletion occurred in the lower half of the Surtsey vessel, below the PAR elevation.

PAR Performance Analyses

Hydrogen depletion rates are used to measure the performance of a PAR. The hydrogen depletion rate is usually determined as a function of the hydrogen concentration in the vessel. Depletion rate analyses can also be used to show the effect of various factors, such as PAR location, oxygen concentration, catalyst poison, etc., on PAR performance.

The following procedure was used to determine the depletion rate. First, the time-dependent amount of hydrogen in the Surtsey vessel (in moles) was determined by multiplying the average hydrogen concentration by the total number of moles in the Surtsey vessel. The average hydrogen concentration was assumed to be that measured by the gas mass spectrometer at the PAR inlet sample point. The total number of moles in the vessel was calculated using the average gas temperature (determined from the array B thermocouples) and the ideal gas law.

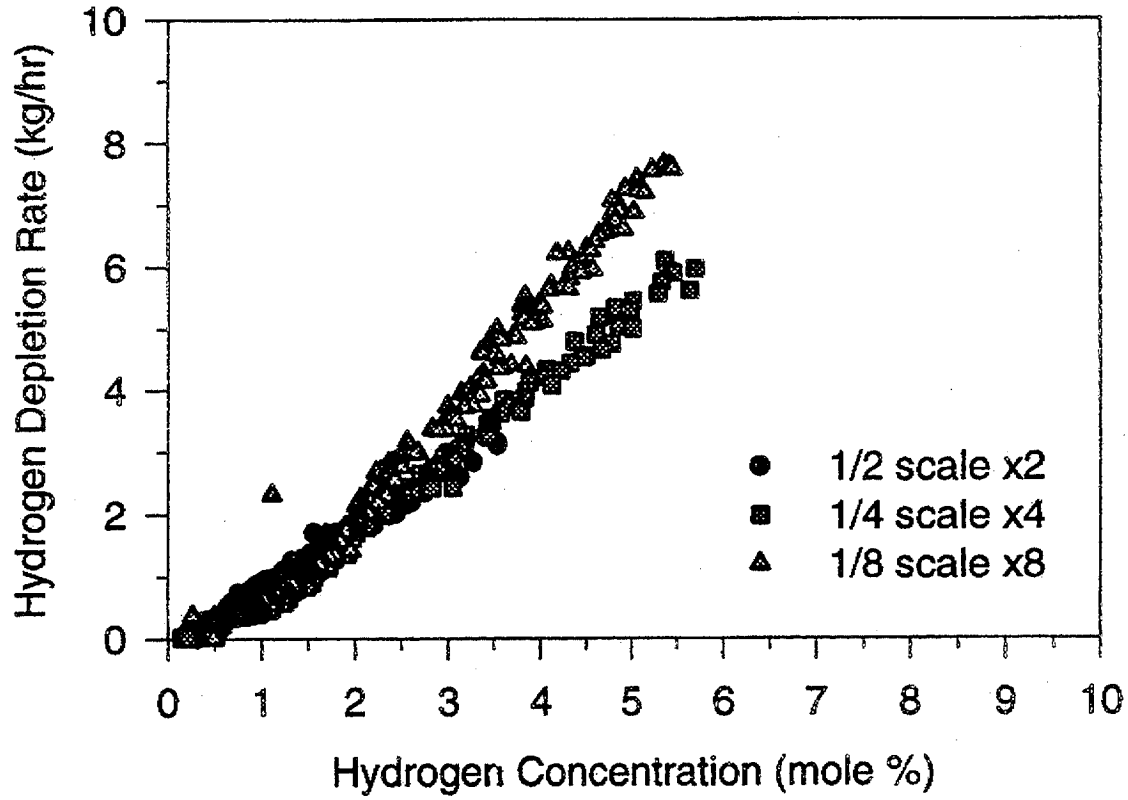


Figure 10 Normalized hydrogen depletion rates as a function of hydrogen concentration

The methodology used to determine the depletion rate assumed that the vessel was well-mixed; this introduced some error since the average hydrogen concentration was not actually measured and cannot be calculated since the local steam concentrations were not known. The measured depletion rates may slightly overpredict hydrogen depletion at the stated hydrogen level since the hydrogen concentration at the PAR inlet sample point, just before the fans were turned on, was lower than the average value. The depletion rate was then determined by calculating the difference in hydrogen moles at each successive time interval, using the data from the steady-state depletion interval, after the hydrogen additions were stopped. The calculated depletion rate was then plotted against the measured hydrogen concentration.

PAR performance and the effects of scale were determined with tests at both low and high hydrogen concentrations. Note that the initial conditions for all tests started with a vessel pressure of about 0.2 MPa, with approximately 50/50 mixtures of air and steam. Preliminary test results indicate that the 1/2 scale depletion rate was ~4 times the 1/8 scale depletion rate.

A comparison of the scaled depletion rate data can be made by normalizing the data. Depletion rate models predict that depletion rate is directly proportional to scale and depletion rate is independent of volume. Therefore, a simple scale factor can be used to normalize the data. Figures 10 shows the scaled depletion rate data normalized to full-scale by applying the scale factor (x2 for 1/2 scale, x4 for 1/4 scale, and x8 for 1/8 scale).

Summary

Hydrogen depletion rates using a scaled PAR were measured in the Surtsey test vessel at Sandia National Laboratories. The experiments were used to determine the hydrogen depletion rate of a PAR in the presence of steam and also to evaluate the effect of scale (number of cartridges) on the PAR performance at both low and high hydrogen concentrations.

The following additional conclusions can be made. The PAR started within 10 minutes in hot, steamy atmospheres when exposed to hydrogen concentrations in the range of 1 to 6 mole %. The PAR appeared to generate a convective flow loop in the Surtsey vessel from the PAR outlet to the dome, down the Surtsey wall until reaching a height near the PAR inlet, and then returned to the PAR inlet.

Reference

1. EPRI ALWR Program (April 8, 1993), "Qualification of Passive Autocatalytic Recombiners for Combustion Gas Control in ALWR Containments."

XA9848580

USE OF PASSIVE AUTOCATALYTIC RECOMBINERS AT INDIAN POINT 2 NUCLEAR POWER PLANT

D. SHAH
Consolidated Edison Company of New York, Inc.,
Indian Point 2,
Buchanan, New York, United States of America

Abstract

This paper discusses the availability and reliability improvements to be achieved at Indian Point 2 nuclear power plant (IP 2) through the use of Passive Autocatalytic Recombiners (PARs). IP 2, owned and operated by Consolidated Edison Company of New York, Inc (Con Edison), will be the first nuclear plant in the United States to install PARs for post accident hydrogen mitigation.

Following a loss-of-coolant accident (LOCA), hydrogen may be generated inside the reactor containment. The U.S. Nuclear Regulatory Commission (NRC) regulations require the control of hydrogen concentration at a safe level following a LOCA. The containment hydrogen control system limits hydrogen concentration so that containment integrity is not endangered. Most nuclear plants use electrically powered thermal recombiners to reduce the hydrogen concentration in containment. The conventional recombiners presently used are mostly elaborate devices that require complex support systems. They are subject to significant reliability and maintenance problems, they require extensive testing. Replacing the existing flame type recombiners with totally passive PARs will reduce the operating and maintenance (O & M) cost, improve reliability of the hydrogen control system and increase availability of the plant. PARs offer a simple, reliable and cost-effective alternative method to limit hydrogen concentration in containment.

1. INTRODUCTION

The hydrogen control system must be designed to maintain hydrogen concentration at a safe level. The accumulation and uncontrolled burn of hydrogen during the Three Mile Island-2 accident in 1979 resulted in more attention being focused on understanding hydrogen generation and the need to control it at a safe level. Although catalytic recombiners have been used for many years in various applications, it was only during the design of advanced light water reactors (ALWRs) that they emerged as a credible option for hydrogen mitigation in nuclear plants (ref.1). It is only recently that they have been considered for use in operating nuclear plants.

Conventional recombiners use high temperature heat to recombine hydrogen with oxygen. They require electric power and other support systems. They are complex to maintain and operate. In contrast, PARs are simple and totally passive. They catalytically recombine hydrogen and oxygen thus producing heat and water vapor. At IP 2 many active components will be replaced by two simple, totally passive PARs. This will improve the reliability of the hydrogen control system and availability of the plant.

2. REGULATORY REQUIREMENTS

Following a LOCA, hydrogen gas may be generated within the containment as a result of:

> metal-water reaction involving the zirconium fuel cladding and the reactor coolant;
> radiolytic dissociation of water in the post accident emergency cooling solutions; and
> corrosion of metals by solutions used for emergency cooling or containment spray.

NRC Regulatory Guide 1.7, "Control of Combustible Gas Concentrations in Containment Following a LOCA," provides a guideline to calculate hydrogen generation. It also requires that the hydrogen concentration in containment not exceed the flammability limit of four volume percent hydrogen.

NRC General Design Criteria (GDC) in 10 CFR 50, Criterion 41, "Containment Atmosphere Cleanup," and 10 CFR 50.44, "Standards for Combustible Gas Control System in Light-Water Power Reactors," require that systems be installed to control hydrogen concentrations and to ensure that containment integrity will be maintained following an accident. NRC NUREG-800, Standard Review Plan 6.2.5, "Combustible Gas Control in Containment," provides the guidelines for designing a system to control hydrogen concentration that will meet the requirements of GDC 41 and 10 CFR 50.44.

3. HYDROGEN RECOMBINERS

The function of the hydrogen recombiner is to prevent the average hydrogen concentration from exceeding four volume percent following a design basis accident. This limit eliminates the potential for reaching flammable conditions. At IP 2, two hydrogen recombiners are located inside the containment. They are the conventional flame type recombiners and use hydrogen as fuel. They require an external source of hydrogen and oxygen to maintain a high temperature stable flame which recombines hydrogen and oxygen in containment air. Ironically, this means we have to pump hydrogen and oxygen into containment to reduce hydrogen. Following an accident 15 truck loads of hydrogen and 7 truck loads of oxygen would be required to reduce the hydrogen in containment. Piping connections are provided outside the containment to hook up the hydrogen and oxygen supply from trucks. This requires containment penetrations, which in turn require containment isolation valves. The hydrogen and oxygen flow and pressure must be controlled to maintain proper flame. This requires control valves, instruments, and control panels, which start, stop and operate the recombiners.

This system was fabricated in 1969. Replacement parts are no longer available for this 30 year old design. Several environmentally qualified (EQ) components of the system are located in a harsh environment, have a limited qualified life, and must be replaced regularly. This system requires significant maintenance and testing. Moreover this system has operating limitations, e.g. to maintain the flame it cannot be started unless containment pressure is below 5 psig (1.358 bar). Following an accident, the system requires manual start and stop by an operator stationed at the control panel located within a radiation area. There is significant preventive maintenance (PM) work for instrumentation, mechanical, and electrical components. Several components must be tested on a monthly or quarterly basis to satisfy surveillance requirements. Actual recombiner flame lighting tests are performed at every refueling outage for both recombiners. During those tests the containment is evacuated for safety purposes. This evacuation results in a loss of approximately one day of critical time during the outage.

4. DESCRIPTION OF PAR

Several different PARs have been designed and tested. Three designs tested most for nuclear plant applications are:

NIS PARs designed by NIS Ingenieurgesellschaft mbH of Germany;
Siemens PARs designed by Siemens-KWU of Germany; and
AECL PARs designed by Atomic Energy of Canada Limited of Canada.

Basically, all PARs work on the same operating principle. The NIS PARs to be installed at IP 2 will be the focus of this paper. The NIS PAR consists of a stainless steel sheet metal box open at top and bottom. The approximate size of the box is 1m x 1m x 1m. There are 88 catalyst cartridges inserted in each box. Each cartridge is fabricated from perforated steel plates. The cartridge frame measures 45 x 20 x 1 cm. and holds more than 400 grams of catalyst pellets. The catalyst pellets are made from aluminum oxide spheres and are coated with palladium and hydrophobic polymers. Each pellet is 3 to 6 mm in diameter. The palladium coating acts as a catalyst. The hydrophobic coating provides water proofing. The catalyst cartridges are held in place by comb-like spacers in each box. The cartridges are installed vertically, spaced 1 cm apart. The spaces between the cartridges serve as flow channels for the gases. Air flow enters at the bottom and the catalyst recombines hydrogen and oxygen in the flow channels to gaseous water. The exothermic reaction of the recombination produces heat, which results in a convective flow that draws more gases from the containment atmosphere into the unit from below. PARs are self starting and self feeding. They require no electrical power or any other support system. The catalyst is not consumed as it functions, and is not subject to long term aging degradation.

5. PAR QUALIFICATION TEST

To date, a substantial amount of testing has been completed by developers, EPRI/EdF (ref.2), and Sandia/NRC (ref.3) as part of an extensive international effort to confirm the PAR performance. However, none of these tests were done to satisfy the quality assurance requirements of 10CFR Appendix B. Con Edison contracted Wyle Laboratories to perform environmental and seismic qualification tests for NIS PARs. These are "first of a kind" tests performed for a PAR using a 10 CFR Appendix B program. These tests will qualify the PARs for use as safety-related equipment in US nuclear plants.

The seismic test was performed to IEEE standard 344 (ref.4). A full size PAR with 88 cartridges was mounted on a shake table and subjected to triaxial multifrequency random motion in the vertical and two horizontal axes. The PAR was subjected to five operating basis earthquake tests and one safe shutdown earthquake test. These tests were performed with a significant margin on earthquake motion.

The environmental qualification tests were performed using a scaled down PAR model. Several cartridges were exposed to high radiation dose and then thermally aged to simulate a 40-year equivalent life. Functional tests were conducted inside an environmental chamber using the irradiated, thermally-aged, and seismically tested cartridges. The chamber had instrumentation to measure hydrogen concentrations, chamber pressure and temperature at several locations. Hydrogen was then added into the chamber. The spray nozzles located at the chamber dome were used for continuous chemical spray to simulate the containment spray.

To date, the results of the tests showed that the PAR performs as expected. The test data was in agreement with calculated values which are based on empirical or theoretical models (ref.5). The test

data also showed that the PAR performance remained almost identical even after exposing it to radiation, seismic motion, thermal aging and chemical spray. At this time an additional test for an accident simulation is in progress. The final test report will be submitted to NRC for review.

6. PAR INSTALLATION AT IP 2

Two full size NIS PAR housings have been installed on the operating floor inside the IP-2 containment. The existing hydrogen recombiner system will be retired and removed. All containment penetrations will be cut and capped. One dozen containment isolation valves, 45 control valves, hundreds of manual valves, 215 instruments and two control panels will be removed. In fact, more than 800 total components in the system currently in service will be removed. This will eliminate numerous tests, PMs, training requirements, EQ requirements, and substantial maintenance. Several procedures including operating procedures will be eliminated. PARs installation will free crucial operator time during a postulated accident. PARs do not have any moving parts. The end result is increased reliability and availability of the hydrogen control system. The existing recombiners are tested as required by the NRC operating license every refueling outage. PARs will eliminate this testing, increasing IP-2's availability by about one day every cycle.

7. CONCLUSION

IP 2 will be the first nuclear plant in the United States to install PARs for post accident hydrogen mitigation. PARs offer a simple, reliable and cost-effective method to limit hydrogen concentration in containment. At IP 2 more than 800 components will be replaced by two simple small stainless steel boxes containing catalyst cartridges. PARs will eliminate numerous testing, PMs, training, maintenance and EQ requirements and will save one day in a refueling outage. Most importantly, availability and reliability of the containment hydrogen control system and availability of the plant will be improved by use of PARs at IP 2.

PAR qualification tests performed by Con Edison pave the way for the use of PARs in US nuclear plants.

REFERENCES

[1] EPRI GC-108770, "Qualification of Passive Autocatalytic Recombiners for Combustible Gas Control in ALWR Containments." EPRI ALWR Program, April 8, 1993.

[2] EPRI/EdF TR-107517, "Generic Tests of Passive Autocatalytic Recombiners (PARs) for Combustible Gas Control in Nuclear Power Plants," June 1997.

[3] T. Blanchat and A. Maliakos, "Performance Testing of Passive Autocatalytic Recombiners," presented at OECD Workshop on the Implementation of Hydrogen Mitigation Techniques, Winnipeg, May 13-15, 1995

[4] IEEE Standard 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."

[5] Rudolph Sher, John D. Trotter, and David E. Leaver, "Passive Autocatalytic Recombiners for Mitigating Containment Hydrogen Concentrations following Design Basis Accidents in Nuclear Power Plants." Presented at Proc. Of 5th International Topical Meeting on Nuclear Thermal Hydraulics, Operation and Safety. Beijing, China, April 14-18, 1997.

COST-EFFECTIVE INSTRUMENTATION AND CONTROL UPGRADES FOR COMMERCIAL NUCLEAR POWER PLANTS SURETY PRINCIPLES DEVELOPED AT SANDIA NATIONAL LABORATORIES

G.E. ROCHAU
Nuclear Reactor Safety Department

L.J. DALTON
Command and Control Software Department

Sandia National Laboratories,
Albuquerque, New Mexico, United States of America

XA9848581

Abstract

Many nuclear power plants use instrument and control systems based on analog electronics. The state of the art in process control and instrumentation has advanced to use digital electronics and incorporate advanced technology. This technology includes: distributed microprocessors, fiber optics, intelligent systems(neural networks), and advanced displays. The technology is used to optimize processes and enhance the man-machine interface while maintaining control and safety of the processes. Nuclear power plant operators have been hesitant to install this technology because of the cost and uncertainty in the regulatory process. This technology can be directly applied in an operating nuclear power plant provided a surety principle-based "administrator" hardware system is included in parallel with the upgrade. Sandia National Laboratories has developed a rigorous approach to High Consequence System Surety (HCSS). This approach addresses the key issues of safety, security, and control while satisfying requirements for reliability and quality. We believe that HCSS principles can be applied to nuclear power plants in a manner that allows the off-the-shelf use of process control instrumentation while maintaining a high level of safety and enhancing the plant performance. We propose that an HCSS Administrator be constructed as a standardized approach to address regulatory issues. Such an administrator would allow a plant control system to be constructed with commercially available, state-of-the-art equipment and be customized to the needs of the individual plant operator.

1. INTRODUCTION

Most of the instrumentation and control equipment currently installed at U.S. nuclear power plants is based on analog electronics. While this equipment is safe and operable, it is now commercially obsolete, difficult/expensive to maintain, and inefficient[1]. The state of the art in process control and instrumentation has advanced to use digital electronics and incorporate technology such as distributed microprocessors, fiber optics, intelligent systems(neural networks). Furthermore, advanced displays optimize processes and enhance the man-machine interface while maintaining control and safety of the processes. These advances have not been captured by U.S. nuclear power plants due to lack of favorable cost/benefit analysis of such technologies combined with the uncertainty of obtaining regulatory approval of the new technology.

2. STATUS OF I&C SYSTEMS IN THE UNITED STATES

Instrumentation and Control (I&C) technology is key to nuclear plant safety, reliability, and availability. A majority of the I&C systems used in U.S. nuclear power plants use analog circuits for the plant safety system. These systems must be frequently tested, adding to the possibility of human error causing a plant trip. An inadvertent signal can take a nuclear power plant off-line in an instant. Consequently, the cost of a I&C failure is substantial when compared to the cost of new systems.

[1] J. Naser, "Integrated Instrumentation and Control Digital Upgrades for Cost Reduction," Proceedings: Distributed Digital Systems, Plant Process Computers, and Networks, EPRI TR-104913, March 1995.

High-reliability instrumentation and control systems are needed for the cost-effective operation of the nuclear power plant. A stable and mature technology is needed to obtain the regulatory approvals. However, I&C digital technology is a developing field of technology and I&C suppliers are rapidly moving away from supporting the systems of nuclear power plants. Manufacturers have: discontinued product lines without replacements, failed to maintain an adequate spare parts inventory, and decreased service support[2].

Industry-wide, I&C systems are currently have highly customized Process Control Systems to meet the operating characteristics for the individual plant and standardized Plant Protection Systems by vendor to meet regulatory requirements. Thus, as the equipment becomes obsolete, a nuclear power plant operator is faced with a dilemma: should the existing technology be maintained in some fashion, or should the technology be upgraded to state-of-the-art and obtain necessary regulatory acceptance? This dilemma is being considered in terms of existing economic conditions, increasing competition from other power producers, and uncertain regulatory issues. The majority of the industry has chosen to maintain their I&C systems and upgrade them, on a subsystem basis, when the plant performance is impacted. Consequently, there is no common vision for the "Control Room of the Future."

3. BENEFITS OF USING DIGITAL TECHNOLOGY

Using digital technology as the basis for nuclear power plant I&C upgrades allows the nuclear market to tap the rapidly developing digital I&C market for industrial process control. By accessing this technology, not only can the nuclear power plant operator be assured of efficient and reliable I&C operation, but also can be assured of a much larger supply of replacement parts and future replacement systems, thereby reducing plant operations and maintenance costs. In addition to availability of hardware, digital technology provides a new infrastructure which allows the plant operator to enhance the efficiency of plant operation, to increase the plant capacity factor, and to possibly reduce the cost of generated electricity.

The use of digital technology is estimated to reduce I&C-related operations and maintenance costs by 10% and increase plant power output by 5%. Industry wide, the total U.S. nuclear generation costs would be reduced by $1 billion per year and power produced would increase by 30 million MWh. Replacement of this generation capacity would require the construction of five 1000 MWe fossil plants costing $5-10 billion[3].

4. REGULATORY ISSUES ASSOCIATED WITH DIGITAL I&C SYSTEMS

The successful integration of digital technology into I&C systems at U.S. nuclear power plants face five significant challenges[4]:

1) technical uncertainty inherent in the introduction of new technology;
2) shift of existing technology base from analog experience;
3) technical problems identified from applications of digital I&C in other nuclear power plants;
4) difficult, time-consuming, and customized licensing approach; and

---

[2] W. G. MacFarland, "A Utility Perspective," Proceedings: Joint DOE/EPRI International Conference on Cost-Effective Instrumentation and Control Technology Upgrades for Nuclear Power Plants," EPRI TR-105148, August 1995.

[3] N. Fletcher, etal., "Joint Nuclear Power Industry/DOE Instrumentation and Control Upgrade Program," Proceedings: Joint DOE/EPRI International Conference on Cost-Effective Instrumentation and Control Technology Upgrades for Nuclear Power Plants," EPRI TR-105148, August 1995.

[4] National Research Council, Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operation and Safety, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Final Report," National Academy Press, Washington D.C., 1997, p 1.

5) lack of consensus on issues underlying evaluation and adoption of I&C technology and the means to obtain a satisfactory resolution.

The key regulatory issues can be summarized as six technical issues and two strategic issues[5]:

Technical Issues:

1) Systems aspects of digital I&C technology - How do all the systems interact?
2) Software quality assurance - How do we know that the software will always perform according to the requirements?
3) Common-mode software failure potential - How do we avoid having bad tools in the software toolbox which causes redundant systems to fail?
4) Safety and reliability assessment methods - How do we derive a probability of failure for a digital system?
5) Human factors and human-machine interfaces - How does digital technology change the operator interface with the plant?
6) Dedication of commercial off-the-shelf hardware and software - How can the usage of digital technology from the process control industry be used?

Strategic Issues:

1) Case by case licensing process - What assurance does the licensing of one digital system give for the next system to be approved?
2) Adequacy of technical infrastructure - What changes do regulatory authorities need to make to support digital I&C regulation?

These issues are roadblocks for implementing digital I&C technology at nuclear power plants. Since specific regulations are not in effect, the cost uncertainty associated with regulatory acceptance is unacceptable to many plant operators.

5. HIGH CONSEQUENCE SYSTEMS SURETY APPROACHES USED AT SANDIA NATIONAL LABORATORIES

Sandia National Laboratories, as steward of the U.S. nuclear weapon stockpile, has developed a rigorous approach to High Consequence System Surety (HCSS). Developed to provide for the safety and security of nuclear weapons, HCSS principles can provide significant support in the design of new digital I&C systems. This approach addresses the key issues of safety, security, and control while satisfying requirements for reliability and quality. HCSS is achieved by using four major principles: isolation, inoperability, incompatibility, and independence. Isolation allows a system to be insensitive to external events. Inoperability makes the system safe before the isolation of the system is overwhelmed by an event. Incompatibility makes the system unresponsive to any signals except those which are uniquely identified. Independence is achieved by design to eliminate commonality between safety subsystems. These four principles are maintained in parallel with a system design. Using "state machines" (digital electromechanical devices) the system behavioral model is captured in a system of interlocks and mechanical analogs. These machines model the system with quantifiable integrity using discriminating devices which are robustly designed to respond to a unique signal. Thus, through the use of state machines the behavior of a system is monitored, not the specific system controller functions. These concepts have been demonstrated for robotic systems used for remote handling of plutonium parts from nuclear weapons[6].

State machines incorporate hardware programmed Application Specific Integrated Circuits (ASICs) and discriminating devices (mechanical systems) which must be moved into proper position for actions to proceed. In the last few years, the state-of-the-art for

---

[5] Ibid., p 4-11.

[6] J. Smith, "Micromachined Sensor and Actuator Research at Sandia's Microelectronics Development Laboratory," Proc. Sensors Expo Philadelphia '96, pp. 143-148, Oct. 1996.

such systems has advanced to possibly use micromechanical actuators which are so small that they can be mounted on a digital circuit chip. The mechanisms, shown in Figure 1, have the capability of operating at up to 300,000 revolutions/minute and operate for over 8 x 10^8 revolutions[7].

6. APPLICATION OF HCSS TO NUCLEAR POWER PLANT I&C SYSTEMS

We believe that HCSS principles can be applied to nuclear power plants in a manner that allows the off-the-shelf use of process control instrumentation while maintaining a high level of safety and enhancing the plant performance. We propose that the Control Room of the Future will incorporate digital I&C technology directly from the process control industry and will also incorporate a surety system to implement regulatory controls and safeguards. A plant control system can be constructed with commercially available, state-of-the-art equipment which can be customized to the needs of the individual plant operator and phased into the plant as economic conditions dictate. A standardized HCSS system would be constructed for a specific Nuclear Steam Supply System (NSSS) which would contain the model for safe operation of the system. The HCSS "administrator" is the state machine for the NSSS and would need to be manipulated into the proper configuration by the I&C system. As long as the proper configuration of the HCSS administrator was maintained, the I&C system could function at any enhanced level or with direct operator control. Failure to maintain the administrator would be the equivalent of a plant trip in some instances or prohibition of an operator action in others.

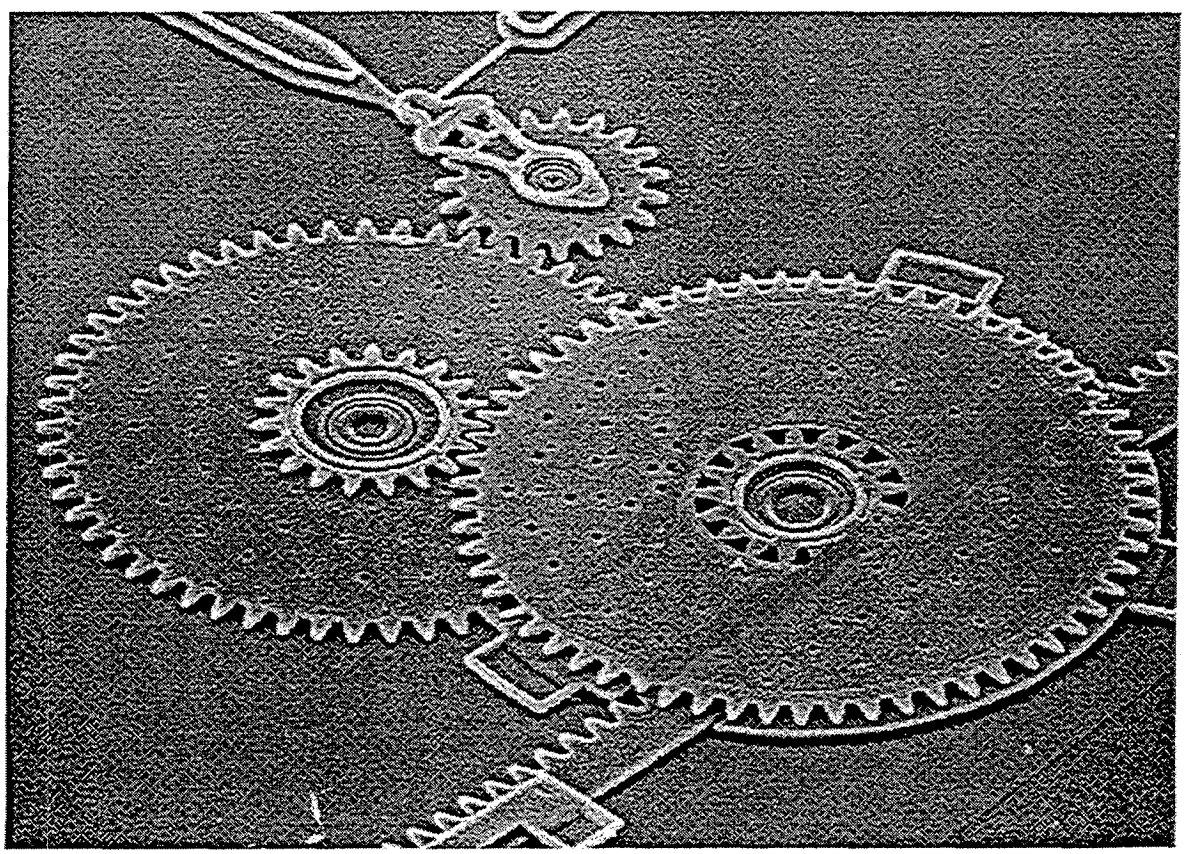


Figure 1. Micromotor with gear train transmission.
(Approx. scale 260 microns, ref.: human hair is about 80 microns)

[7] Sandia National Laboratories, "High Consequence System Surety," version 3, video tape, 8 minutes, March 31, 1995.

In theory, the HCSS administrator functions as a digital electromechanical analog computer modeling the reactor system. The administrator responds to and generates digital signals, but uses mechanical analogs and interlocks to model the system operational space.

Three advantages of an HCSS administrator would be:
1) Utilization of the state-of-the-art I&C technology from the process control industry,
2) Allowing the regulatory issues to be addressed through a standardized surety principle-based administrator, and
3) Minimum concern for safety-related I&C software design, quality assurance, and maintenance.

In practice, the HCSS administrator would be placed in parallel with the plant process control system (Figure 2). The administrator would have specific requirements for proper alignment and have exclusive control of plant safety-related components. The plant process control system must meet the input requirements of the HCSS administrator in order to maintain control. Should this condition not be maintained, the administrator would take control of the reactor to place it in a safe condition. Under operator control, the administrator would allow any action permitted under the system model and prohibit operator actions that would violate the system model. This configuration scheme may eliminate the need for extensive software testing and quality control. We believe that rather than examining all possible failure scenarios, the surety of the system is maintained by monitoring the system parameters to be within the operational space of the system and preventing those parameters from leaving that space.

In application, the HCSS administrator would be installed in the plant first, eventually replacing the plant protection system. The administrator would be subject to intense regulatory review, but this review would be based on the system model, not on unresolvable issues. The plant operator would then be allowed to make I&C system

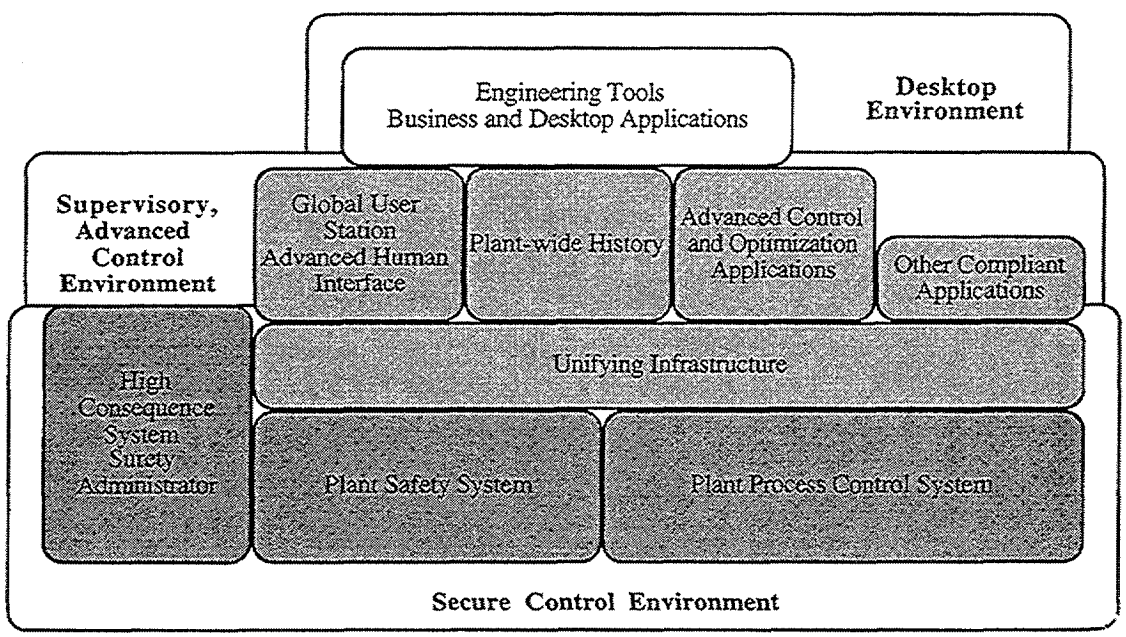


Figure 2. High Consequence System Surety Administrator applied to a state-of-the-art process control system[8]

[8] Process Control System is the TotalPlant Solution System schematic courtesy of Honeywell Corporation.

equipment changes as the need dictates and the economics allow. These I&C changes should be accomplished with a minimum of regulatory review.

7. CONCLUSION

Cost-effective instrumentation and control upgrades for nuclear power plants are possible using standardized digital technology if a standardized approach can be found to resolving regulatory issues. A system "administrator" developed for standardized nuclear reactor types which employ High Consequence System Surety (HCSS) principles developed at Sandia National Laboratories meets this need. An HCSS administrator would allow the nuclear power industry to utilize the state-of-the-art digital I&C technology from the process control industry while maintaining the same level of system safety required by nuclear safety regulators.

XA9848582

DEFENSE AGAINST COMMON-MODE FAILURES IN PROTECTION SYSTEM DESIGN*

R.H. WYMAN, G.L. JOHNSON
Lawrence Livermore National Laboratory,
Livermore, California,
United States of America

Abstract

The introduction of digital instrumentation and control into reactor safety systems creates a heightened concern about common-mode failure. This paper discusses the concern and methods to cope with the concern.

Common-mode failures have been a "fact-of-life" in existing systems. The informal introduction of defense-in-depth and diversity (D-in-D&D)—coupled with the fact that hardware common-mode failures are often distributed in time—has allowed systems to deal with past common-mode failures. However, identical software operating in identical redundant systems presents the potential for simultaneous failure. Consequently, the use of digital systems raises the concern about common-mode failure to a new level. A more methodical approach to mitigating common-mode failure is needed to address these concerns.

Purposeful introduction of D-in-D&D has been used as a defense against common-mode failure in reactor protection systems. At least two diverse systems are provided to mitigate any potential initiating event. Additionally, diverse displays and controls are provided to allow the operator to monitor plant status and manually initiate engineered safety features.

A special form of common-mode failure analysis called "defense-in-depth and diversity analysis" has been developed to identify possible common-mode failure vulnerabilities in digital systems. An overview of this analysis technique is provided.

Introduction

The term "common-mode failure" (CMF) has been in the reactor vocabulary for a number of years. It has been somewhat controversial because there were few concrete examples of CMFs; those few were not always accepted as having failed from some common mechanism at work. The problem stemmed from the way the failures occurred. There were no cases where a large number of "identical" devices failed at nearly the same time in nearly the same way. The failures occurred randomly over time and thus appeared to be ordinary random failures. It was only upon closer inspection that the common-mode failure became clear.

However, with the advent of software operated devices—where multiple redundant units would all be executing the same program with essentially the same inputs and outputs and more-or-less synchronous—the possibility of simultaneous failure in redundant units becomes all too real.

The purpose of this paper is to describe some of the issues of software-induced common-mode failures including assessment issues and methods of avoiding catastrophic failure in the event that such a common-mode problem exists.

Common-Mode Failures

For the purposes of this paper, CMFs are failures attributable to a common cause. The results of a CMF may be the complete loss of a protective function at a critical time.

*This work was performed under the auspices of the US Department of Energy by Lawrence Livermore National Laboratory under contract W-7405-Eng-48.

CMF mechanisms may be the result of requirement errors or omissions, design flaws, manufacturing problems, installation faults, application errors, quality control (QC) failures, etc. However, really good QC may actually enforce a CMF that is caused by other problems, in that good QC will force all items to be very similar if not identical.

Many CMFs give the appearance of random failures because the failures are random in time, although the mechanism of the failure is the same in all units. Variable environment and usage will spread the failures out in time so that they appear to be failures from random causes.

Examples

Experience in the industry has shown that, while not common, common-mode failures do in fact occur in hardware. Some examples follow.

Salem

The original reactor trip breakers were not specifically designed for the application in that they did not contain an undervoltage trip coil as such. A modification was made so that the trip mechanism was spring-operated and the spring was held by a relay or solenoid that was energized during normal operation. When the voltage fell below some value, the coil would release the spring tripping the breaker, or so the designers thought.

The pivots in the trip mechanism required lubrication that was not provided. The spring was not strong enough to overcome the lack of lubrication since the relay pulling on the spring was not forceful enough. After time, when the voltage holding the relay fell below its drop-out point, the spring was not strong enough to trip the breaker. Since this mechanism was the same in all the breakers, none of the breakers would trip on low voltage.[1]

BWRs Scram Mechanism Failures

A number of events involving common-mode failure in boiling water reactor (BWR) scram systems and their related support functions such as the air system and electric power system occurred. Specifically, it was discovered that water could be in the scram discharge volume (SDV) of a BWR as a result of poor drainage or an air supply failure. Water in the SDV would inhibit the insertion of control rods. The failure involving the air system was of particular concern because it involved a system that had been considered a portion of the reactor protection system not related to safety. Action was taken at all boiling-water reactors to correct this problem.[2]

This group of common-mode failures resulted from the use of a "fail-safe" design approach that in reality required a number of non-safety-related features to function and, therefore, the design did not truly rely on fail-safe principles. In the case of the air system, the system was assumed to fail safe, i.e., bleed off, and, as a result, a partial failure was not adequately addressed in the design. It was also noted that the electric supply system to this scram system had been modified previously because of a similar type of concern. Specifically, the electric power was originally assumed to fail safe (i.e., voltage going to zero) and, as a result, partial failure (such as low voltage or high voltage) was not appropriately addressed. In one case, 76 out of 185 "independent" control rods failed to fully insert.[3]

Scram discharge volume level monitoring systems designed to detect these failures also exhibited common mode failures themselves. In one plant operators discovered that the scram discharge volume (SDV) continuous water level monitoring system had failed to respond as expected. The continuous water level utilized a single transmit/receive ultrasonic transducer for each of the four level monitoring channels.

The expected high level annunciator alarms were not received in the control room following scram when the SDV filled with water. Investigations determined that the ultrasonic detectors were inadequately coupled to the SDV piping.[4] This problem was compounded by noise problems created by cable routing, improper sensor placement, and cross-talk between detector channels.[5] In other cases, level sensor designs using differential pressure transmitters and resistance temperature detectors had unacceptably long response times.[6]

The HFA Relays

The HFA relays were commonly used in relay logic protection systems. They were widely used in the industry. In most applications they were continuously energized and operated in relatively tight enclosures that were designed to keep dust, dirt, and other industrial contaminants out of the relay mechanisms and contacts.

A series of problems were encountered that prevented these relays from changing state when de-energized. These problems included coil spool cracking,[7] melted coil spools,[8] and deposition of vaporized insulating materials on relay armatures or contacts.[9] These failures were common to many functions at some plants and occurred at a large number of plants.

A Danish Study

In 1975, J. R. Taylor of the Danish Atomic Energy Commission published a report entitled "Common Mode and Coupled Failures"[10] in which he studies event reports from the USA. He characterizes common-mode and common-cause events and classifies the events of the study according to their characteristics. He then proceeds to establish statistical models for common-mode and coupled failures.

How Have We Managed to Survive

To date, the conservatism of reactor designs together with D-in-D&D have kept the industry out of trouble. Defense-in-depth is the concept of multiple lines of defense against a perceived threat so that if one line of defense is penetrated, another line is invoked to limit the damage caused by the penetration. This can be carried through several levels. For example, to prevent the release of radioactive material to the environment, there are three physical barriers, each of which is supported by the three diverse control systems: the instrumentation and control (I&C) system of the reactor, the reactor protection system, and the Engineering Safety Features Actuation System (ESFAS). The first line of defense is the cladding on the fuel rods. This line is supported by (1) the reactor I&C system that attempts to keep the rector operating in the normal power producing regime, (2) the reactor protection system that will scram the reactor if required, and (3) the ESFAS system that will attempt to keep the reactor cool in emergency situations. If for some reason the various reactor cooling systems fail, the next physical line is the reactor pressure vessel that attempts to keep radioactive material from the failed fuel rods within the vessel. The vessel is also supported by the three control systems mentioned. Finally, the last boundary is the containment system which is designed to prevent release to the atmosphere if the pressure vessel fails. Containment is supported by the ESFAS. Lastly, the evacuation plan is invoked if all else fails. This is the classic D-in-D&D strategy and it has been successful in that evacuation plans have never been invoked.

Diversity is the notion that if redundant systems are different in some substantial way from each other, a failure in one will not necessarily imply a failure in the other. For example, some emergency core cooling pumps may be electrically driven, some steam driven, and the pumps themselves may come from different manufacturers.

The other phenomenon that has worked to our advantage has been alluded to previously. Because of variability in manufacturing, application environment, and usage, many CMFs look like random failures since they occur randomly in time and the likelihood of all redundant systems failing simultaneously is small. But, if there is a common-mode mechanism at work, this likelihood is considerably larger than it would be otherwise, particularly if operational and environmental conditions are similar.

Software as a Particular Vulnerability

With the advent of digital computer-based systems and the attendant software, the problem of CMF has become more pressing. Software errors in one system are now carried exactly to the other redundant systems; no variability in manufacturing, application environment, or usage will produce any time randomness in the execution of the bug. Since each computer of the redundant set is seeing closely similar, if not identical, inputs at approximately the same time, the same software will be invoked in each computer. When a software error exists, all will execute a bug more-or-less simultaneously, and if this error causes the system to operate improperly or crash, each of the redundant machines will fail simultaneously.

N-Version Programming

As an answer to this problem, a method called "n-version programming" has been proposed. The notion here is that, working from the same software specification, several independent groups of programmers would write the code to meet the specification, perhaps even using different programming languages. This idea has not met with much acceptance for several reasons. First, the cost of maintaining several different sets of software has been daunting. More importantly, studies have shown[11] that the linkage at the requirements level is fatal. If the requirement is wrong, the software cannot be expected to overcome the problem. Further, there is some evidence that coding errors are not the big problem; errors in the requirements cause much more trouble than coding errors.

Software Testing

For large complex software systems, exhaustive testing becomes impossible because of time constraints. Typically a software vendor will send pre-release versions of software systems to friendly customers with instructions that they would like the customer to use the software in his normal course of work with the understanding that they are doing beta testing on the software. (Alpha testing is what the vendor does before he distributes it to beta testers.) The understanding includes a "hold harmless" clause and the customer agrees to report bugs to the vendor. After several months of beta testing, the vendor allows the product to go to paying customers and those customers are allowed to find the rest of the bugs. This is the reality. The number of software releases without bugs is small. Mostly it is hoped that the remaining bugs are no more than irritants.

In the reactor business, beta testing is not accepted. The software is expected to be free of bugs. Testing gets rid of most of the problems, but what about the remaining problems? Are there any problems remaining? The vendor would like to believe "no," but the reality is "yes." The issue is how to get the bugs down to an acceptable minimum and what to do about those that remain.

Software Quality Control

The ability of professional software production organizations to produce operating software with only benign bugs has greatly improved in the past decade. The reason for this is the introduction of "software engineering" techniques. The days when a customer loosely described what he wanted vocally to a coding hacker are mostly gone. Today, a Software Requirements Specification is developed and put under configuration control. Next, design proceeds in a stepwise evolution of requirements to conceptual design, detailed design, component design as the software process moves forward to produce code. (This is very similar to the traditional hardware design process.) This paper will not discuss the software engineering process in detail, but it has been very successful. The software engineering effort starts with a commitment by all the members of the software organization to high software quality and "bug free" operation. Currently, software flies our commercial airplanes, navigates our wartime missiles, runs our traffic lights, and is included in many of our ordinary day-to-day activities. Software engineering works and is getting better all the time. But it is not perfect. So what do we do to guarantee the safety of the public in reactor operations?

First of all, do software bugs pose a threat to reactor safety?

What is the Experience?

Software has been implicated in several safety failures, one of which actually caused several deaths. Not all of the examples below are reactor examples, but they are illustrative of what can occur when software fails

Therac-25

The Therac-25 was a medical accelerator used for irradiating cancer patients. It was a two-mode machine, one mode being an x-ray mode and the other where the patient received an electron beam directly. The machine was controlled by a computer that took information from the operator and set the machine up for operation.

Unfortunately, the software was very overcomplicated for the application and had a mode that it got into if the operator typed too fast wherein it would do the wrong things. This resulted in several patients getting severe doses of radiation which, in several cases, killed.

This was written up in great detail by Nancy Leveson.[12]

The Space Shuttle

The space shuttle uses four redundant computers for control of the shuttle during launch and at other times. These machines are synchronized using a common clock. There is a fifth computer that serves as a backup to these four. It is a diverse machine running diverse software. It uses the common clock for synchronization.

During a launch sequence, while the vehicle was on the pad and within a few minutes of the launch, the four main computers appeared to fail. The launch was aborted and—other than a few red faces—there was no damage. However, if this failure had occurred during the launch, the mission would have aborted. In that case, a second problem involving an unexpectedly high loft pitch angle of the shuttle would have caused failure of the software designed to steer the shuttle to a landing. The results of these couple failures could have been fatal to the crew.

The problem was clock synchronization.

The people programming for the space shuttle pride themselves on writing bug-free code. They have an extensive QC program and have a great deal of pride in never having killed anyone. But considering the example, they were just lucky.

This is not a reactor example, but it illustrates what can occur despite all of the best efforts.[13]

Turkey Point Load Sequencer

This sequencer used multiple redundant programmable logic controllers (PLCs) to perform its function. The sequencer had self-test features which allowed individual PLCs to perform local tests to verify proper operation. In the event that the diesel generators were required while a unit was in self-test, the self-test mode was to be abandoned and normal operation was to be resumed. But there was a bug in the code and just when the sequencer was called upon, all of the units were in self-test. The bug prevented the units from resuming normal operation. As it turns out this problem was found during a testing operation so there were no safety consequences of this failure.[14]

South Texas Qualified Display Processing Software Error

An over-temperature/delta-temperature (OT/delta T) reactor trip occurred due to a software error. The reactor trip occurred at a reactor coolant system temperature of 530°F. Initial observation was that channel II T-hot output rose to 568°F giving a OT/delta T trip coincident with an OT/delta T trip already inserted in channel IV due to maintenance work. Subsequent investigation resulted in the identification of a software design error in the qualified display processing system (QDPS) temperature averaging system which erroneously calculated an average hot leg temperature of 568°F for channel II when the temperature was actually 530°F.[15]

The error was in the conservative direction and occurred prior to initial plant criticality. Therefore, there were no safety consequences. Similar errors in the non-conservative direction are certainly possible.

Additional Examples of Common-Mode Failure in Digital Systems

A U.S. Nuclear Regulatory Commission (NRC) study examined failures of digital I&C systems in U.S. nuclear power plants from 1990 through 1993. This study found that software errors was one of the prime causes of failures in these systems.[16] Each software error represents a potential common-mode failure.

The U.S. Nuclear Regulatory Commission Four-Point Position

The NRC debated for a considerable time on the problem of CMFs in redundant digital computer systems. The solution was the time-tested D-in-D&D that has been so effective over the years. The problem for software systems is, then, to establish what is adequate and effective for D-in-D&D for nuclear reactors in the U.S.

In order to establish the ground rules for what would be considered adequate D-in-D&D for computer based systems, the NRC has developed a four-point position that has been formally approved by the NRC.[17] The four points are:

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failure have been adequately addressed.

2. In performing the assessment, the vendor or applicant shall analyze the postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate (using realistic assumptions) methods.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room shall be provided for the manual system-level actuation of critical safety functions and monitoring or parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

Note that in point four, above, there is a requirement for "...the same function or a different function." If the "different function" is invoked, this paragraph is interpreted to mean that the different function has the same or equivalent system function as the "...same function." That is, if one method for cooling the core fails, another method may be started up.

D-in-D&D Assessment – NUREG/CR-6303

For a number of years the NRC relied on NUREG-0493[18] to provide a method and a model for D-in-D&D assessment. This NUREG was very effective for the purpose, but as computer systems and their developers got more sophisticated, the NUREG needed to be updated to account for this evolution. NUREG/CR-6303 is that update,[19] building on the solid foundation provided by NUREG-0493 and the experience gained by its use. Of course, as with all NUREGs, NUREG/CR-6303 is advisory and the method described is not mandatory. The assessment method in NUREG/CR-6303 was used in the assessment of all of the Advanced Light Water Reactor (ALWR) designs.

The Block Concept

To do a D-in-D&D assessment using the method outlined in the NUREG, the system needs to be divided into reasonably sized blocks and for each a reasonable probability that a failure in that block will cause all identical blocks to fail in the redundant systems. If these blocks are too big, the assessment is simple but it produces an assessment that is much too harsh. If the blocks are too small, the assessment becomes too complex to be accomplished in a reasonable time.

Once the blocks have been chosen, an analysis is performed for each block and each event in the catalog of events to which the system must respond effectively. It is presumed that all blocks similarly located in each of the redundant systems will fail at the same time for each event in the accident analysis. Then for each event with the chosen block inoperative, the remainder of the system is examined to see if it has enough diverse functionality left to respond effectively to the event.

Types of Diversity

If a block fails, the question becomes one of deciding whether or not the remaining system is sufficiently diverse from the failed block so that it will continue to function adequately in the face of the failure. It must be able to respond to the failure in such a way that the overall system is put or kept in a safe state.

There are a number of types of diversity outlined in the NUREG. Briefly, there is equipment diversity, functional diversity, human diversity, signal diversity, and software diversity. The NUREG explains why all diversities are not created equal and how it is decided whether or not adequate diversity exists. In

particular, functional diversity and signal diversity are particularly strong forms of diversity. Decisions regarding what is diverse and what is not are not particularly objective and engineering judgment plays an important role in diversity assessment.

It is particularly important that the analysis be performed by highly competent engineering staff with a thorough and complete understanding of system performance. Otherwise the analysis may be worse than useless in that it will either give too optimistic an assessment of system performance or it will condemn a system that is otherwise perfectly usable. It should be noted that the former assessment is much more common than the latter so that analysis is typically not fail-safe.

Conclusion

Common-mode failures in hardware were not typically much of a problem in traditional reactor systems. With the introduction of digital systems into reactor protection systems, the possibility that the entire reactor protection system would fail at a critical juncture in reactor operations became much more plausible. This was attributed to the issue of common software being operated in all units of a redundant system where a bug in one would be a bug in all.

Testing to find these latent bugs in the software is not a reasonable means of coping with this eventuality because of the huge number of variations that must be tested. The time required for exhaustive testing is simply not available if a system is to be fielded in a reasonable time. Testing is an essential part of software production but experience shows that latent bugs are a fact of software production. However, the number of bugs in a code can be greatly reduced by good software engineering practice and a firm commitment to high software quality. The notion of "safety critical software" is now part of the software engineering world and methods are in place that allow the production of software for safety-critical applications. An example is the "fly-by-wire" systems in commercial aircraft.

The problem of common-mode failure in redundant systems can be addressed by defense-in-depth and diversity in the design of those systems. NUREG/CR-6303 provides a method for assessing D-in-D&D for digital systems which may have the potential for common-mode failure in redundant units running common software. The analysis method outlined in the NUREG has been successfully applied to several designs for nuclear reactor protection systems.

References

[1] NUREG-0977. "NRC Fact-Finding Task Force Report on the ATWS Event at Salem Nuclear Generating Station, Unit 1, February 22 and 25, 1983." March 1983.

[2] Generic Letter 89-18. "Resolution of Unresolved Safety Issue A-17: 'Systems Interactions In Nuclear Power Plants.'" September 6, 1989.

[3] IE Bulletin No. 80-17. "Failure of 76 of 185 Control Rods to Fully Insert During a Scram at a BWR." July 3, 1980.

[4] IE Information Notice No. 80-43. "Failures of the Continuous Water Level Monitor for the Scram Discharge Volume at Dresden Unit No. 2." December 5, 1980.

[5] IE Supplement 4 to Bulletin No. 80-17. "Failure of Control Rods to Insert During a Scram at a BWR." December 18, 1980.

[6] IE Information Notice No. 87-17. "Response Time of Scram Instrument Volume Level Detectors." April 7, 1987.

[7] IE Information Notice No. 81-01. "Possible Failures of General Electric Type HFA Relays." January 16, 1981.

[8] IE Information Notice No. 82-13. "Failures of General Electric Type HFA Relays." May 10, 1982.

[9] IE Bulletin No. 84-02. "Failures of General Electric Type HFA Relays in Use in Class 1E Safety Systems." March 12, 1984.

[10] Taylor, J.R. "Common Mode Coupled Failures," Danish Atomic Energy Commission, 1975.

[11] Knight, John C. and Nancy G. Leveson. "An Experimental Evaluation of the Assumption of Independence in Multiversion Programming." In *IEEE Transactions on Software Engineering*, Vol. SE-12, no. 1, January 1986.

[12] Leveson, Nancy G. and Clark S. Turner. "An Investigation of the Therac-25 Accidents." *Computer* (1993): 18-41.

[13] "Shuttle First Put to the Test," *IEEE Spectrum* (August 1981).

[14] LER 94-005-02. "Turkey Point Units 3 And 4, Design Defect in Safeguards Bus Sequencer Test Logic Places Both Units Outside the Design Basis Event." November 3, 1994.

[15] LER 88-014 REV 01. "South Texas 1, Update on Reactor Protection System Actuation due to a Software Problem in QDPS." May 18, 1988.

[16] U.S. Nuclear Regulatory Commission. "Technical Review Report, Computer Based Digital System Failures." AEOD/T94-03, July 1994.

[17] SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

[18] NUREG-0493. "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System." March 1979.

[19] NUREG/CR-6303. "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems." December 1994.

ACHIEVING HIGH AVAILABILITY FOR NEW PLANTS

(Session 4)

Chairman

T.J. PEDERSEN
Sweden

NEXT PAGE(S)
left BLANK

XA9848583

DEVELOPMENT AND COMPLETION OF THE FIRST ABWR AND FURTHER IMPROVEMENT

N. ANAHARA
Nuclear Power Engineering Department,
Tokyo Electric Power Co., Inc.,
Tokyo, Japan

Abstract

Unit 6 and 7 at Tokyo Electric Power Company's Kashiwazaki-Kariwa Nuclear Power Station are the first advanced boiling water reactor plants in the world, of which Unit 6 started up commercial operation in November 1996 and Unit 7 followed it in July 1997. This report describes the objectives of the ABWR development project that was decided on the basis of our experience in plant operation, discusses major features of the plant design adopted to achieve such objectives and the design and verification methods used for design improvements under the project.

1. INTRODUCTION

Currently Tokyo Electric Power Company has 17 nuclear power plants in commercial operation at three sites (the Fukushima Daiichi, Fukushima Daini and Kashiwazaki-Kariwa NPSs). These plants have a good track record of operational experience, attaining a capacity factor of 84.1% in fiscal 1996 which ended March 1997, with 3 (including preoperation plants) unplanned shutdowns. Fifteen of these TEPCO facilities are standardized, improved versions of three base plants.(BWR-3, BWR-4 and BWR-5) originally developed by General Electric Co. Meanwhile, the 16th and 17th plants (i.e., Units 6 and 7 of the Kashiwazaki-Kariwa NPS) are the Advanced Type BWR recently commercialized under our development project.

2.ABWR DEVELOPMENT PROGRAMS

As stated above, TEPCO's nuclear power plants maintain an excellent operation record these days but, in its early days of BWR introduction, the company could not always operate these plants satisfactorily. In the mid 1970s, in particular, our NPP operation was severely affected by such troubles as fuel leaks and stress corrosion cracking of stainless steel piping, resulting in a lower capacity factor, a higher radiation exposure rate of plant workers and an increased volume of radioactive waste.

Over the years, we gradually increased the electric output of NPPs from 460 MW (BWR-3) to 780 MW (BWR-4) and further to 1,100MW (BWR-5). The first plant of each of the three BWR versions was designed with the technology introduced from the United States under contract with GE. Then we signed contracts with Toshiba and Hitachi, both Japanese BWR manufacturers, for construction of the second and subsequent plants in a bid to build our NPPs essentially with domestic resources. Efforts were also exerted to improve our NPP technology reflecting the past operational experience while following GE's plant basic design. These improvement efforts helped gradually solve major problems we faced in our early days of NPP operation.

In the process of accumulating experience in plant design and construction, Japanese BWR vendors steadily raised their technological level. In view of such technological improvement in the country, we decided to actively push forward with the development of technology aimed at the best plant design conceivable at that time by integrating the superior technologies of BWR manufacturers in the world. Based on this concept, all BWR manufacturers of the world, comprising GE, Toshiba, Hitachi, ASEA Atom, and AMN, conducted a feasibility study on the development of a future BWR in 1978. This was the beginning of ABWR development.

After the conceptual design concept was thus decided on, a basic ABWR design was developed through a continued joint study by Japanese electric utilities operating BWR plants

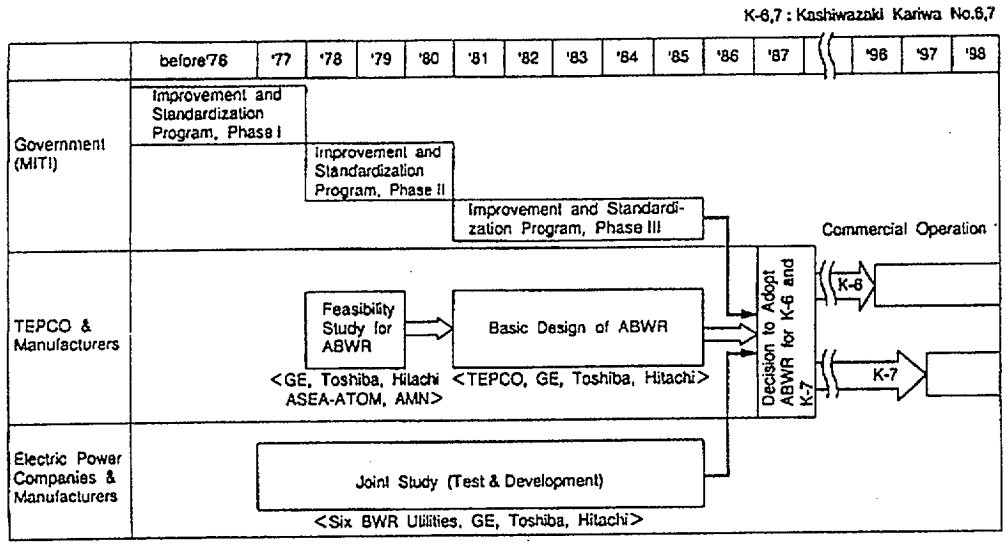


Fig.1 Mileston of ABWR Development

and three major reactor manufacturers - Toshiba, Hitachi and GE. At the same time, verification tests were conducted on improved designs of equipment to prove their applicability to actual plants. In 1987, we decided to use ABWRs for Units 6 and 7 of the Kashiwazaki-Kariwa NPS (See Fig. 1 for milestone of the ABWR development).

3.ABWR DESIGN OBJECTIVES

The following are the objectives of ABWR design set at the development stage:

- Enhanced safety and reliability
- Excellent operability & Maneuverability
- Improved Economy
- Reduced occupational radiation exposure and radioactive waste

To achieve these objectives, the strategy for the development was as follows:

- The-simpler-the-better

Compared with the pressurized water reactor, the BWR has greater potential in terms of safety and economical efficiency because of its simpler system configuration. Accordingly the ABWR project should seek higher safety and economical efficiency by further simplifying the plant systems.

- Setting of realistic goals

A huge development cost and a long demonstration period are needed to apply entirely new technologies to NPPs that are required to maintain high reliability. In principle, therefore, we decided to conduct an extensive survey on existing technologies already demonstrated in the world and to examine an optimal combination of systems that could fully meet our requirements.

- Reduction of operators' work load

Since reduction of plant operators' work load and human errors would contribute to the enhancement of plant reliability and safety, we intended to adopt improved technologies, especially electronics that is rapidly advancing now, for improvement of instrumentation systems as far as possible.

- Contribution to the solution of technical problems

An urgent task in the area of BWR technology in those days was to solve SCC of piping, lower the radiation exposure rate of plant workers and reduce the amount of radioactive waste. The ABWR project called for realization of a new plant that could solve these problems, and it was desired that research and development efforts for the proposed ABWR would lead to the improvement of existing BWR plants.

- Verification and demonstration of improved technologies

In order to prevent a setback in development activities and equipment troubles or malfunctions during plant construction and operation, it was decided that improved technologies to be adopted for ABWR plants in Japan should be exhaustively verified and demonstrated prior to the construction of the plants.

4.FEATURES OF ABWR DESIGN

The key features of the ABWR plant design include increased plant output, internal pumps for reactor coolant recirculation, fine motion control rod drives, simplified NSS system along with an improved emergency core cooling (ECC) system, advanced controls and instrumentation utilizing microprocessor based digital technology and multiplexed fiber optic signal transmission, a cylindrical reinforced concrete containment integrated with a compact reactor building, an improved turbine plant that utilizes a turbine design that includes 52-inch last-stage buckets, a two stage reheater, and both high and low pressure pumped-up drains. Table 1 summarizes the major plant specifications and compares them to the current BWR in Japan.

Table 1 Major Specifications Of ABWR

Item	ABWR	Current BWR
Electrical Output	1,356MWe	1,100MWe
Reactor Thermal Output	3,926MWt	3,293MWt
Reactor Pressure	73.1kg/cm²a	71.7kg/cm²a
Steam Flow	7,640t/hr	6,410t/hr
Feed Water Temperature	216°C	216°C
Core Flow	52×10⁶kg/hr	48×10⁶kg/hr
Number of Fuel Assemblies	872	764
Number Of Control Rods	205	185
Core Average Power Density	50.6kW/ℓ	50.0kW/ℓ
Diameter of RPV	7.1m	6.4m
Height of RPV	21.0m	22.2 m
Coolant Recirculation (Number Of Pumps)	Internal Pump(10)	External Recirculatiion Pump (2)
Normal Drive of CRD	Fine Motion Electric Motor Drive	Jet Pump(20) Hydraulic Locking Piston Drive
Scram Function of CRD	Hydraulic Piston Drive Electric Motor As Back Up	Hydraulic Piston Drive
Emergency Core Cooling System (ECCS)	DIV. I : RCIC+LPFL(RHR) DIV. II : HPCF+LPFL(RHR) DIV.III : HPCF+LPFL(RHR) ADS	DIV. I : LPCI+LPCS DIV. II : LPCI+LPCI DIV.III :HPCS ADS
Residual Heat Removal System	3 Trains	2 Trains
Primary Containment Vessel	Reinforced Concrete Containment With Liner	Self Standing Steel Containment
Turbine Cycle	TC6F-52"(2-Stage Reheaters)	TC 6F-41" (Non Reheat)

(1) Increased Plant Output and Turbine Design

The ABWR plant is designed for a rated thermal output of 3926 MWth with an electrical output of 1356 MWe. In order to improve plant efficiency, performance and economy, the turbine design incorporates a 52-inch last stage bucket design. Combined moisture separator / reheaters remove moisture and reheat the steam in two stages. Also to help increase plant output and reduce costs, the design has incorporated the concept of both high pressure and low pressure pumped-up drains. Rather than cascading the heater drains back to the condenser, the pumped-up drain system takes advantage of this waste heat and injects it back into the feedwater ahead of the heaters. This concept has increased the generator output nearly 5 MWe, has reduced the capacity of the condensate polishers.

(2) Reactor Vessel Incorporating Internal Pumps

The most dramatic change in the ABWR from previous BWR designs is the elimination of the external loops and the incorporation of internal pumps for reactor coolant recirculation. The reactor pressure vessel (RPV), and core internals have been optimized for the internal pump concept. As shown in Figure 2, all large pipe nozzles to the vessel below the top of the active fuel are eliminated. This improves the safety performance during a postulated Loss of Coolant Accident (LOCA) and allows for decreased ECCS capacity.

The RPV is 7.1 m in diameter and 21 m in height. The reactor vessel height and total volume have been minimized, which has resulted in reduced volume requirements for the containment and reactor building. In-service inspection (ISI) has been reduced by adoption of the internal pumps and elimination of the recirculation pipe nozzles and reduced amount of vessel welding during vessel fabrication. This will lead to radiation exposure reduction. Taking advantage of many design features and capitalizing on early General Electric separator performance test data, the separator stand pipes were shortened. The velocity limiter on the control blade was deleted due to the FMCRD design. Height of ABWR type RPV is 1.2 meter shorter than the current one by adopting these designs.

The ABWR incorporates ten internal recirculation pumps (see Figure 2) located at the bottom inside of the RPV. This simplifies the nuclear boiler system and satisfies compact space requirements of the RCCV and R / B. Elimination of the external recirculation loops has had many advantages. Key advantages are the reduction in containment radiation level compared to current plants, no rotating shaft seal by adopting wet motor design which can reduce leak potential, and the excess flow provided by the pump design allows for full power operation with one pump out of service.

(3) Fine Motion Control Rod Drive (FMCRD)

The ABWR incorporates the electric-hydraulic FMCRD, which provides electric fine rod motion during normal operation and hydraulic pressure for scram insertion.

The drive mechanism operates to allow fine motion (18 mm step size) provided by the ball screw nut and shaft driven by the electric motor during normal operation. The electric motor also provides increased reliability through diverse rod motion to the hydraulic scram and acts as a backup with motor run-in following scram. The fine motion capability allows for small power changes and easier rod movement for burnup reactivity compensation at rated power. It also reduces the stress on the fuel and enhances fuel rod integrity. Ganged rod motion (simultaneous driving of a group of up to 26 rods) and automated control significantly improves startup time and capabilities for load following.

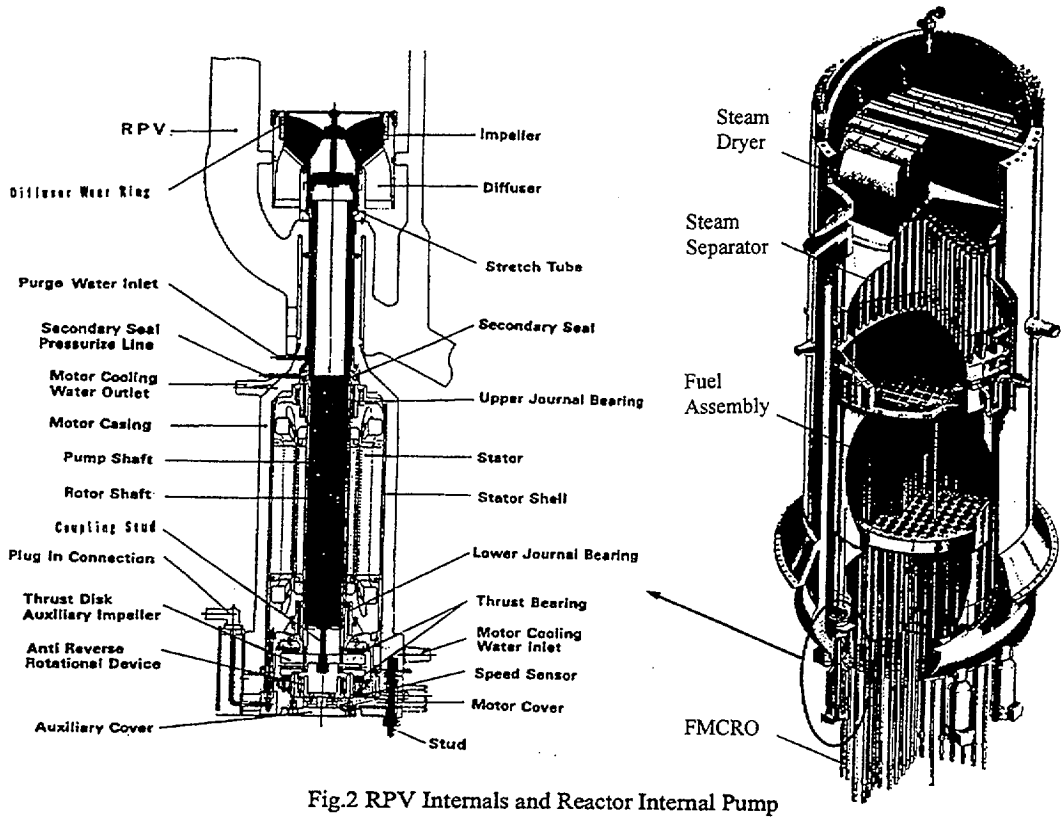


Fig.2 RPV Internals and Reactor Internal Pump

The ABWR FMCRD design has been developed from the European design by reducing the length and diameter, and by adding the fast scram function. Other design features are: (1) a two-section design for the CRD housing with the wearing parts concentrated in the compact spool piece section at the bottom of CRD in order to reduce both maintenance time and radiation exposure during maintenance. (2) The FMCRD scram water is discharged directly into the reactor vessel, eliminating the scram discharge volume and associated valves and pipings. (3) Continuous full in indication.

Figure 3 shows the outline of the FMCRD.

(4) Advanced Control and Instrumentation Systems

Digital technology and multiplexed fiber optic signal transmission technology have been combined in the ABWR design to integrate control and data acquisition of both the reactor and turbine plants. For the feedwater, recirculation, and pressure control systems, triplicated fault tolerant digital control is utilized, similar to Japan operating BWRs. A redundant design for the rod control and information system is used. These systems feature automatic self-test and built-in calibration and trip test to improve reliability. Microprocessorbased digital monitoring and control (DMC) has been implemented for most principal NSSS and Balance of Plant monitoring and control functions. ABWR DMC technical advantages include self-test, automatic calibration, user interactive front panels, full multiplex system compatibility, standardization of the man-machine interface, and where possible, use of common circuit cards.

The use of multiplexed fiber optic data transmission in the ABWR is another improved feature applying advanced technology. The use of fiber optic multiplexing reduces the amount of cabling and cable pulling time during construction. This also reduces the overall cost of the control and instrumentation area. Multiplexing easily provides a high degree of redundancy in the control system, and also improves maintainability.

(5) Containment and Reactor Building Design

For the ABWR the cylindrical RCCV, with its pressure suppression concept, was selected as the reference design of the primary containment vessel. The concrete walls of the RCCV are integrated with the reactor building and form a major structural part of this building.

The upper drywell encloses the reactor, and the process lines and valves of the reactor coolant system. The lower drywell, located under the reactor vessel, is the space for pump installation and maintenance of the internal pump motors, their heat exchangers, and the control rod drives. Personnel and equipment access are provided for by hatches in the upper drywell, and through access tunnels in the lower drywell.

The wetwell provides an air space and a pool to suppress the steam from the postulated LOCA. Multiple horizontal vents derived from the Mark III containment design discharge the vessel blow-down steam water mixture and the air from the drywell to the wetwell pool. The steam is condensed, and the fission products are scrubbed and retained in the pool.

Optimal arrangement of the containment such as internal pump adoption, horizontal vents design and lower drywell arrangement enabled the center of gravity of the reactor pressure vessel to be lowered and it contributed to making the reactor building more resistant against earthquakes together with the integrated design of RCCV and reactor building.

The ABWR design represents a very significant reactor building volume and cost reduction. The reactor building volume has been reduced to approximately 92,000 cubic meters compared to the latest 1100 MW plant (Kashiwazaki-Kariwa Unit 3). Figure 4 shows the outline of the RCCV.

5. CONSIDERATION GIVEN TO OPERABILITY AND MAINTAINABILITY

As mentioned in the paragraphs concerning the objectives of ABWR development, careful consideration was given to designs relating to plant operability and maintainability from the initial stage of the ABWR project. This section shows some examples of such consideration.

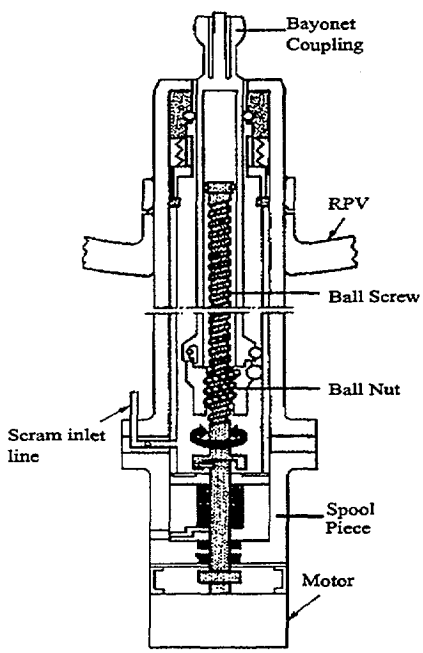


Fig.3 Fine Motion Control Rod Drive

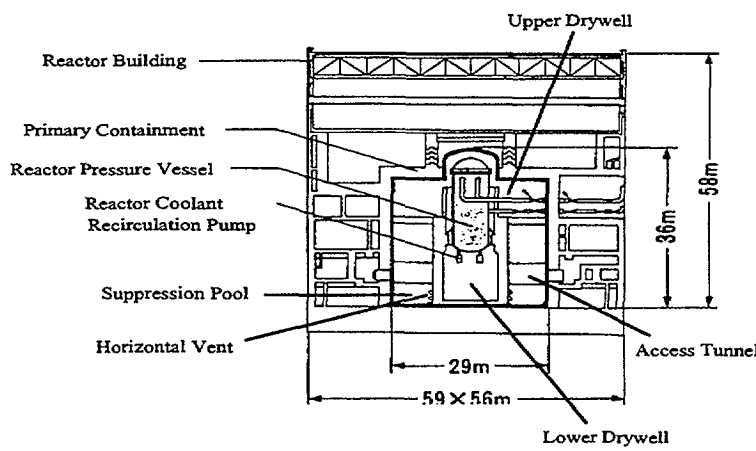


Fig.4 Reinforced Conrete Containment Vessel

(1) Consideration of Maintainability of Internal Pumps

Internal pumps are inspected in the lower part of drywell, but plant workers may be subject to serious radiation exposure during the overhaul of these pumps because particulates of cladding are settled in the lower plenum of reactor internals. In developing the proposed improved internal pump, therefore, efforts were exerted:

a. To adopt a purge system and a seal mechanism that could prevent the pump motor from coming into direct contact with reactor water during operation and maintenance ; and
b. To provide as much remote-control and automatic operation capabilities as possible for work in the lower part of drywell.

The devices in a. above were studied during the development of the internal pump itself. For the capabilities in b., steps were taken to carry out the design of handling devices, preparation of experimental devices and mockup tests, along with a study on the pump itself. Then those handling devices whose performance had been fully proven were installed in the plants.

(2) Consideration of FMCRD Maintainability

The fine motion control rod drive (FMCRD), which is also installed in the lower plenum of reactor internals, involves problems similar to those of the internal pump. Therefore, FMCRD also adopt a purge system for preventing reactor water from flowing into the control rod drive mechanism. In addition, handling maintenance devices were developed to provide remote-control and automatic operation capabilities for CRD inspection and maintenance as far as possible.

The conventional CRD has carbon seal rings, wearing materials, installed in its main body. These rings, with a service life of about seven years, are to be replaced during an annual plant outage and this has formed a critical path in the annual inspection. In developing the proposed FMCRD, therefore, arrangements were made to integrate all wearing items in the compact spool piece at the bottom of the CRD, so the inspection and maintenance of the FMCRD unit could be essentially carried out by maintaining these wearings in spool piece. This provided an effective tool to reduce the amount of CRD handling work, and to remove a CRD maintenance period from the critical path of annual inspections and lead to shortened outage period.

(3) Improvement of Operability

Under the ABWR project, efforts were made for the improvement of man-machine interfaces to achieve better plant operability. This subsection gives some examples of improvements in the main control room. Even the conventional main control console has been provided with significantly increased CRT displays, a hierarchical display system of warnings and some other new devices, reflecting lessons learned from 1979 Three Mile Island accident. In addition to these equipment, the following improvements were incorporated in the ABWR plants:

- Significant improvement of the display system for the main control console
  All operators in the main control room can share important information on plant operations promptly and accurately by the use of the large screen display panel instead of oral communication in current plant.

- Reduction of a load occurring immediately after a scram
  Based on the result of operator workload analysis, recovery operations following scrams and the ordinary control rod operations demand a considerable amount of work by operators. These items have been automated in order to enhance operator support functions of the system. Thus, the number of actions required by operators diminishes and more reliable operation of the plan can be expected.

- Reduction of shift operators' lines of motion during operation
  In order to minimize operators' movement required for operation and supervision during normal operation of the plant such as startup and shutdown, a compact main control console with 7 m width is used to integrate important supervising and controlling functions.

These improvements provided the ABWR plants with better operability than that of conventional BWR plants.

(4) Consideration of Maintainability using 3-D CAD

As noted earlier, the ABWR plants were designed to reduce the total amount of required materials through the rationalization of equipment and facilities, leading to the reduction of building volume.

Amid these rationalization efforts, an attempt was made to ensure sufficient maintainability for the equipment of the ABWR. A review was carried out using the computer-aided design that had been used since the basic design stage of the project with the participation of TEPCO to find whether the required inspectability and maintainability were secured for the plant equipment and whether sufficient accessibility were given to each equipment. The review was divided into 2 phases; one (the first review) was conducted at the final design phase of the arrangement of main equipment and the layout of large-diameter piping, and the other (the second review) was performed when the designs of such components as operating stages and small piping were fixed.

After the project entered the construction stage, a joint team of inspectors formed by the assigned TEPCO personnel and the plant manufacturers' technical staff carried out another three-phase review (first prior to the completion of the reactor pressure boundary, second prior to fuel loading and third prior to the commercial operation) at the construction site, according to progress in equipment installation, to review the performance of equipment mainly in respect of maintainability, accessibility and operability.

6. PROPER REVIEW, VERIFICATION AND DEMONSTRATION OF IMPROVED DESIGNS

Improved designed plant systems and components were properly verified and demonstrated mainly through design review, model tests and full-scale tests prior to their installation in the plant.

(1) Verification and Demonstration of Internal Pump

A European product was used as the basis of the proposed improved internal pump. The base pump was imported from the European manufacturer and its design was subjected to the following exhaustive verification in Japan:

- Hydraulic characteristics and continuous operation tests
- Operation tests under severe conditions (an operation test under cavitation conditions and another operation test with cooling water shut off)
- Overhaul of the pump after tests above

Along with these examinations, an in-vessel dynamic flow test was conducted in view of a predicted change in the lower structure of the reactor pressure vessel resulting from the use of the new internal pump.

Through these activities a high reliability and improved internal pump was developed.

(2) Verification and Demonstration of FMCRD

A European product was also used as the basis of the proposed FMCRD. The base CRD was imported from the European supplier and its design was subjected to the following exhaustive verification:

- Performance test and life time test
- Scram test during seismic condition

- Operation test under severe condition (CRD performance test with cladding particulates getting into the CRD and with CRD driveline misalignment)
  In addition, a FMCRD was installed at the U.S. plant (La Salle-2) for one fuel cycle and the reliability of the system and mechanism was verified by a practical test.

7. CONSTRUCTION AND PREOPERATION TESTING OF ABWR PLANTS

Following the finalization of the ABWR design through the verification and demonstration work described above, we decided in 1987 to use the ABWR for Units 6 and 7 of the Kashiwazaki-Kariwa NPS. Compared with the 48-month standard construction time for ABWR plants (from a bedrock inspection to the commercial operation), the construction period for these two units was extended to 52 months, taking into account the winter weather conditions at the NPS site (e.g., heavy snowfalls and strong winds resulting in lower efficiency of construction works in winter) and the need to provide a sufficient preoperation period for these units which are the first ABWR plants in the world.

After going through the prescribed licensing procedure, we started construction works on Unit 6 in September 1991 and on Unit 7 in February 1992. The construction and preoperation testing of these plants progressed smoothly, with Unit 6 fuel loading in November 1995 and starting up commercial operation in November 1996. Meanwhile, Unit 7 was loaded with fuel in October 1996 and put in commercial operation in July 1997. The two plant projects were carried out ahead of the original progress schedules, and the construction period from the bedrock inspection to the startup of commercial operation was reduced to 51 months (in the case of Unit 6). Based on these actual results, we predict, the next ABWR plants will be built within 48 months.

Although Units 6 and 7 were the first ABWR plants ever built in the world, their preoperation testing was carried out smoothly because of sufficient verification and demonstration tasks performed at the design stage. After the initial fuel loading, Unit 6 suffered two nonscheduled shutdown and Unit 7 suffered one, none of which was attributed to the malfunction of improved designed equipment peculiar to the ABWR.

8. FURTHER IMPROVEMENTS

As stated in the foregoing sections, two ABWR plants were put inservice as new operational units of the Kashiwazaki-Kariwa NPS. There are plans to build eight additional ABWR plants in Japan and two others in Taiwan in the near future.

In the United States, meanwhile, the Nuclear Regulatory Commission approved the design certification of ABWR last May.

From these developments of the situation, it is expected, the ABWR will become the standard type of BWR. In addition, it is predicted, a more advanced version of the present ABWR will be commercialized in the 2010s when the BWR plants now inservice are likely to be replaced with new ones. With this in view, Japanese electric utilities operating BWR plants and three major plant manufacturers - Toshiba, Hitachi and GE - launched a research project for further improvement and development of the ABWR in 1990. The project covers three major themes:

- Further improvement in economy
- Optimized design including the reactor building, turbine building and the BOP
- Development of new technologies

Based on these themes, the project partners are conducting studies for further improvement of the ABWR in terms of thermal output, safety, reliability, improved economy and operability.

REFERENCES

[1] TOMONO K.et al.,1992, "Technological Innovations in Advanced Light Water Reactors (ABWR & APWR) in Japan", Proceedings, The 8th Pacific Basin Nuclear Conference.

[2] TOMONO K.et al.,1990, "Development and Application of Advanced Boiling Water Reactors", Proceedings. The 7th Pacific Basin Nuclear Conference.
[3] SAWYER C.D. et al.,1997, "Current Status of Next Generation Reactor Concept Study" , Proceedings, ICONE-5 Conference, Nice, France, May, 1997

XA9848584

ADVANCED PLANT ENGINEERING AND CONSTRUCTION OF JAPANESE ABWRs

N. GOTOH, J. SUMIKAWA, N. YOSHIDA, M. YOSHIDA
Nuclear Plant Engineering and Construction Department,
Hitachi Works, Hitachi Ltd,
Ibaraki, Japan

Abstract

Remarkable improvement -has been made in recent nuclear power plant design and construction in Japan. These many improved engineering technologies -has been made a good use in the lately commercial operated two world's first 1,356MWe ABW's (Advanced Boiling Water Reactors), and made a great contribution to the smooth progress and the completion of the highly reliable plant construction. Especially, two engineering technologies, (l), three-dimensional computer aided design system through engineering data-base, and (2), large scale modularising construction method, have been successfully applied as the -integrated engineering technologies of the plant construction.

And two integrated reviews, "integrated design review, confirmation of new and changed design and prevention of failure recurrence" in the design stage, and "constructing plant review" at the site, have been widely and systematically conducted as a link in the chain of steady reliability improvement activities.

These advanced and/or continuous and steady technologies are one of most important factors for high reliability through the entire lifetime of a nuclear plant, including planning, design, construction, operation and maintenance stages.

1. INTRODUCTION

In Japan, continuous efforts have been made to improve the design, the construction, the operation, and the preventive maintenance technologies applied to nuclear power plants. Consequently, high reliability through the entire plant lifetime has been featured, and a higher load factor, a smaller unscheduled outage number and a shorter periodical inspection time have became possible in Japanese nuclear power plants.

Various high and improved technologies based on past experience, research and development and accumulated data were certainly applied to the design, the construction and the plant data management of Japanese two 1,356 MWe ABWR power plants which began commercial operation on Nov. '96 and July '97. The construction of these plants are recognized to have completed with high quality and reliability.

Especially, from the viewpoint of plant design and construction engineering,

- three-dimensional computer aided design (3D-CAD) system with engineering data-base
- large scale modularizing construction method using large capacity lifting device

are worth giving attention as successful technologies.

And in Hitachi, the high quality engineering and the reliability improvement activities have been continuously performed using computerized "Integrated Reliability

Management System for Nuclear Power Plant" with centralized managed data-base, and two integrated reviews ,

- integrated design review
- constructing plant review at site

from various viewpoints at some key stages have been systematically conducted as a part of those activities in CO-operation with each other of design, fabrication, construction and quality assurance (QA) sections.

This paper describes these outlines, features and some examples as follows.

2. IMPROVED TECHNOLOGIES FOR PLANT DESIGN AND CONSTRUCTION

2.1. Three-dimensional Computer Aided Design (3D-CAD)

At present, what is called " 3D-CAD system" is widely applied to nuclear power plant layout design in which objective plant facilities are visually modeled by using three-dimensional computer graphic function.

Though there are some general-use 3D-CAD systems in the world, Hitachi have practically used own developed and customized system functionally reflected own plant design practice. The system configuration is shown in Figure 1. The centralized managed design data in engineering data-base easily enable wide and effective data applications, for instance preventive maintenance planning (accessibility, maintainability, etc.) and construction work planning (installation procedure, equipment set-on /carry-in, temporary scaffolding, etc.). The 3D-CAD system with engineering data-base has became indispensable to the high quality plant layout design.

Particularly, the carefully considering and executing items using this system at the design stage with the intention of putting the higher reliability into operating plant are as follows.

(1) To insure the passability and the accessibility

- · · · the indication of pass and access space on graphic model, the restriction of arrangement planning into those spaces, and the confirmation of these abilities by simulation function (Figure 2)

(2) To insure the operability, the maintainability, and disassembly / inspection ability

- · · · the indication and confirmation each needed spaces same above, and the check & review by maintenance / inspection staffs (Figure 3)

(3) To insure the easiness and/or reasonableness of installation procedure

- · · · the indication of site work points (weld point, interference point, etc.), and the check & review and the work planning by work staffs

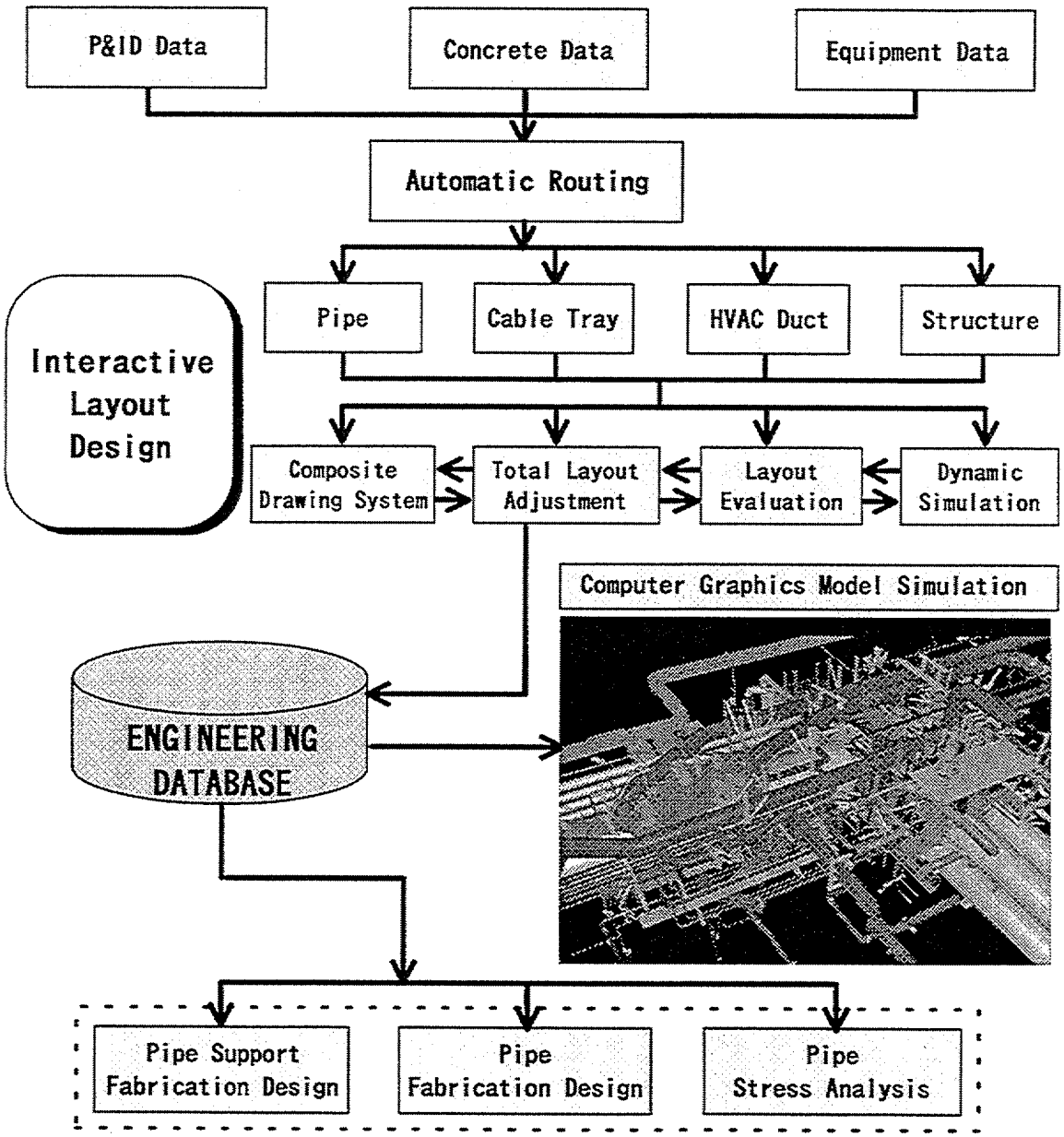


FIG. 1. System Configuration.

And, the 3D-CAD design with high accuracy and the application technique of consistently managed data in the engineering data-base enable to adopt the large scale modularization method in the construction stage shown in following section.

This engineering data-base is very effective to not only plant design and construction but also plant data management, preventive maintenance, and improving design, etc. (Figure 4), and its widely practical use through the entire lifetime of a nuclear plant will be greatly expected.

2.2. Large Scale Modularization Method

There is a modularizing construction method in which each parts are pre-fabricated and combined up to adequate size at factory, yard, and in-site assembly area, etc. instead of

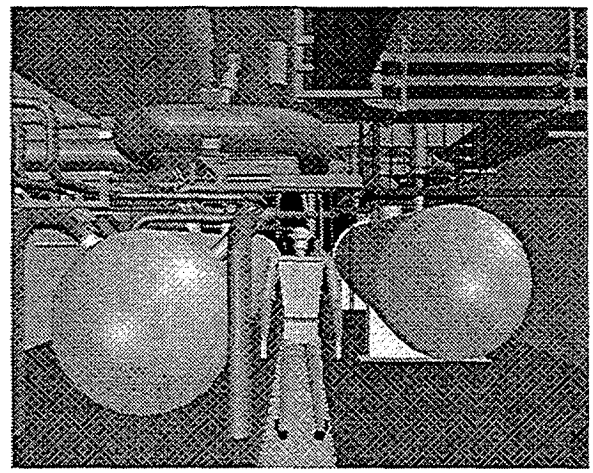


FIG. 2. Access Simulation.

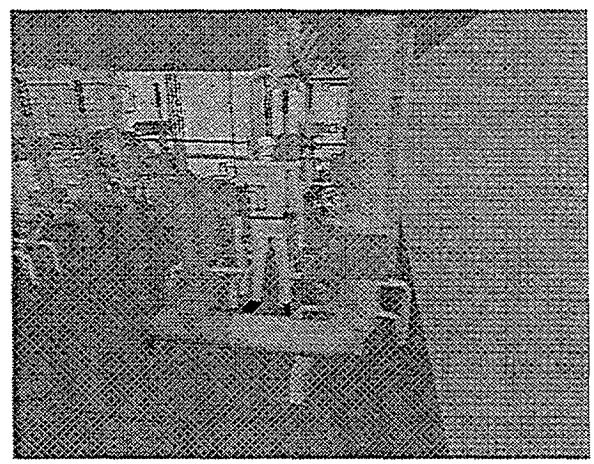


Fig. 3(a). Operability Review.

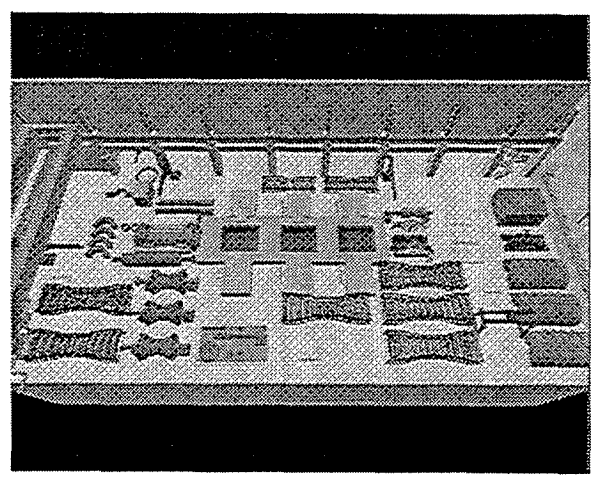


FIG. 3(b). Equipment Removal Simulation.

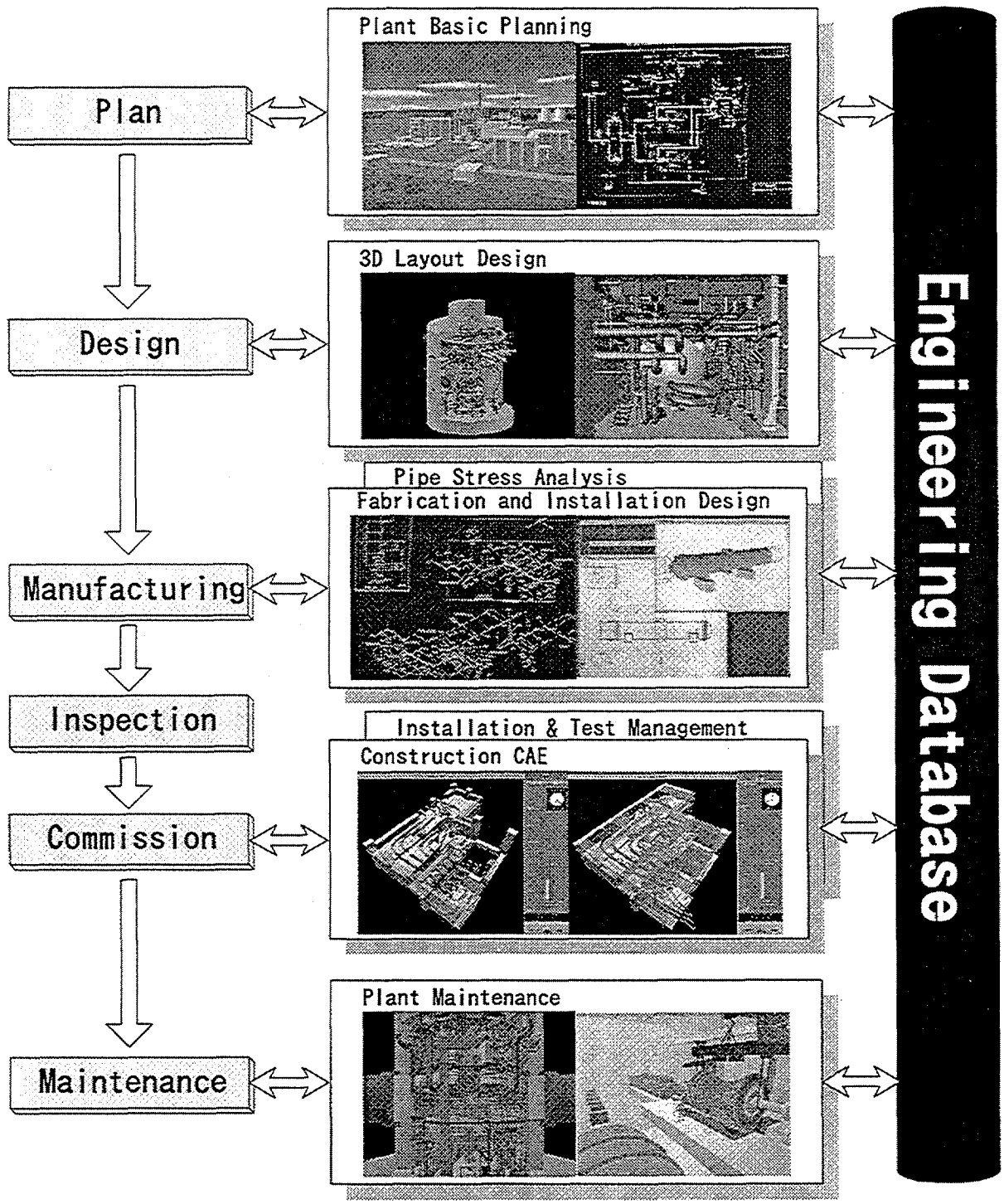


FIG. 4. Plant Integrated CAE System.

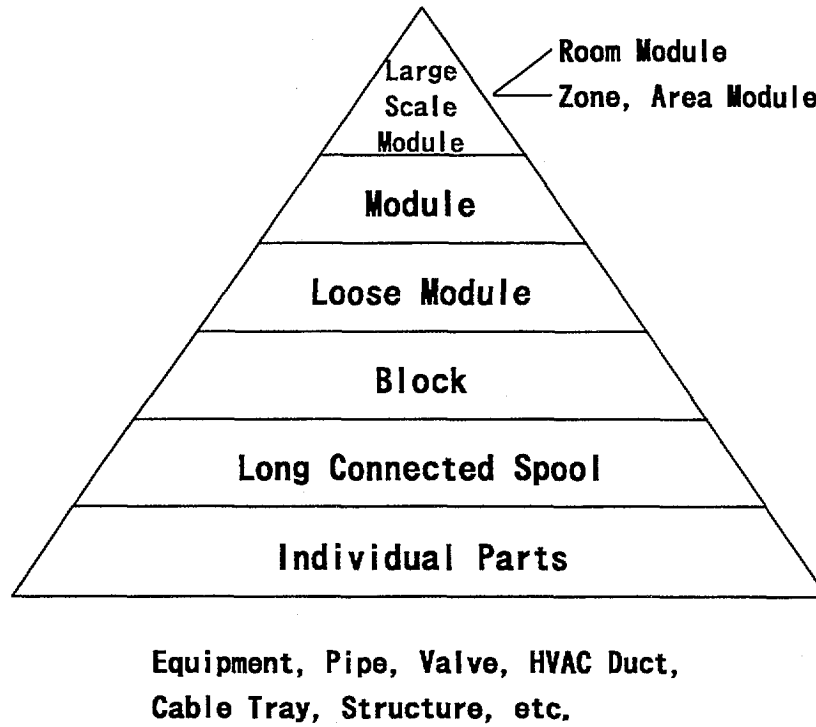


FIG. 5. The Concept of Modularization.

conventional method constructing each parts by parts at the final setting point. In the "Large Scale Modularization Method", each parts are more pre-fabricated as larger and/or higher completed as practicable, and lifted up at a stroke and down to final installation point using a large capacity lifting device.

The merits of the modularization from the viewpoint of plant reliability improvement are summarized below.

- To obtain higher quality and accuracy through better conditioned work
  (workability, fabricating devise & tool, and other surroundings)
- To average human resource and resultantly preserve quality potential

Also considering other purposes and merits, the expansion, the size enlargement and the higher pre-completion of modularization are being oriented. The concept and the actual results of modularization are shown in Figure 5 and 6 respectively. Especially, super large scale module, whole room module and combined module with civil parts are situated at the top of the concept of modularization, and to be standardized in future nuclear plant construction.

This large scale modularization is accomplished by using large capacity lifting device (e.g. 1,000 ton cap. giant crawler crane or 130 ton cap. tower crane) in addition to related various technologies such as high accurately optical measuring of interface point with the strong support of 3D-CAD design.

Outlined below are typical results of the modularization.

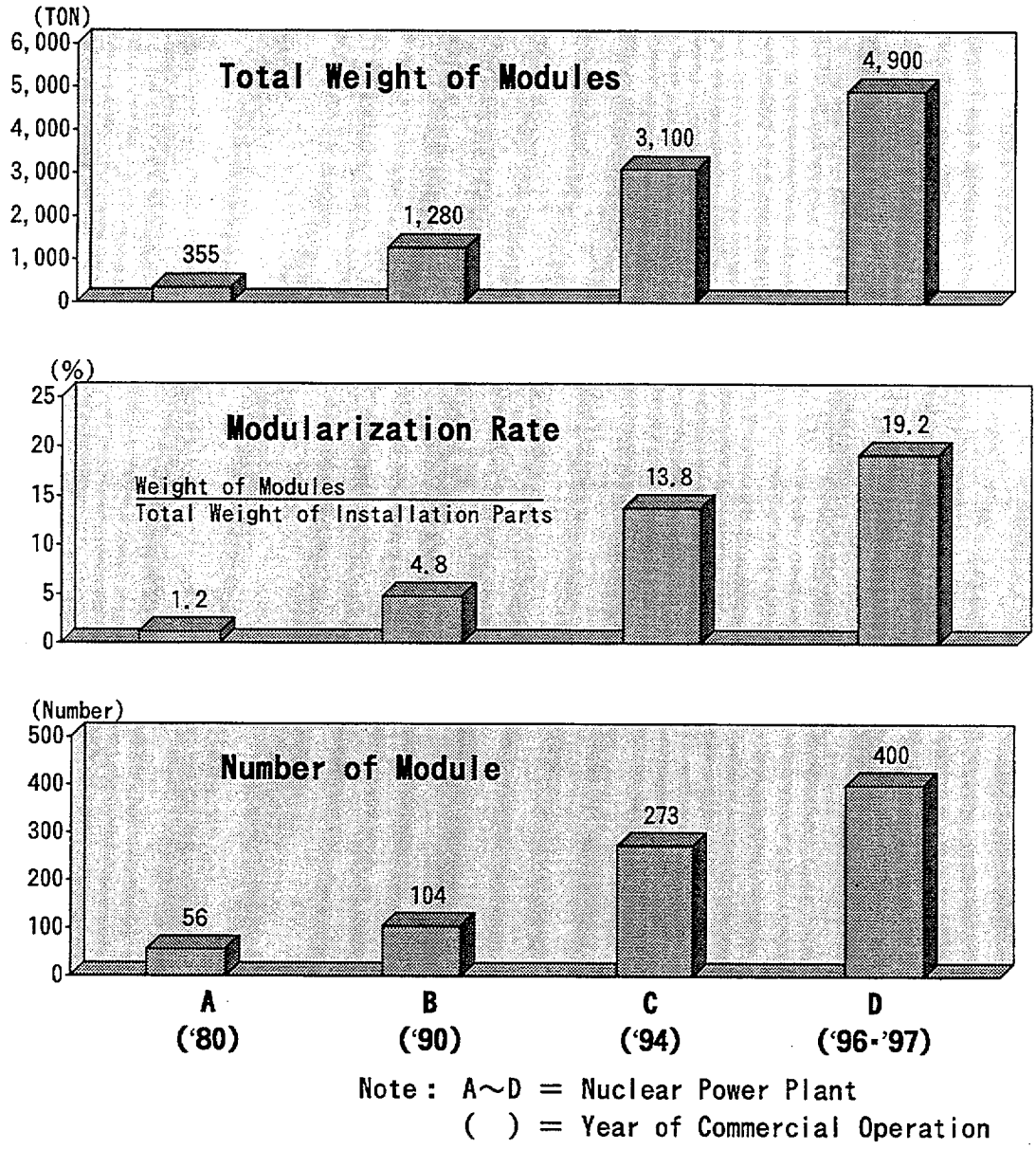


FIG. 6. Actual Result of Modularization.

(1) Upper Drywell Super Large Scale Module

This is the heaviest and most complicated module for the purpose of the avoidance of critical pass and the high quality fabrication under good condition. It consists of γ-shield wall, pipes, valves, cable-trays, air-ducts and their support structures, and weights 650 tons. (Figure 7 ,8)

(2) Whole Room Module

Two rooms were successfully modularized with the combination of civil structures, rebars and mechanical / electrical equipments and parts (weight: 300 tons and 440 tons). (Figure 9)

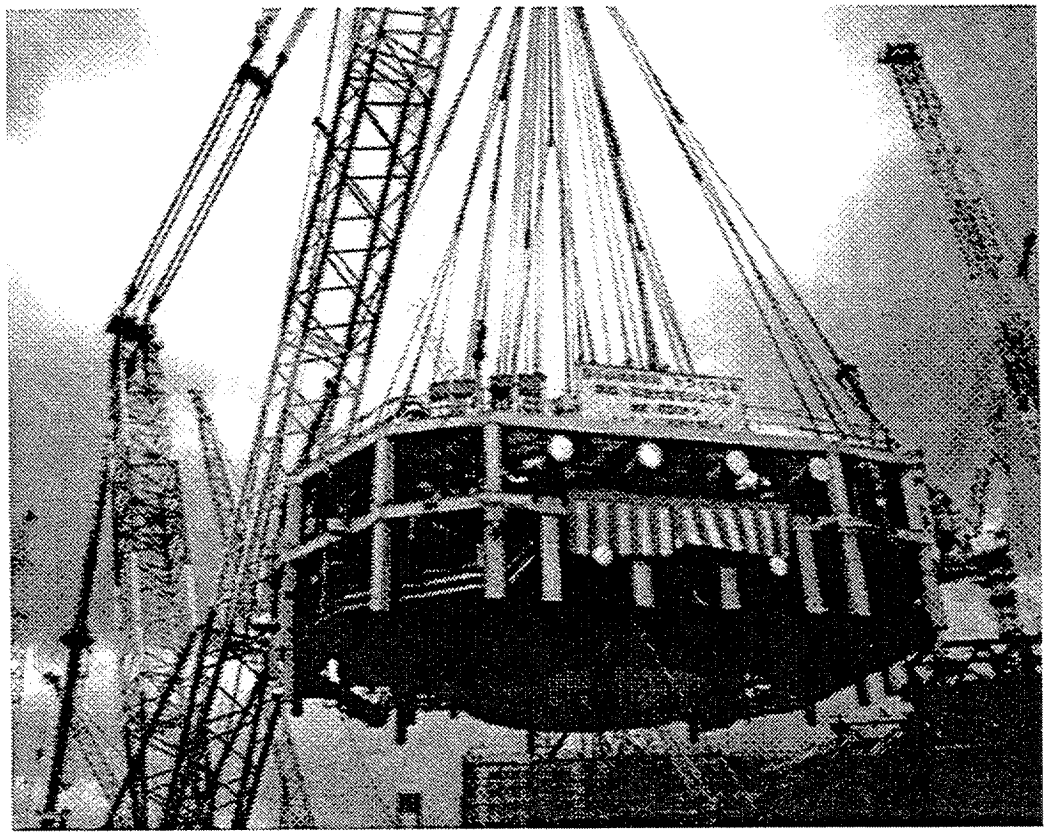


FIG. 7. RCCV Module.

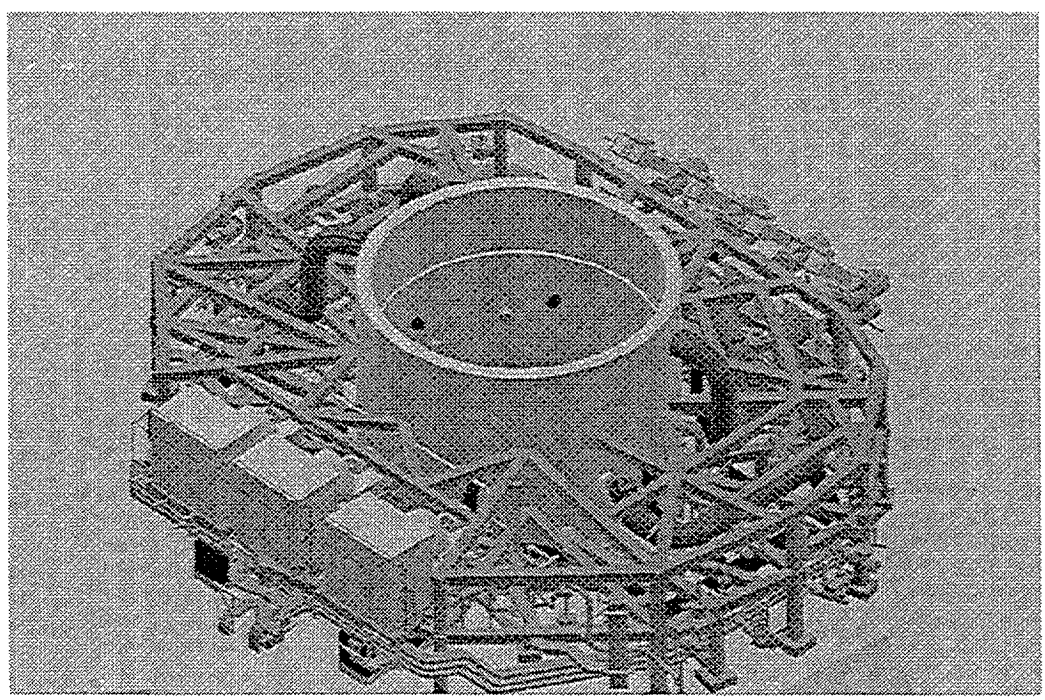


FIG. 8. RCCV Module CAD Model.

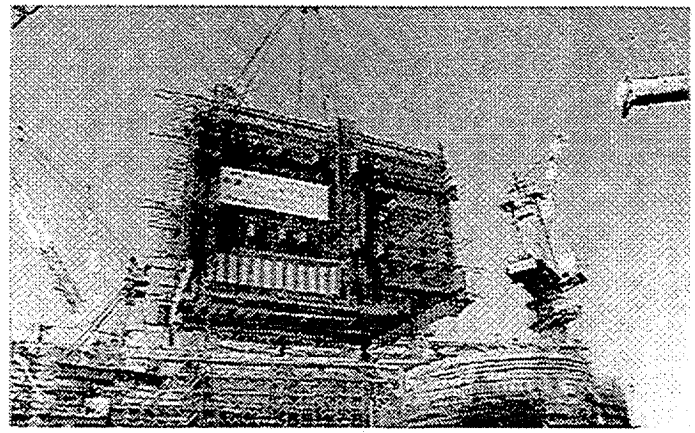


FIG. 9. Room Module.

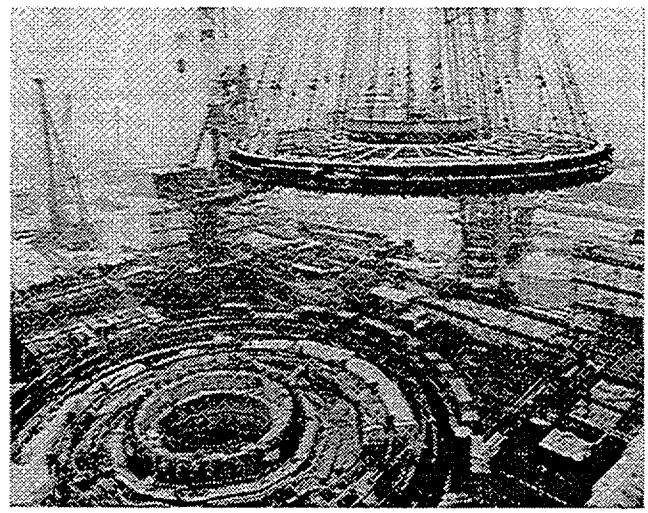


FIG. 10. Top Slab Module.

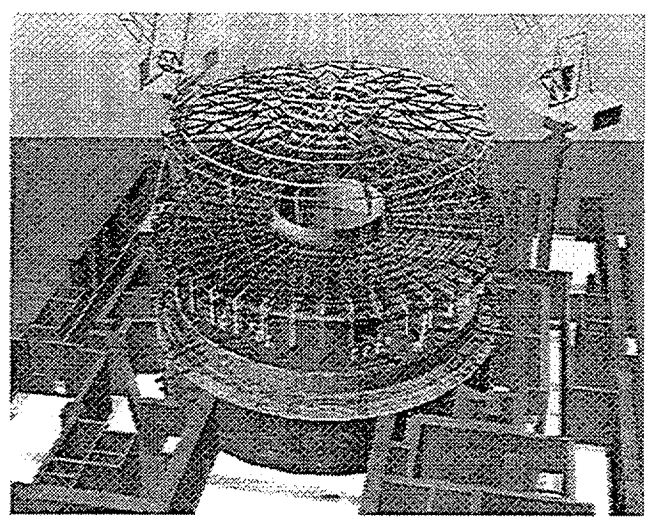


FIG. 11. Top Slab Module CAD Model.

(3) Reactor Building Center Mat Module and RCCV Top Slab Module

These two complexly overcrowding parts, a combination of civil structures, rebars, and mechanical equipment foundation, were formed into large modules in a yard adjacent to reactor building, and carried onto the each locations. (Figure 10, 11)

The above (1) is featured as super large scale and high completed and (2), (3) are civil combined modules, and again, the modularization is oriented as the one of most effective method in future nuclear plant construction.

Additionally, structural simplification of nuclear plant buildings to be easily modularized will be a important theme to be realized in the future.

And for reference, general ideas of improvement of new and future plant construction including the modularization method are shown in supplemental figure and table.

3. RELIABILITY IMPROVEMENT ACTIVITIES FOR NEW CONSTRUCTING PLANT

3.1. Integrated Design Review

The reliability of each design is insured through activities based on the quality assurance system for nuclear plant construction. The " Integrated Design Review" is a re-check of design contents on the final design stage with informed people, and concretely, these two items,

- contents of prevention of failure recurrence
- contents of new and modified design

are mainly confirmed.

(1) Confirmation of prevention of failure recurrence

In the integrated design review, the status of previous failure prevention which is counter-measured and/or re-designed at each design stage is reviewed in a sense of final check.

(2) Confirmation of new and modified design (design change)

New designs and/or design changes are usually done on account of the development and the improvement of system, equipment and various technologies, and site unique conditions. The status of activities to prove the appropriateness of those design changes is reviewed in the integrated design review.

3.2. Constructing Plant Review at Site

The integrated site review on some key stages of construction progress are conducted with related sections, and pointed out facilities are modified if needed. Those key stages and review contents are shown below.

- Before 6.9 kv power receiving
  - prior check of power related facilities preparatory to first power receiving

- Before reactor pressure vessel pressure test
  - · · · general check of installed mechanical equipment and facilities at the peak time of constriction work
- Before fuel loading
  - · · · general check of installation completed plant facilities
- Before commercial operation
  - · · · general check of plant facilities during or after partial and/or full power test operation

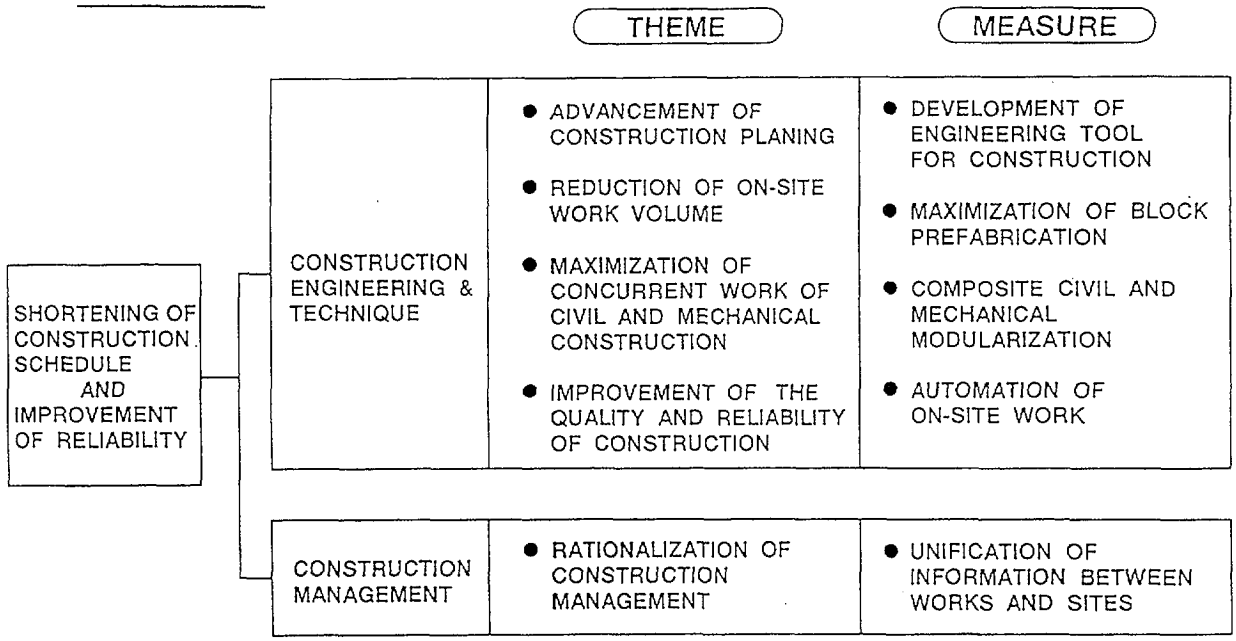
In addition to two integrated reviews above, the task force activities are practiced to check and review procedures and results of various start up tests. To effectively manage and control these many plant reliability related data and information, the computerized "Integrated Reliability Management System for Nuclear Power Plants" are being functionally operated as a supporting tool of reliability improvement activities.

4. SUMMARY

To improve availability and reliability of nuclear power plant, it is quite necessary that reliability related items and technologies are considered and potentialized into design and construction work with taking account of the entire plant lifetime. From this viewpoint, our improved technologies applied to the lately commercial operated world's first ABWRs' design and construction are outlined above.

Conclusively, under continuous reliability improvement activities, 3D-CAD plant layout design with engineering data-base and large scale modularization method with large capacity crane are greatly effective for reliable plant design and construction, and they, therefore, should be more improved and rationalized as one of major technical field in nuclear plant engineering.

SUPPLEMENT



IMPROVEMENT OF THE PLANT CONSTRUCTION

Table IMPROVEMENTS OF NEW CONSTRUCTION TECHNOLOGY

VIEWPOINT	NEW TECHNOLOGY
MAXIMIZATION OF CONCURRENT WORK	● RPV DIRECT-ON BY SUPERLARGE CRANE ● Q-DECK SYSTEM FOR FLOOR SLABS ● PREFABRICATED STRUCTURAL UNITS FOR MAIN CONTROL AND ELECTRIC PANEL ROOM ● POOL LINING UNITS ● COMPOSITE CIVIL AND MECHANICAL MODULARIZATION ● T-G PEDESTAL BEAM AND ANCHORBOLT MODULARIZATION ● CONCURRENT WORK OF CIRCULATING WATER PIPE AND BASEMAT
REDUCTION OF ON-SITE WORK VOLUME	● VERTICAL EXCAVATION METHOD (TIE-BACK TECHNIQUES) ● PREFABRICATION OF REBARS ● PREFABRICATION OF LARGE SCALE PCV BLOCKS ● STRUCTURE, EQUIPMENT AND PIPING MODULARIZATION ● EXTENSIVE APPLICATION OF BENDING PIPE
IMPROVEMENT OF WORK PRODUCTIVITY	● AUTOMATIC CABLE PULLING MACHINE ● AUTOMATIC WELDING MACHINE ● AUTOMATIC TUBE LOADING MACHINE FOR CONDENSER

DESIGNING FOR NUCLEAR POWER PLANT MAINTAINABILITY AND OPERABILITY

XA9848585

T.J. PEDERSEN
Nuclear Systems,
ABB Atom,
Västerås, Sweden

Abstract

Experience has shown that maintenance and operability aspects must be addressed in the design work. ABB Atom has since long an ambition of achieving optimised, overall plant designs, and efficient feedback of growing operating experience has stepwise eliminated shortcomings, and yielded better and better plant operating performances. The records of the plants of the latest design versions are very good; four units in Sweden have operated at an energy availability of 90.1%, and the two Olkiluoto units in Finland at a load factor of 92.7%, over the last decade. The occupational radiation exposures have also been at a low level. The possibilities for implementing "lessons learned" in existing plants are obviously limited by practical constraints. In Finland and Sweden, significant modernisations are still underway, however, involving replacement of mechanical equipment, and upgrading and backfitting of I&C systems on a large scale, in most of the plants. The BWR 90 design focuses on meeting requirements from utilities as well as new regulatory requirements, with a particular emphasis on the consequences of severe accidents; there shall be no large releases to the environment. Other design improvements involve: all-digital I&C systems and enhanced human factors engineering to improve work environment for operators, optimisation of buildings and containment to decrease construction time and costs, and selection of materials as well as maintenance and operating procedures to reduce radiation exposures even further. The BWR 90 design was offered to Finland in the early 1990s, but development work continues. It has been selected by a number of European utilities for assessing its conformance with the European Utility Requirements (EUR), aiming at a specific EUR Volume 3 for the BWR 90. Some characteristics of the ABB BWRs, with emphasis on features of importance for achieving improved economy and enhanced safety, are described below.

1. INTRODUCTION

The operating records of ABB BWR plants show high plant availability and power production reliability. A prerequisite for such achievements is a good basic design of the plant; not only with respect to systems performance and component reliability, but also a design which from the beginning has taken the needs for maintenance and service into consideration. Facilitated maintenance work normally yields shortened outage time for refuelling and maintenance, and generally, an improved quality of maintenance work - with better prospects for an undisturbed period of power production to follow.

Designing for low occupational radiation exposure doses for maintenance personnel is a natural part of the "ease of maintenance" design; experience clearly shows that a low radiation exposure is important with respect to proper maintenance activities. With respect to costs, it should be born in mind that a key lesson learned from the operating history of nuclear power plants is that the total life cycle cost is a much more important economic factor than the initial investment cost.

The operating utility quite obviously has a profound influence on the performance of a specific plant with respect to availability, power production reliability, occupational radiation exposure to plant personnel, etc. since the utility is managing the maintenance work as well as the operating procedures. But even a proficient utility will have difficulties in achieving high availability and reliability figures, if the plant design does not address this aspect properly.

A suitable plant design covers many different aspects - the design of the various systems, the choice of materials and components, their installation, radiation shielding, accessibility to components, transport routes, proper routing of ventilation air, general building arrangement, etc. The end result will always represent a compromise between a number of concerns, and co-operation with and continuous feedback from the operating utilities are of paramount importance for the development of new designs.

It is difficult to discuss "suitable plant design" aspects in a general way, and therefore, the BWR 90 and its reference plant, the Oskarshamn 3 plant (of BWR 75 design) in Sweden - in operation since 1985, are utilised for examples; measures taken to facilitate easy and proper maintenance are discussed with respect to different parts and systems of these plants.

2. THE BWR 75 AND BWR 90 DESIGNS

The BWR 75 design which was developed in the mid 1970s, represents an overall plant design, including the turbine plant and balance-of-plant systems, based on the experience gained from the design, construction, and operation of earlier ABB Atom plants, including turn-key deliveries. The need for improvement of structures, systems and components was evaluated by a special task force, putting emphasis on both operational, safety and maintenance aspects.

The BWR 75 design effort focused on providing a plant that would provide owner a good basis for a good operating economy with low radiation exposures to the crew and maintenance personnel, as well as low releases to the environment. The objective was to comply with the most stringent safety requirements while at the same time trying to avoid the tendency of some requirements to negatively impact the plant availability. Specific design objectives included:

[1] simplicity by avoiding complicated designs of systems and components;

[2] identification and elimination of weak points;

[3] design work bearing in mind the function of the plant as a whole, based on ABB Atom experience as reactor vendor and architect engineer, as well as turn-key supplier for complete plants, and observing that the split responsibility reported in a number of plants by other vendors had, beyond doubt, been a source for many interface problems and shortcomings; and

[4] maintainability and accessibility of systems and components addressed in parallel with the systems design work - a special group is regularly assigned to this task in ABB Atom development work.

The development of the BWR 90 design [1] started in 1986 as a review of "lessons learned" from projects with the previous plant design version, the BWR 75 in Finland and Sweden; in particular, from design and commissioning of the third units at the Forsmark and Oskarshamn nuclear power stations in Sweden. The development work was conducted in co-operation with the Finnish utility TVO (Teollisuuden Voima Oy), the operator of two BWR 75 plants, ensuring an efficient feedback of operating experience.

The basic design was developed by making specific changes to the design of the reference units, Forsmark 3 and Oskarshamn 3; a main emphasis in the development work was to maintain "proven design" features, unless changes would yield improvements and simplifications. This development approach follows the traditional ABB way of cautious step-by-step improvements rather than dramatic changes. The efficiency of this process is supported by the performance records of the operating plants; the annual "energy availability" for the four BWR 75 plants in Sweden, - the Forsmark 1, 2 and 3 and the Oskarshamn 3 units, - averages 90.1% over the last decade, and the two TVO units, the Olkiluoto I and II, are among the best performing nuclear power plants in the world; last year's capacity factors were 92.5 and 95.1%, respectively, and the average over the last ten years is 92.7%. Annual occupational radiation exposure figures are also low for the six units.

The basic design has been completed, and it was offered to Finland in October 1991, as one of the contenders for the fifth Finnish nuclear power plant project. The result is a plant with reduced building volumes, shortened construction time and decreased amounts of systems and components. Measures for simplified operation, testing and maintenance have been included, and the new design thus offers lowered costs and more simple operation.

The BWR 90 design is characterised by the use of internal recirculation pumps, fine motion control rod drives, and extensive redundancy and separation of safety systems in the same way as its predecessor, the BWR 75 design. For the BWR 90, modifications were made to adapt to technological progress, new safety requirements and to achieve cost savings.

There is one easily distinguishable departure from previous designs, however; the containment arrangement. In the new design, the piping connections between the drywell and the condensation pool in the wetwell are accomplished in a quite different way, and design measures to cope with a "degraded core" accident have been incorporated (by provision of a core catcher arrangement and filtered venting for the containment), in order to ensure that public and environment will be protected even in the event of a degraded core accident situation. This way the "remaining risk" for the public is reduced to an extremely low value.

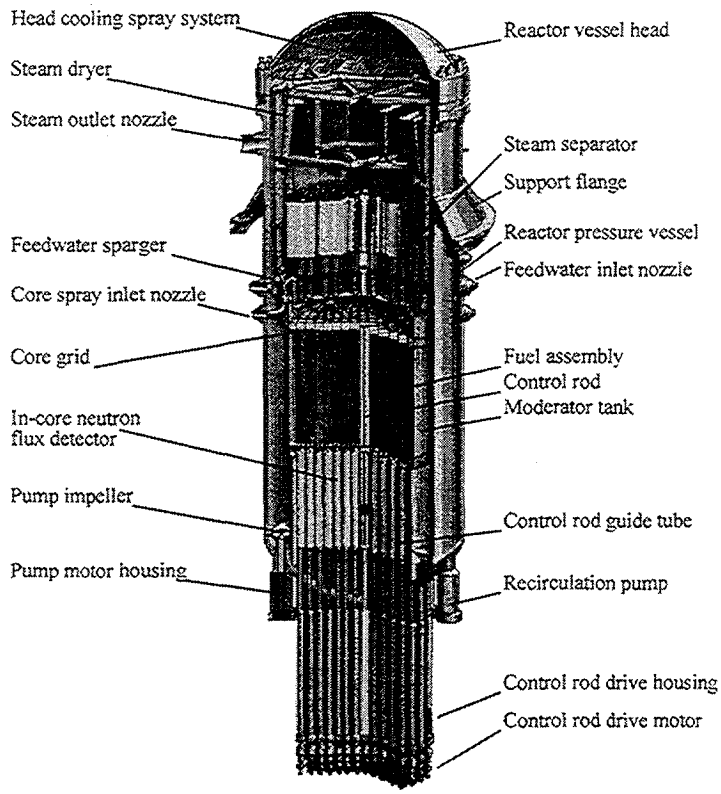


FIG. 1. BWR 75 - Reactor pressure vessel and internals

The thermal power rating of the base version is 3,800 MW_{th}, supplemented by a smaller version of 3,300 MW_{th}. The BWR 90 takes advantage of the margins that are gained by utilisation of a newer generation of ABB BWR fuel, which differs from earlier versions by the use of thinner fuel rods, yielding a significant increase in total fuel rod length and surface and a corresponding decrease in average heat rate and surface heat flux.

3. THE REACTOR PRESSURE VESSEL AND ANCILLARIES

The central - and largest - component in a BWR reactor plant is the reactor pressure vessel (cf. FIG. 1) which contains the reactor core and a number of reactor internals. In a BWR, the steam is generated inside the reactor vessel, and since the recirculation pumps are incorporated into the reactor vessel of the BWR 75 and the BWR 90, the steam supply system has become very compact.

The BWR 75 was designed for "fast refuelling"; there are no external pipe connections to the reactor vessel head and it can therefore be removed directly when the flange bolts have been loosened (by means of "multi-stud-tensioner" equipment - an equipment that can handle a number of flange bolts [and nuts] simultaneously). The hold-down force on the reactor internals is provided by a spring beam arrangement on the underside of the head. The internals are stacked onto eachother without bolt connections, and they can be lifted out directly when the vessel head has been removed.

The compression force from the spring beams is small when the reactor is cold, but when heated to operating conditions, the stainless steel internals expand more than the pressure vessel made of low alloy steel. Then the spring forces become significantly higher and a very stable aggregate has been accomplished.

These features make the core available for refuelling, rapidly and smoothly, with little radiation exposure to the personnel. It can be noted that the pool above the containment dome (cf. Fig. 2) is filled with water during normal plant operation, serving as a radiation shield for the reactor service room. It may also be noted that short refuelling outages are normal practice at the BWR 75 plants, e.g., at the Olkiluoto plants which are shut down for two weeks one year and three the next in a two-year cycle.

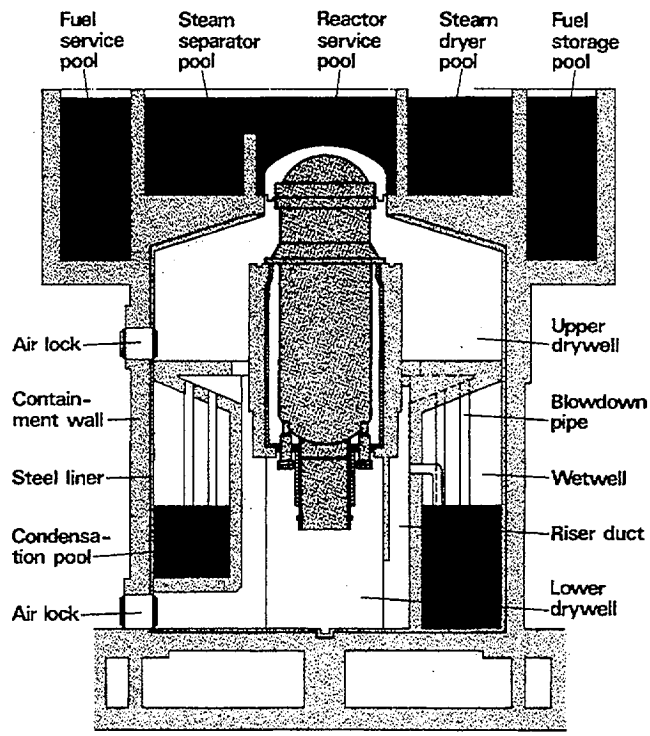


FIG. 2. BWR 75 - Reactor containment arrangement

The pump deck at the reactor vessel bottom and the cylindrical support of the moderator tank are welded to the vessel. All other internals, including feedwater spargers and control rod guide tubes, are easily removable. This makes the whole inside of the reactor vessel accessible for In-Service Inspection (ISI) of welds.

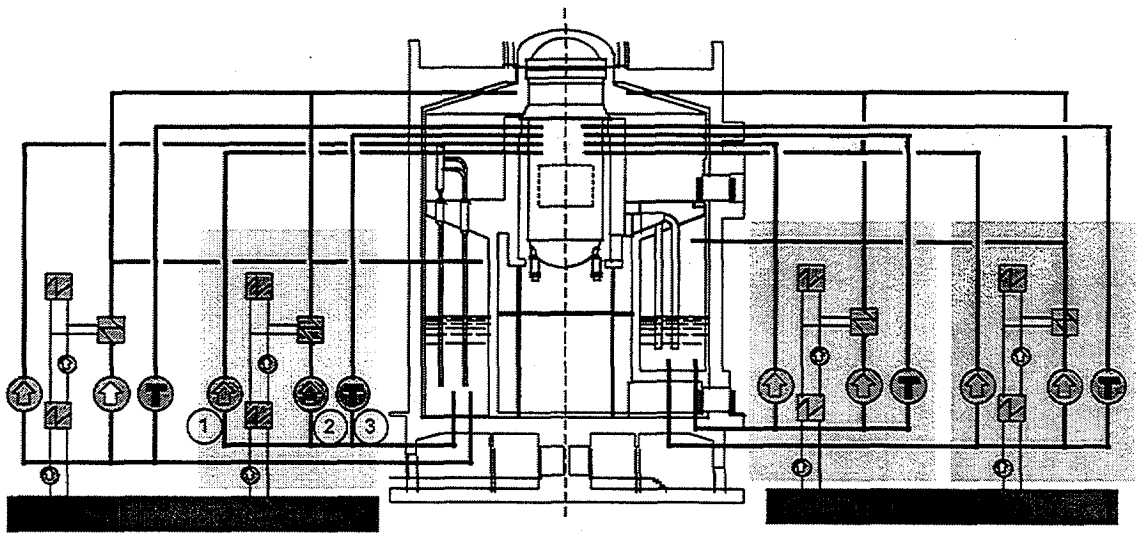
The reactor vessel bottom of the BWR 75 was modified compared with previous designs in order to reduce number of welds; in the BWR 90 the number of welds have been further reduced. This decreases the amount of ISI work that is required during a refuelling outage, i.e., it shortens the outage time with respect to inspections and reduces the associated radiation exposure.

The internal recirculation pumps have the impellers located inside the reactor vessel with the wet motors in housings on the outside, welded to the reactor vessel bottom. In order to enable dismantling the pumps have a split shaft design. The pump impeller shaft extends through the hollow motor shaft, to which it is fixed by a bolt connection at the bottom.

If a dismantling of the motor is needed, the thrust bearing of the motor unit is lowered slightly and the impeller will provide a first step seal against the reactor water. A secondary, inflatable seal is located above the motor; after activating this seal, the motor housing can be drained of water. Then the motor can be lowered by means of an hydraulic tool, and brought out to a service station outside the containment, for service. If the impeller has to be taken out for inspection, the motor housing is blinded and refilled with water. The secondary seal is depressurised, and the impeller can then be lifted upwards through the reactor downcomer by means of a tool operated from a service platform in the reactor service room.

These dismantlings can be performed without draining the reactor vessel, but it has to be depressurized. During plant operation, a purge flow of clean water is supplied to the pump shaft. The purge water flows up around the pump shaft to the reactor, preventing intrusion of reactor water and deposition of crud and other reactor impurities in the motor housing: This is an important feature for keeping the radiation exposure to the maintenance personnel low.

An important advantage of the internal pumps with wet motors is the elimination of the shaft seals; another the elimination of external recirculation loop piping. The piping calls for In-Service Inspection of welds which increases the work load close to radioactive sources and often implies extra critical path working time during maintenance periods. The radiation level at the service floor for the



1: Low Pressure Coolant Injection
2: Containment Vessel Spray System
3: Auxiliary Feedwater System

FIG. 3. Emergency core cooling systems

internal pumps has proven to be very low - about 1-2 mrem/h (10-20 μSv/h) - and the motor itself has negligible radiation level as a result of the closed motor water volume and the purge water flow. Replacement of a motor with a spare unit takes less than 24 hours and will not interfere with the critical path. The overhaul of the motor unit can be performed at a suitable time.

The internal pumps and their static "variable frequency-variable voltage" power supplies are advantageous with respect to operability; they permit rapid load following and power changes and with a suitable overcapacity in recirculation flow rate enable improving fuel cycle costs by "spectral shift" operation towards the end of the operating cycle. The built-in overcapacity and the arrangement of the core inlet plenum serve another purpose, making it possible to continue power operation - at up to 100% power, if one of the pumps should fail; a positive feature for ensuring operability even though pumps and power supplies have proven to be very reliable.

In an ABB Atom BWR, the fine motion nut and screw control rod drives are hanging under the reactor vessel bottom. The control rod drives are, in similarity to the arrangement at the recirculation pumps, supplied with a purge flow of clean water in order to minimise contamination. When a control rod drive is to be serviced, it is disconnected and lowered down to the bottom of the lower drywell under the reactor, brought out of the containment and to a special service station. The time needed and the total dose burden for this work are so low that remotely operated or automatic tools have not been considered justified to develop.

Wet motor pumps, without shaft seals, are used also for the reactor shutdown cooling system, reducing significantly inspection and maintenance needs; on the other hand, maintenance can be carried out rapidly and efficiently, using a special servicing equipment, when maintenance is needed.

4. SAFETY SYSTEMS ARRANGEMENT

In the BWR 75, the 2 x 100 % safety system configuration used earlier was replaced by a 4 x 50 % arrangement; i.e., the safety systems are generally divided into four separate subsystems, each with a 50 % capacity with respect to the design basis event (cf. FIG. 3). A strict physical separation of the four subsystems of each safety system was also included in the design. In this way, an enhanced redundancy and subsystem independence were ensured. The BWR 75 concept was re-assessed during the BWR 90 design review - and compared with alternative concepts. It was concluded that the 4 x 50 % represented an optimal solution from the view point of safety, availability, maintenance and cost; hence, it was maintained also in the BWR 90 design.

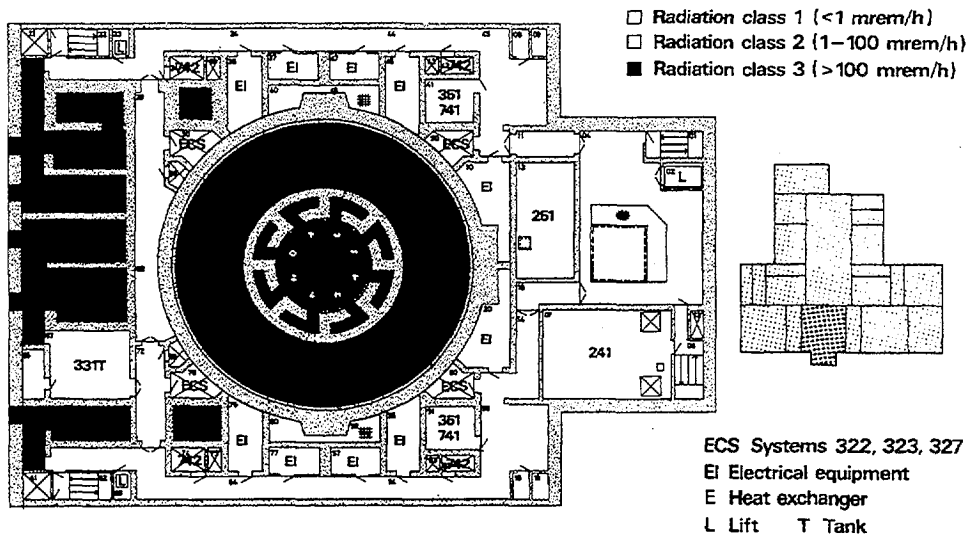


FIG. 4. BWR 75 - Reactor building installation and radiation classification, Level +13.3m

With respect to plant maintainability, the 4 x 50 % arrangement represents a significant improvement, since sufficient system capability/capacity will remain even if:

[1] one subsystem is taken out of service for repair or maintenance; and

[2] another subsystem fails upon request; the single failure criterion.

As a consequence, testing and preventive maintenance may be carried out during plant operation - on one subsystem at a time. This gives the plant management flexibility in planning the maintenance activities in the most efficient way; the work load during the annual refuelling and maintenance outage can be significantly reduced.

Another advantage relates to "permitted repair time". If a failure is detected in a 4 x 50 % safety system during normal plant operation, ample time is available for repair. As an example, the Technical Specifications for the Forsmark 3/ Oskarshamn 3 BWR 75 units permit a delay of up to one month for making the repair, without restrictions in plant operation. This means that the repair work can be carried out at a suitable time.

5. LAYOUT AND INSTALLATIONS

The requirements on physical separation of the subdivisions of safety systems have strongly affected the layout and installation of components in the plant buildings. The design goal of high maintainability and low radiation exposure has also had considerable influence.

In order to attain high maintainability the equipment has been installed in such a way that it is easily accessible for the maintenance personnel. Adequate communication routes have been provided throughout the plant - both for personnel and for transports of equipment. Space for performing hands-on operations, and for radiation shielding around components, is also important.

The accessibility to various portions of the plant is to a great extent determined by the radiation from different components, but also by the amount of airborne radioactivity. In order to reduce the direct effects of the latter the ventilation systems will supply the clean intake air to the corridors (more or less uncontrolled access areas), from which the air will flow into the rooms with radioactive components. Areas in which the dose rate level will be below 0.3 mrem/h (3 μSv/h) and where there will be no risk of radioactive contamination, are defined as uncontrolled areas, while all other areas are controlled access areas.

The communication routes throughout the plant are separated in accordance with this, all the way from the entrance building which is the only normal personnel access to the plant. The main communication area between the reactor building and the turbine building is divided into two separate transport passages on two different floor levels, one controlled and one uncontrolled. The communication routes along the turbine building and to adjacent buildings are branched off from these main communication routes.

With respect to facilitating maintenance a number of ground rules and guidelines are applied in the design work on plant layout and equipment installation (FIG. 4). The most important of these are:

[1] Non-radioactive systems and components are separated from pipes and components containing radioactive substances, except when absolutely necessary for the function of the radioactive systems

[2] In order to reduce maintenance doses, large radioactive components like filters, heat exchangers, pumps, tanks, etc. are either located in separate rooms or separated from each other by radiation shields.

[3] Each room containing radioactive system parts should have its own entrance from a corridor or communication area, where the radiation level is low; below 1 mrem/h (10 μSv/h), i.e., to a Class 1 area.

The corridors should also be arranged so that they can be used by the maintenance workers for preparing operations in the radioactive environment and for use during short breaks or waiting periods.

[4] Each radioactive component must be easily accessible and have a suitable working space for maintenance and In-Service Inspection. The component orientation must as much as possible facilitate maintenance.
Adequate space shall be provided for necessary handling equipment, and in some cases for temporary radiation shields.

From the point of view of radiology it is sometimes beneficial to remove the component and perform maintenance or repair in a better environment, e.g., in the active workshop. Therefore, it must be possible to remove and re-install the component rapidly.

[5] Valves in rooms with high radiation levels shall be remotely operated or have spindles to more accessible areas, in order to save doses to the operational and maintenance staff. For the same reason, other controls and checks, such as instrument readings, are as much as possible located in Class 1 areas.

[6] Radioactive pipes should have as short lengths as possible and be located at a distance from other components. This is important, because in many rooms the main portion of the radiation emanates from the pipes.

Accordingly, the radioactive systems in the reactor building are concentrated to the part that is closest to the turbine building. This arrangement results in short lengths of radioactive pipes since the main communication system which runs between these buildings, includes also a culvert for active pipes.

[1] Electrical components are to the extent practically possible located in separate rooms.

An important improvement with respect to accessibility for maintenance and service was introduced in the layout of the upper drywell of the BWR 75 containment; the major portion of the components (relief valves, isolation valves, etc.) are installed at the outer wall, in such a way that a transport space is available for all components.

6. MATERIALS SELECTION AND WATER CHEMISTRY

Proper materials selection is a key to the successful operation of a nuclear power plant. The best material is that which will be endurable, not crack, and not corrode significantly, i.e., that will suppress the need for maintenance and/or repair.

For purposes of maintainability it is essential to avoid elements which create radiation sources. Co 60 is the dominant gammaradiation source in primary system materials, and ABB Atom therefore early prescribed low cobalt contents in materials for reactor internals - less than 0.05 % (500 ppm) in stainless steels and less than 0.1 % (1,000 ppm) in Inconel.

The typical average annual occupational radiation exposure over the last ten years for the BWR 75 plants is 0.9 manSv (90 manrem), including some repairs and adjustments beyond normal maintenance and service, i.e., a rather low level compared with the experience from many other plants throughout the world confirming that the design measures incorporated in the BWR 75 design have been beneficial. There is a trend of increasing Co 60 contributions, however, and therefore further restrictions on cobalt contents have been found motivated.

There is also a strong ambition to further reduce the annual occupational radiation exposure, down to a target value of 0.5 manSv (50 manrem) for normal operation and maintenance. This makes the cobalt reduction efforts even more important. Cobalt-based alloys are always to be avoided. and a programme for Stellite replacement is ongoing. The 0.05 % (500 ppm) restriction on cobalt content is extended to include also components made in Inconel, the steam dryers, and the stainless steel cladding on the RPV inside. This value is also applied to smaller parts inside the RPV and to the preheaters/ coolers of the feedwater system. For ferritic steels in large-bore piping (D > DN 200) and casings of valves, apparatuses, and pumps the Co limitation has been set at an even lower value, 0.03 % (300 ppm). With respect to small parts and plant parts of austenitic steel and nickel alloys outside the RPV a higher cobalt content is allowed; the limit is here set at 0.2 % (2,000 ppm).

A good water chemistry characterised by low concentrations of impurities is also essential to keep radiation exposures low. In the ABB Atom BWR the reactor water is purified in mixed-bed ion exchangers with radial flow. The normal cleanup flow rate is small and varies with the need for cleaning as determined by conductivity measurement. During plant shutdown and startup, the cleanup flow rate is normally increased to a maximum value, corresponding to 4 % of the feedwater flow rate at full reactor power. The filter system operates at 40-60 °C.

The condensate flow from the condenser is purified in a pre-coat filter-demineralizer. This is preferable compared with the use of deep-bed ion exchangers since the main impurity in the condensate is particulate iron.

The conductivity is a good measure of water quality. In all ABB Atom BWR plants the conductivity of the reactor water is approximately 0.1 µS/cm (at 25 °C) and about 0.06 µS/cm in the feedwater. The iron content of the water is of great importance for the radiation buildup, since the corrosion products of interest form compounds with iron oxides. In ABB Atom BWR plants the feedwater has an iron content of less than 0.5 ppb, typical of "low-radiation BWR plants".

7. CONTROL EQUIPMENT AND POWER SUPPLY SYSTEMS

Maintenance and operability aspects have also been taken into account in the design of the instrumentation and control and auxiliary power supply systems. I&C and power supply are integrated parts of the safety-related systems and have therefore been divided into four independent and separated parts. Literal application of the requirements on physical separation between redundant groups also in the control room may involve complications for the plant's operating personnel, and the goals of a high safety level implies risks of spurious plant trips; hence, great care must be taken to minimise the risk of unnecessary trips without jeopardising nuclear safety.

The design of the control equipment is governed by a Swedish safety requirement, in use since the early 1960s, that operator interventions shall not be needed within 30 minutes in the event of an accident with respect to ensuring nuclear safety. In addition, there are supplementary general design goals saying that a failure or malfunction of one component, or faulty calibration of a measuring channel should not cause a plant trip, and that the degree of automation for major process systems - with respect to keeping the plant in operation - should allow the operator some 10 minutes action time.

In addition to the measures intended to keep the plant in operation, there are also features aiming at reduced work load during maintenance and refuelling periods. Some specific features of the control equipment and power supply systems may illustrate these design efforts.

In the early plants, inputs to the reactor protection system (RPS) were taken from local limit switches, e.g., for temperature and pressure inside the containment. In the BWR 75, data are generated by transmitters located on instrumentation rooms outside the containment which means that less manhours are needed for work inside the containment for limit switch checking and calibration. The RPS input is generated by an electronic trip unit when the DC signal from the transmitter exceeds a set value; the calibration of the trip function is easily checked during plant operation by adding a voltage signal from a test generator and recording the trip function value.

Each of the parameters used for the RPS is supervised by four redundant measuring channels, and the process computer is routinely monitoring the proper function by comparing the signals of the four channels; a defective channel is detected rapidly and can then be disconnected and repaired at a convenient time. The RPS is built up with a "two-out-of-four" coincidence logic, and disconnecting one channel results in a transfer to "two-out-of-three" which is a fully acceptable situation from both safety and plant availability point of view. The RPS logic is built with electronic modules, without relays, which means that testing can be performed during operation, reducing the amount of work needed during the refuelling and maintenance periods.

In the BWR 90, it was decided that the control equipment for process communication, process monitoring and control, as well as for man-machine communication should largely be based on programmable equipment, including digital controllers for the major control systems. One of the advantages offered by this new control equipment is an improved communication with the operator; human factors engineering can be incorporated in the design activities. Another advantage is the possibilities for introduction of new control functions without "disturbing" the normal operation of the plant, and automatic test procedures for safety systems, etc. The new equipment is advantageous also in the longer term; when the "computers" become "obsolete" after some ten years, they can without too much impact on the plant be replaced by new generations, since most of the software can be maintained for the new equipment.

The introduction of programmable equipment is quite natural for a new plant design, but it is of interest also for operating plants; significant modernisation programmes are under way at the nuclear power plants in both Finland and Sweden. It may be noted that these programmes do not involve an "abrupt" change of all equipment on one occasion during a long plant shutdown, but are based on step-wise implementation during normal outages in accordance with a pre-determined plan - to achieve a desired final structure. The utilities note that the increased computing capacities enable more efficient and flexible operation and saves money, e.g., by reducing start-up times after outages by some hours, and the impact of the investment on the life-cycle-cost is small and may even be positive.

The division into four subsystems (mainly of the safety-related portions) means that loss of one sub-division will have only limited effects on plant operation. Maintenance work can therefore to a great extent be performed at a convenient time during normal plant operation. Examples on such maintenance work are checking and tightening bolted joints in busbar systems, checking relay protections, and testing of batteries.

With respect to the testing of batteries, it may be noted that a battery arrangement with two "50 %" halves, each provided with its own rectifier, was introduced in the Forsmark 3/Oskarshamn 3 plants. In this way, the batteries could be tested thoroughly during plant operation, including deep discharge tests, without affecting the plant operation. The only distinguishable effect is that the battery capacity, of the system and subdivision being tested, temporarily is reduced to about 50 %, from "2 hours" to "1 hour". The Forsmark 3 and Oskarshamn 3 plants have DC distributions at 110 V, 48 V and 24 V, i.e., the number of batteries and distributions is large and the above arrangement was well motivated.

In the BWR 90, there is distribution of battery-backed AC to local converters, instead of using central DC systems. The converters of the battery-backed AC system busbar systems are provided with automatic switching devices for supply from the diesel-backed AC system instead which permits testing and maintenance to be carried out also during plant operation. This simplification and the reduced number of batteries, as well as DC distributions, yield a considerable reduction in maintenance work.

8. OTHER SYSTEM FEATURES AND DESIGN MEASURES

The BWR 75 design includes a certain redundancy also for non-safety-related systems, but primarily not for maintainability reasons. Typical examples in the turbine plant are the condensate and feedwater pumps and the circulating water pumps, with 3x50 % or 4x33 % pumps operating together on a common piping system, and providing a functional redundancy with respect to the power operation impact of a malfunction of an active component. Similar arrangements are utilised for service systems of the reactor plant, e.g., the primary and secondary cooling water systems, but there are also cases where 2x100 % have been found most beneficial, e.g., for the shutdown cooling system of the reactor.

Anyhow, the main purpose of the functional redundancy in these systems is not to facilitate maintenance but to improve the functional reliability by making the power plant process less sensitive to component failures. The installed redundancy or over-capacity will involve an increase in the initial plant cost, but taking into account the potential gains in operational reliability, the effect on the total life-cycle cost will most likely be positive.

9. EUR EVALUATIONS OF THE BWR 90

Following the initiative of some of the utilities in the European Utility Requirements group, the BWR 90 has been selected to be one of the designs for which a detailed assessment against the requirements of Volumes 1 and 2 of the EUR document will be made. This activity is part of an effort to develop a Volume 3 for the EUR document with specific requirements for specific designs. The work was started up in the Spring of 1997, and is scheduled to be finished in 1998.

10. CONCLUSIONS

The operation experience of the BWR 75 plants has been very good. The average energy availability factor of the Swedish plants last year (refuelling outages included) was 90.1 %, including considerable load following and coast-down operation, yielding a recorded capacity factor of 85.8 %. Even more impressing are the capacity figures attained by the two units at Olkiluoto in Finland, - e.g., 92.5 % for Olkiluoto 1 and 95.1 % for Olkiluoto 2.

The high availability and capacity factors that have been attained, prove that the operability, reliability and flexibility of these plants are in the "top category" of operating plants; the Olkiluoto plants are ranked at the absolute top among the best performers of the world. At the same time, the recorded low occupational radiation exposures and the short annual refuelling outages show that the design measures that have been outlined above, have been beneficial for the plants "operability"; they have become easier to manage in an efficient way.

The BWR 90 design draws on the experience that has been gained from design, construction, commissioning and operation of BWR 75 plants. Based on this experience basis, design modifications and adjustments (or supplements) have been implemented in areas where design reviews indicated that significant improvements were within reach. In other areas, it was decided that a maintained proven design was the most appropriate and prudent approach.

The BWR 90 plant design incorporates a number of improvements with respect to operability and maintainability compared to the operating BWR 75 plants, and it has the capacity to equal and even surpass the excellent performance of the BWR 75 plants.

REFERENCE

[1] BWR 90 description in "Status of advanced light water reactor designs, 1996", IAEA-TECDOC-968, September 1997

Background material:

Lars Leine, "Design for maintainability", Proceedings of IAEA International Symposium on Nuclear Power Plant Outage Experience (IAEA-SM-274), Karlsruhe, Germany, 18-22 June 1984.

NEXT PAGE(S) left BLANK

LEARNING FROM EXPERIENCE: FEEDBACK TO CANDU DESIGN

P.J. ALLEN, J.M. HOPWOOD, G.P. ROUSSEAU
Atomic Energy of Canada Limited,
Mississauga, Ontario, Canada



Abstract

AECL's main product line is based on two single unit CANDU nuclear power plant designs; CANDU 6 and CANDU 9, each of which is based on successfully operating CANDU plants.

AECL's CANDU development program is based upon evolutionary improvement. The evolutionary design approach ensures the maximum degree of operational provenness. It also allows successful features of today's plants to be retained while incorporating improvements as they develop to the appropriate level of design maturity.

A key component of this evolutionary development is a formal process of gathering and responding to feedback from:

- **NPP operation, construction and commissioning;**
- **regulatory input;**
- **equipment supplier input;**
- **R and D results;**
- **market input.**

The processes for gathering and implementing the experience feedback and a number of recent examples of design improvements from this feedback process are described in the paper.

1. Introduction

AECL is the designer of the CANDU® reactor system. There are 25 commercial-size CANDU reactors in operation in 4 countries. In Canada, 19 units are in operation in Ontario, and one CANDU 6 unit each in Quebec and New Brunswick. There are also CANDU 6 units operating in Argentina (1), Korea (2) and Romania (1). A further five CANDU 6 units are under construction, one in Romania, two in Korea and two in China.

The largest group of CANDU reactors came into operation in the late 1970s and early 1980's. Overall, more than 300 reactor-years of operation have now been accumulated. Commercial CANDU plants range from 1971 to 1997 in date of commercial operation. This large and growing operational experience base provides an important source of information to use as feedback to improve the design of the CANDU products of today and tomorrow.

2. CANDU Product Line

AECL has two proven products, the CANDU 6 and CANDU 9 Nuclear Power Plants (NPP's), summarized below.

The CANDU 6 Product

The 700 MWe rated CANDU 6 nuclear power plant has recorded outstanding operating performance since the startup of the first four CANDU 6 units in 1983. The CANDU 6 units have a

capacity factor of about 85% over the last ten years, and have frequently achieved world number 1 ranking on an annual basis. They also have excellent records in such figures of merit as scram frequency, fuel operational integrity, radioactive waste management and emission levels.

More recently, Cernavoda-1, in Romania and Wolsong 2 in Korea have come on line and a further two units at Wolsong will come on stream in 1998 and 1999. Construction has started this year on two additional CANDU 6 units at Qinshan, in China.

The CANDU 6 is a mature power plant design, with a history dating back to the 1970's. The outstanding track record of the CANDU 6 design means that it represents an attractive basic design today. Part of the success of CANDU 6 is due to its past evolution from earlier CANDU designs.

The CANDU 6 units adopted many of the features pioneered and developed at earlier Canadian CANDU stations, notably Pickering A and Bruce A. CANDU 6 utilizes the basic reactor in use at Pickering, the 37-element fuel in use at Bruce, the Bruce reactor control system (with some improvements), and two steam generators and heat transport pumps for each figure-of-eight reactor loop.

The CANDU 6 design represents a mature application of current technology, with experience from development on previous designs, a solid track record of operating experience supplemented by a process of evolutionary low risk development.

The CANDU 9 Product

CANDU 9 is the next step in the evolution of the CANDU product line with key components already proven in operating CANDU plants. Specifically, the CANDU 9 nuclear steam supply system is based on the proven Bruce B and Darlington design, single unit features from CANDU 6 and incorporates developed and proof-tested advanced technologies. Given the modular nature of CANDU, the CANDU 9 design includes the benefits noted above for CANDU 6.

CANDU 9 systems and equipment incorporate specific design features and technologies to meet current customer's expectations. The requirements for a warm sea water site with higher seismic condition, similar to those specified for sites in Korea for example, are met, as are requirements for a plant design life of 60 years. Utility requirements were built-in as part of the conceptual design process, by including utility staff in the CANDU 9 design team.

AECL's current design program has completed all documentation required to demonstrate design integration A licensability statement was obtained from the Canadian Regulatory (AECB) at the beginning of 1997.

Product Summary

The operating CANDU 6 plants have achieved success in operations in a wide variety of situations, in four different countries and with both large and small utilities. In most cases, the utilities have used CANDU as their first step in nuclear electricity.

3. AECL Application of Feedback

Since the initial years of operation of the first CANDU plants, AECL has recognized the role of feedback and hence participated in programs to respond to nuclear operating experience, both in R and D and in engineering activities.

CANDU Owners Group

COG is an alliance formed in 1984 between the Canadian CANDU utilities and AECL. It was established to create a forum for the planning and funding of generic programs and to provide a framework for cooperation among CANDU plant owners and designers for the successful support, operation and development of the CANDU technology. To meet its mandate, COG established cooperative programs in the areas of:

- **Information Exchange**
- **Joint Projects**
- **Research and Development**

The exchange of operating experience information remains fundamental to COG's mission. Through the operating experience exchange (OPEX) program, lessons learned from operations are fed back into design, good practices are exchanged, events are reported against specific criteria, data relevant to safe plant operation is collected, screened, reviewed and distributed to COG members.

The program provides a direct link between all CANDU station staff worldwide as well as direct and immediate access to CANDU designers via an electronic messaging system. The messaging system has interfaces with INPO and WANO information exchange programs, with relevant information from these areas reviewed and posted, as appropriate, by COG Operations staff.

In addition to managing the information exchange function, other ongoing activities include preparation of bulletins, newsletters and good practices documents on topical issues of common interest to CANDU designers and plant operations.

Since COG's inception in 1985, numerous workshops, conferences and symposia have been held. These events foster improved communication, cooperation and sharing of station and operational experience.

The overall thrust of the COG program is:

- **To improve performance and extend operating life of CANDU plants by providing increased knowledge about performance of key plant components and by supporting interpretation and modeling of operating data.**
- **To protect the investment in basic CANDU technology by a vigorous program of research geared to ensure a competent response capability.**
- **To support the safety and licensing basis for current and future CANDU units.**
- **To improve the design of current and future CANDU units.**
- **To ensure high standards of protection for plant workers, the public and the environment to support CANDU plants as "good neighbours" with public and environmental acceptance.**
- **To develop and gain acceptance for decommissioning and nuclear waste disposal concepts with primary emphasis on safe disposal of high level waste.**

To meet these strategic objectives, the COG R&D program is divided into five program areas:

- **Safety and Licensing**
- **Fuel Channels**
- **CANDU Technology**
- **Waste Management**
- **Radiological Health and Safety**

Feedback to Design

In addition to supporting operating plants, AECL has placed increasing emphasis on the incorporation of operating feedback, and other CANDU feedback, into the current CANDU designs. In this sense product "provenness" is something which is continuously re-established, by ensuring lessons learned from experience are systematically applied to design.

Feedback from CANDU and other nuclear plant programs is part of AECL's systematic process of feedback review. AECL's feedback process incorporates regular, formal review of lessons learned from the following areas:

- **NPP operations worldwide;**
- **Plant design, construction and commissioning programs;**
- **Regulatory input (both Canadian and international);**
- **Results of R and D programs;**
- **Suppliers' input.**

Regular input from other stakeholders, in particular utilities (both currently operating CANDU's, and utilities considering future NPP's) is sought to maintain a design which reflects customer requirements.

This formal feedback process has been established with a broad mandate, covering all aspects affecting Nuclear Power Plant design. Both Nuclear Steam Supply and Balance of Plant issues are covered. Operations and maintenance implications are addressed, as well as impacts on the functional performance of the design. This design feedback process is linked to similar CANDU utility operations experience (OPEX) review processes. Design feedback is also an input to, and is closely linked to, initiatives to support CANDU Plant Life Management and Plant Life Extension.

The formal process to review feedback, and incorporate lessons learned into design, is as follows:

- **Feedback teams identify, review and perform first cut evaluations.**
- **Design Feedback Manager and staff ensure that all feedback is entered in the CANDU Feedback Monitoring System for follow-up. All affected projects are informed and decide on the disposition of each feedback item, i.e. to be implemented or rejected (with reasons documented.)**
- **Once agreement is reached that the feedback item will be addressed, each project reviews the feedback in detail and develops strategies for implementation. The CANDU Feedback Monitoring System is available to all design staff, as an online resource.**

The responsibility for reviewing feedback recommendations in the context of future CANDU 6 and CANDU 9 projects, lies with the respective Product Managers. An important part of this review is to ensure a very accurate and comprehensive definition of the current product configuration. One general lesson learned from many NPP operational experiences is that control of plant configuration is a vital pre-requisite to good operating reliability and successful maintenance. In a corresponding way, good configuration management is vital to effective application of feedback into current designs. This is made easier by the rapid development of plant wide Information Technology tools. For example, both CANDU 6 and CANDU 9 plant designs are established on a comprehensive 3D CADDS database, linked in turn to material management and technical specification databases. Similarly, a comprehensive database including operations feedback information has been created as an on-line tool for system and component designers, to enable cross-fertilization of lessons learned among different parts of the NPP design.

Feedback Monitoring System

The Feedback Monitoring System (FMS) is designed to capture feedback, securely hold and manage the data in a database, and ensure the information is readily available on-line to designers for their use. A user-friendly interface, ad-hoc search tool, and report capabilities are incorporated, making this tool inherently easy to use with very little system training required.

The two main components of FMS are an Oracle database with a FormFlow (from JetForm) front end. Oracle was chosen for its security facilities, extensive size capabilities, as well as being one of AECL's standard tools. FormFlow offers a toolset for creating forms, managing the associated workflow, and controlled capture of data into a myriad of databases, including Oracle. The information is viewed through FormFlow, the Oracle structure being invisible to users.

General users have read-only access to the database information. All AECL designers are given the capability to provide feedback by filling in an Issue Form on-line, sending it to their respective management for approval, and subsequently to the appropriate feedback team. Similar processes apply to completion of the Evaluation Form, when a project provides information on their approach to the issue already identified. Information is not visible to the general users until the feedback team reviews the form for completeness and commits it to the database, at which time a unique identifier is automatically assigned. Feedback team members are the only users with electronic permissions to save or alter information in the database. This secures integrity of the committed data.

Extensive FormFlow capabilities have been embedded in the design of the smart forms to make data entry easy, and ensure consistency of information. These tools include numerous field drop-down lists, on-line help clearly identifying the specific type of data for every field, spell checking, compulsory filling in of essential fields and customized menu bars and buttons. The routing is integrated directly with MS Exchange which is AECL's standard electronic mail system.

Roll-out of FMS to designers' desktops started 97 March 31, and has been embraced by the AECL design community. Additional system enhancements are scheduled for this year, including a browser front end to provide greater search capability, more flexible reporting, automatic selection of system/equipment name and identifier, provision of predefined acronyms, and direct links to supporting feedback documentation. Access to information pre-existing in databases outside of AECL is also currently being addressed.

Examples of Feedback to Design

Recent examples which have proceeded through the feedback process to design improvements include:

- **Steam Generator improvements such as provision of additional access ports for chemical cleaning and improved divider plates for long life performance**
- **ECC simplifications and performance improvements including better strainer design for long term circulation of cooling water**
- **Control room improvements to display annunciation organization and overall human factors as per feedback from operations staff.**
- **Reduced plant emissions and operator dose by optimization of reactor building airflow and improvements to liquid collection provisions.**
- **Improved safety system signal monitoring with updated digital displays, increased computerized testing for reduced operation burden and increased system reliability.**

- **Improvements to Liquid relief valve component and system design for heat transport pressure and inventory control, based on operational experience.**
- **Improved support systems to facilitate effective management of plant operations.**
- **Optimization of design margins to reduce plant cost and improve operating margins.**
- **Updated equipment technical specifications, based on manufacturers and ongoing project feedback, to reflect up-to-date component concepts, materials, manufacturing processes and standards, including adoption of international standards (such as ISO).**
- **Improvements in construction sequencing and detailed equipment layout to assist project schedule reduction.**

The feedback process also generates a stream of minor change recommendations each of which will improve either manufacturing, installation, operations or maintenance, for the standard CANDU designs.

4. Conclusions

As CANDU and other nuclear plant programs have gained experience, these data have had an important impact on design. AECL has increased its emphasis on collecting, evaluating and responding to feedback in a systematic way. AECL's current designs, CANDU 6 and CANDU 9, include a number of design improvements based on lessons learned from experience feedback. By maintaining this feedback process, AECL will be able to ensure improved performance of current and future CANDU plants.

THE CIDEM PROJECT FOR INTEGRATING AVAILABILITY, OPERATING EXPERIENCE AND MAINTENANCE IN THE DESIGN OF FUTURE NUCLEAR POWER PLANTS

XA9848587

C. DEGRAVE, M. MARTIN-ONRAET
Electricité de France,
Villeurbanne, France

Abstract

To minimize the kWh cost of future nuclear plants EDF has decided to implement the CIDEM project (French acronym for Design Integrating Availability, Operating Experience and Maintenance), an analytic and systematic process for studying new projects.

The first CIDEM application is centered on the future French nuclear unit construction program, known as the REP 2000 Program but the approach could be applied to other Reactor type.

The CIDEM studies at the beginning, were oriented to the issues strongly impacting the availability. They have concerned: planned outages forced outages and preventive maintenance.
The studies were carried out by a team grouping engineers from the 3 EDF's Divisions (Engineering-Generation-Research), ,and working together in a Concurrent Engineering- Mode. This team works in close collaboration with the vendors and the German Utilities involved in the REP 2000 EPR program.

The implementation of the CIDEM process constitutes for EDF a new approach to the study of the new Nuclear Power Plant projects. The studies conducted in the availability field have already high lighted a number of critical points and have made it possible to establish a series of specifications for the REP 2000/EPR project. The integration in the design process of Preventive Maintenance and Logistic Support studies will allow a better control of the maintenance cost. The competitiveness of nuclear energy greatly depends on the success of such an approach.

1. BACKGROUND OF THE CIDEM PROJECT

Energy self-sufficiency is a major strategic need for France. The competitiveness of nuclear energy relative to fossil fuel power is an essential goal for EDF. For future nuclear plants to remain competitive, it is necessary to limit and even to reduce investment and operating cost, while keeping safety at the right level required.

Considering its plant operating experience, the analysis of foreign practice and the development of new design approaches and tools, Electricité de France (EDF) is convinced that it is possible to improve new plant design, operation and maintenance without increasing investment costs too much.

To minimize the kWh cost EDF has decided to implement the CIDEM project (French acronym for Design Integrating Availability, Operating Experience and Maintenance), an analytic and systematic process for studying new projects, aiming at a design optimization including investment, maintenance, availability and radiation exposure objectives [1].
This approach aims at a single goal : to minimize the kWh production cost incorporating investment operation and fuel cost, based on experience from French and foreign units.

This process, already widely practiced in other industries or services (aerospace, defense, ...), uses concepts known by the acronyms RAM (Reliability, Availability, Maintainability) RCM (Reliability Centered Maintenance) and ILS (Integrated Logistic Support).

The first CIDEM application is centered on the future French nuclear unit construction program, known as the REP 2000 Program, particularly in the framework of the design studies of the new French-German Nuclear Island (European Pressurized Reactor, EPR) but the approach could be applied to other Reactor type or fossil-fired units in particular for its methodological aspect.

2. THE MAIN GOAL AT THE BEGINNING OF PROJECT

Based directly on EPRI/Utilities Requirements Document and on European Utilities Requirements, a number of goals intended to maintain the overall costs of the future generating units at a competitive level relative to the other generating modes were set for the REP 2000/EPR project. These goals are :

-availability of at least 87%
-annual radiation exposure less than 0.5 Men.Sv/unit/year for the EPR nuclear island
-maintenance costs equal or less than those of current units.

To ensure that these objectives can be achieved, it was necessary to define and implement, very early in the program, a design study process based upon :

-analyses of the operating experience from the EDF park, from foreign power plants, in particular the German Konvoi series, and other nuclear industrial facilities,
-the techniques borrowed from maintenance engineering and from the field of dependability studies (mainly reliability, availability and maintainability analyses on structures, systems and components).
-an organization of the Concurrent Engineering type, bringing together specialists from the different branches involved in the program.

3. A CONCURRENT ENGINEERING ORGANIZATION

The CIDEM studies are managed by a team grouping engineers from the 3 EDF's Divisions involved (Engineering-Generation-Research), in charge of activities coordination, implementation of some specific tasks (allocations definition, validation of results, writing up summary documents or specifications). This team works in close collaboration with the vendors and the German and other European Utilities involved in the REP 2000 program.

4. FIELD AND STUDIES AREAS COVERED BY THE PROJECT

The main contributors to kWh can be represented as in Figure 1.

Considering this representation and the main goals assigned to the project, the various fields of CIDEM studies are oriented towards :

- Operating Experience analysis
- Availability analysis (forced and planned outages)
- Logistic Support
- Radiation Exposure
- O&M costs analysis
- Preventive Maintenance
- R&D needs.

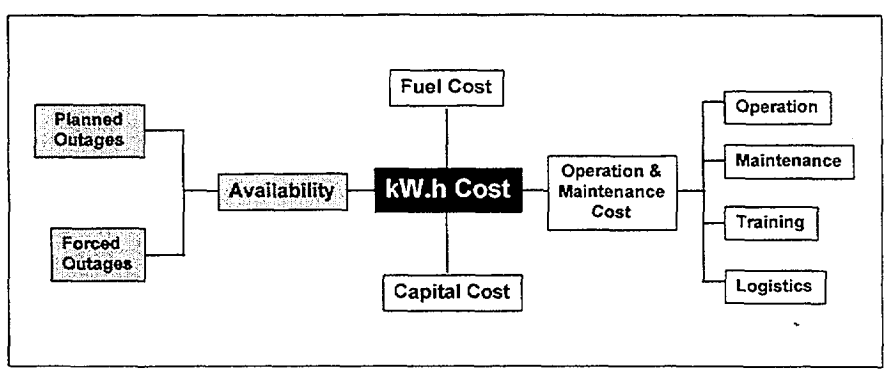


Figure 1 Contribution to the Generated Power

5. RESEARCH AND DEVELOPMENT PROGRAM

The CIDEM approach calls for the development of methods (and related tools) in the dependability, logistic support, radiation exposure and operation experience fields.

For this purpose, a 3-year research and development program has been implemented. The main actions planned are :

- analysis of the approaches used in similar study processes,
- definition of methodologies and associated tools in the following areas:
  - -functional analysis and FMECA (Failure Mode, Effects and Criticality Analysis),
  - -reliability centered component behavior models,
  - -predictive radiation exposure,
  - -operating experience data processing software,
  - -cost models,
- definition of a Technical Information System for design and maintenance assistance,
- validation of these methods and tools by a feasibility study on a system chosen from a power plant in operation.

6. OVERVIEW OF THE STUDIES

The CIDEM studies for the REP 2000 Program were started at the beginning of 1993. A number of results have already been obtained in the various fields covered by CIDEM. The most significant results have been obtained in the availability field [1] , [3].

6.1. Availability studies

For Utilities, the availability improvement of Nuclear Power Plants in project or in operation is a key goal to ensure their competitiveness.

6.1.1. Main causes of unavailability

The main causes of unavailability for a Nuclear Power Plant are (Figure 2):

- forced outages during operation,
- planned outages for refueling and maintenance,
- outage extensions for works or unplanned events.

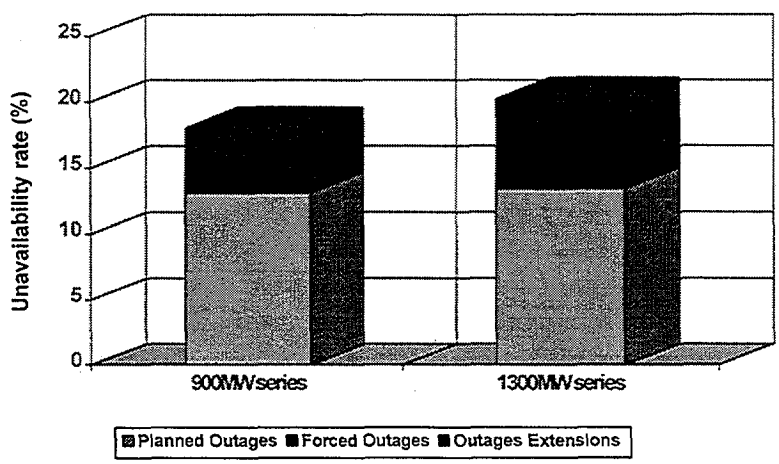


Figure 2 Main cases of unavailability

This last case is not yet studied in the frame of the CIDEM Project.

6.1.2. The different steps of an availability study

Goal fixing

The first action consists in fixing a global availability allocation (plant in design phase) or an availability improvement objective (plant in operation) to reach. This allocation depends on the general technical-economical objective fixed at the outset and refers to the Utilities' requirements (EPR/URD, EUR...).

Operating Experience global analysis

Any availability study starts with an operating experience feedback global analysis of performances of current plants :

- of the plant itself, when the study concerns an operating plant,
- of close design plants, when the study concerns a new designed plant,

This analysis aims at emphasizing the main causes of unavailability and to guide the studies.

Example of diagram obtained by operating experience global analysis

Special studies:
Depending on the critical point shown by the operating experience feedback analysis, special studies are then realized :

- either in the field of forced outages
- or in the field of planned outages analysis.

To start these analyses, partial allocations to the main contributors are defined at this step.

These detailed analyses allow drawing up a list of design arrangements (for next plants) or modifications (operating plants).

6.13. Availability assessment

The CIDEM Project group has developed a calculation method for assessing, in a simple and user-friendly manner, the availability of a nuclear power plant.

This method allows taking into account the main causes of unavailability : forced, planned, extensions.

It allows calculating three kinds of unavailability :

- **the theoretical availability** which represents the maximum technically achievable, and does not consider any outage extension,
- **the target availability**, which, in addition to the theoretical availability, takes into account outage extension for special works,
- **the realistic availability**, which, in addition to the target duration, considers unplanned events encountered during the outage. *This availability is used for cost assessments.*

Method

The method consists in assessing an average availability on a 10 years operating period in order to take into account all kinds of unavailability : forced outages, planned outages including 10-year regulatory inspection and outage extensions.

The yearly availability of a plant can be expressed as below :

$$D = 100 - \left(\frac{1}{10}(I1 + I2 + K.I3 + I5 + I7) + I4 + I6 \right) \frac{100}{8760}$$

with :

I1 : reference duration of refueling outage including the 10-year inspection activities in hours (from breaker to breaker)

I2 : reference duration of refueling outage including the turbine-generator overhaul in hours (from breaker to breaker)

I3 : reference duration of a normal refueling outage in hours (from breaker to breaker)

K : number of normal refueling outages in a 10 years operating period depending on the fuel cycle length.

I4 : yearly forced outage in hours

I5 : total unavailability, in hours, for special works

These special works include modifications (on systems or components) or major components replacement (for example Steam Generators).

I6 : yearly unavailability, in hours, for starting and tests

I7 : total unavailability, in hours, for outage extension

These outage extensions include organization problems as unavailability of resources or tools, or miscellaneous events.

6.2. Forced outage studies

The purpose of forced outages studies is to identify the critical systems or components responsible for shutdowns of the plant, to propose design modifications and to assess their impact on the global availability.

The general methodology implemented is very close to the RAM (Reliability, Availability, Maintainability) approach applied in various industries, Armament, Aeronautics, Chemicals, but rarely used until now in nuclear power field.

6.2.1. Methodology

The methodology implemented is in 4 steps :

- operating experience feedback analysis, critical systems or components identification and ranking,
- design modifications proposal and quantitative assessment of their impact on the availability
- drawing up of related requirements for design modification

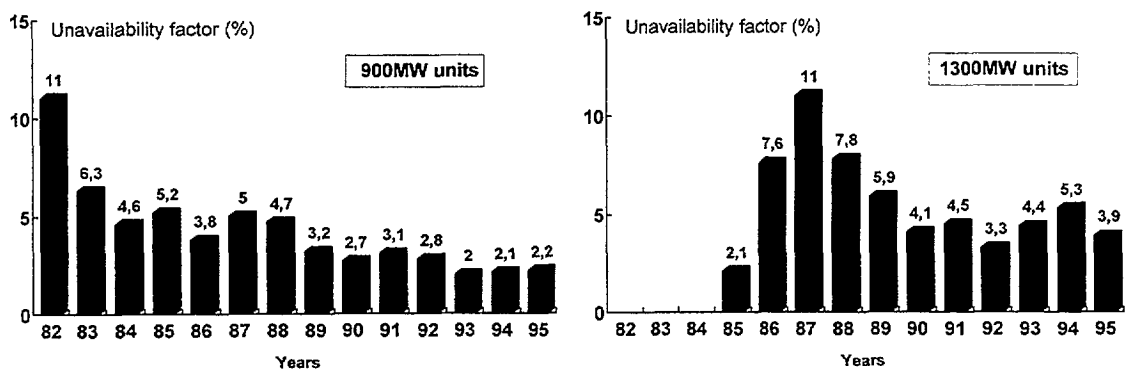


Figure 3 Unavailability Factor of EDF's Current 900 MW and 1300 MW Units

Operating Experience analysis

This analysis uses the statistical data bases of the operator or the designer. Figure 3 presents a diagram resulting from the analysis of data bases concerning EDF's current 900 MW and 1300 MW series.

The values obtained by operating experience analysis will serve as a basis for the definition of the forced unavailability partial allocations of the main systems, to reach the overall allocation of 2% per unit and per year as early as the first years of service. This is an aggressive goal for the French units, but one which is currently reached by some foreign units. The detailed analysis of the data bases enabled the main systems and components responsible for the unavailabilities to be ranked.

The main contributors are the main generator, valves, steam generators, the main steam turbine and I&C. In fact, the analysis shows that 9 systems or components are responsible for nearly 2/3 of the forced unavailability of the 1300 MW units. This analysis clearly allows the critical contributors identification and ranking (Figure 4).

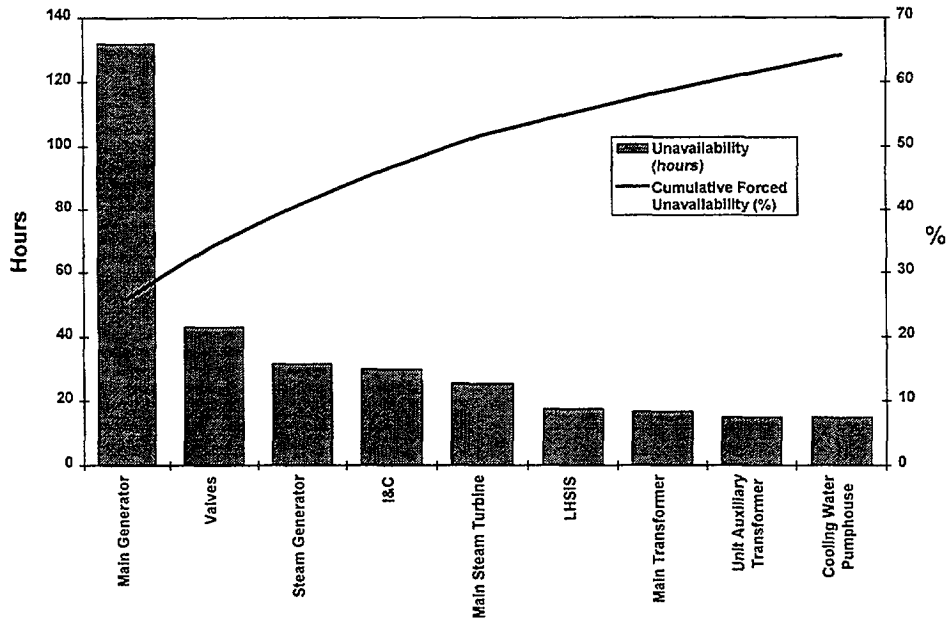


Figure 4 Unavailability Factor of the main contributors

The next step is to specify the characteristics of these critical items in term of reliability and maintainability. A software was developed to extract from Operating Experience data bases reliability parameters as Failure Rate (λ), Mean Time To Repair (MTTR, μ).
These parameters are used first to give a qualitative estimation of their impact on the forced unavailability. Figure 5 gives an example of such a detailed analysis of the EDF's 1300MW series main generator.

Design *modification proposal*

The previous analysis allows proposing design modifications of critical systems or components. As an example, these modifications can be :

-addition of redundancies in some parts of systems,

-reliability improvement or change of type of components,

-decrease the MTTR by arrangements to facilitate the maintenance of the most critical components.

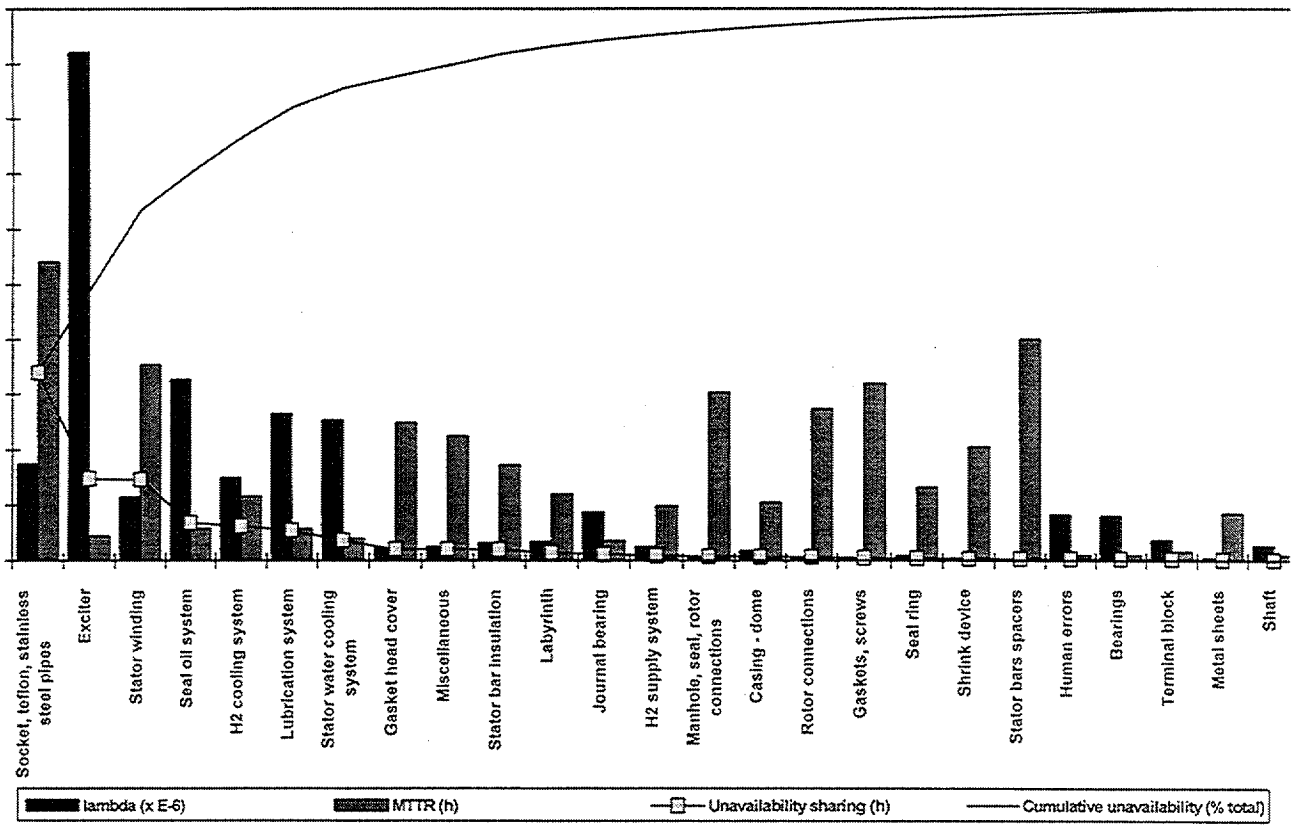


Figure 5 *Unavailability Factors of the Main Generator (components) of an EPR 1300 MW*

Quantitative assessment

The impact of these modifications is assessed with reliability tools, based on the Fault Trees method. The reliability data are taken either in Utility's or International data bases when components are similar to those of current plants or if not, elaborated with new techniques as the Bayesian approach (based on experts judgment modeling).

EDF has several detailed reliability data bases used for their own Probabilistic Risk Assessment (PRA) or Reliability Centered Maintenance (RCM) studies.

6.2.2. First studies implemented

A series of studies on an existing system benefiting from a significant operating experience was undertaken. The 1300 MW units "Feedwater" system was selected. These studies confirm the operating experience : the critical components in this system are the feedwater flow control valves.

A sensitivity study was also conducted to assess the influence of different system designs on the availability of the feedwater system. The results were used for the definition of the new design of the future Nuclear Plant Feedwater system.

6.3. Reliability Availability Maintainability specifications

All the availability and reliability studies previously conducted will result in a number of specifications which will have to be incorporated into the main components purchasing contracts. These specifications are the logical issue of systems availability analysis.

This approach constitute a new kind of relationship between the Utilities and the vendors.

Goals

The main goals of these specifications are :

-to define the components availability allocations to reach and the related test means

-to specify the vendors' liability regarding these allocations

-to quantify the maintenance activities in order to control the kW.h cost

-to implement a close collaboration between all those taking part in the project, designers, vendors, operators, as early as possible (concurrent engineering).

Methodologies implemented

The RAM specifications drawing up use some well-tried methodologies in high tech industries as :

-Functional Analysis to make a complete description of the various functions of the material,

-Failure Mode Effect Analysis (FMEA) to assess the influence of the failure of the main components on the availability of the different functions.

Structure of specifications

General specifications (applied to any kind of components) : they aim at specifying the main Utility's requirements as component availability and reliability assessment, maintainability studies and definition of logistic support elements.

Special specifications : they specify for the main components the mode of application of the general specifications, and quantify partial allocations.

First application

EDF has run an investigation in this area and has conducted a first study on the main turbine and generator.

A first set of General Requirements of the Reliability, Availability, Maintainability has been drafted. A second study is under way to draw up RAM requirements sufficiently general to be applicable to most components.

6.4. Refueling and maintenance outage studies

The EDF Nuclear Operation Division organizes the planned maintenance operations around 3 types of outage :

-normal refueling outage

-refueling outage including general turbine inspection (every 5-6 years)

-refueling outage including the 10-year inspection activities.

For outage studies on current or new designed plants, EDF has defined 3 kinds of outage duration :

-the reference duration, maximum technically achievable by the design of the plant,

-the target duration, which, in addition to the reference duration, takes into account some additional works (as the replacement of heavy components or modifications)

-the realistic duration, which, in addition to the target duration, considers unplanned events encountered during the outage (organization problem, failure of components or tools etc...).

Figure 6 shows the relative importance of these 3 kinds of duration for EDF's current plants of the 900 and 1300 MW plants.

In the framework of the CIDEM Project oriented towards future plants, the studies will be only centered on the reference duration which is directly linked to the design of the plant.

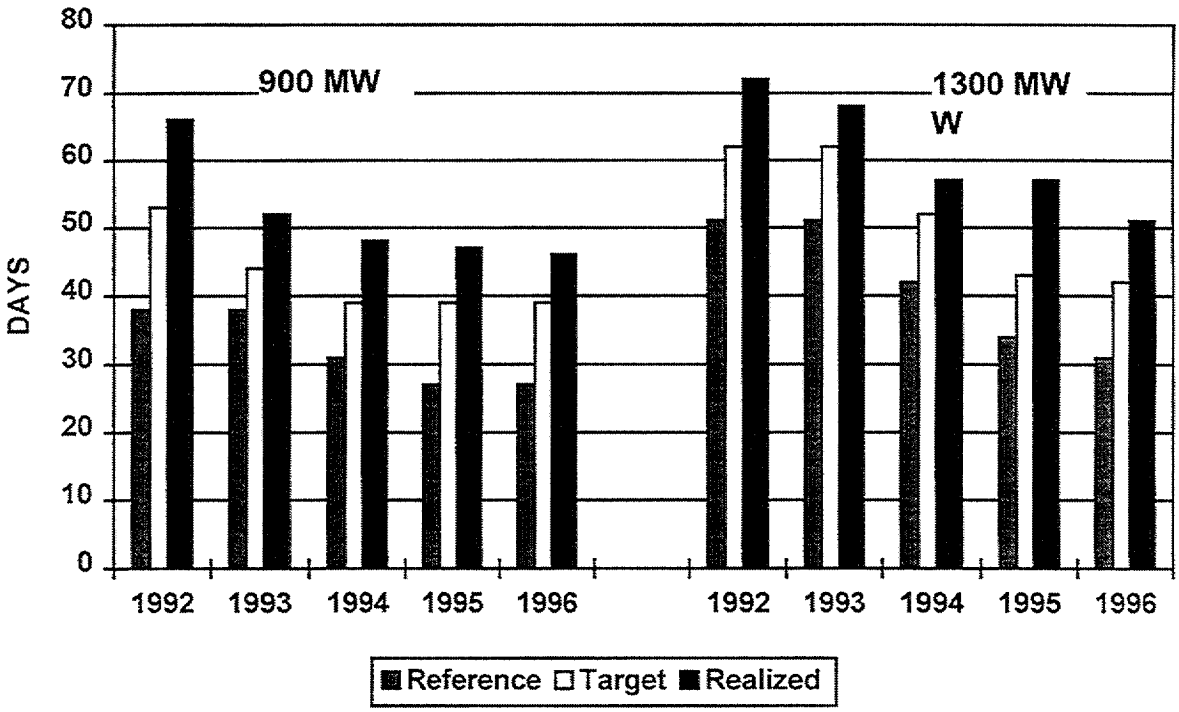


Figure 6 *Outage Duration Studies of EDF's Current 900 MW and 1300 MW Units*

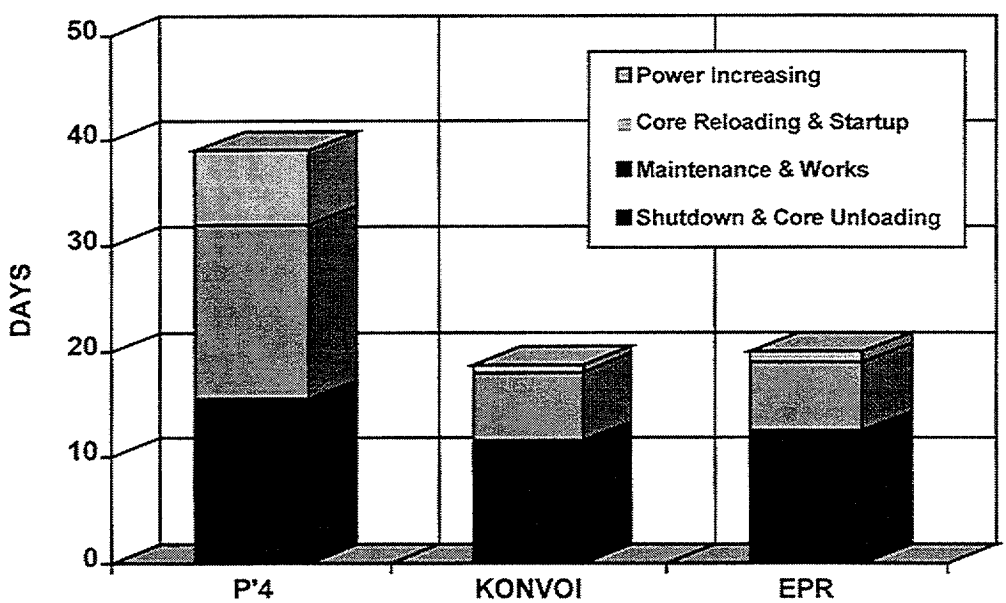


Figure 7 *Main Phases of a Refueling Outage for the French 1300 MW Units, German CONVOY Units and EPR Project*

6.4.1. Methodology for a refueling outage study

The general methodology for refueling outages study, either for a plant under design or for an operating plant, is to build up a schedule including the different phases of the physical process (i.e. cooling, purification), the handling works (i.e. vessel opening, core unloading) and the maintenance activities (i.e. inspection and control of safety trains ...).

The aim of this schedule is to provide the shortest critical path technically achievable by the plant, taking into account the design options, the Utility's maintenance policy and the regulatory constraints.

MAIN PHASES OF A REFUELING OUTAGE

The 4 main phases of a refueling outage are :
-the shutdown and core unloading phase,
-the maintenance and works phase,
-the core reloading and startup phase,
-the power increasing phase.

Figure 7 presents the relative importance of these different phases for the French 1300MW series, the German KONVOI series and for the European Pressurized Reactor project.

6.4.2. The EPR Refueling Outage study

The specifications of the EUR (European Utilities Requirements) and those of the EPRI recommend an outage duration for PWR units not exceeding 25 days. In the frame of the EPR (European Pressurized Reactor) very detailed comparative studies of the French and German operating experience were conducted and resulted in a refueling outage schedule of 19 days (from breaker to breaker). The related requirements, allowing one to reach this objective, were drawn up by the EDF and the German Utilities involved in the EPR and sent to the designer, NPI(Nuclear Power International).

A simplified schedule is presented in the Figure 8.

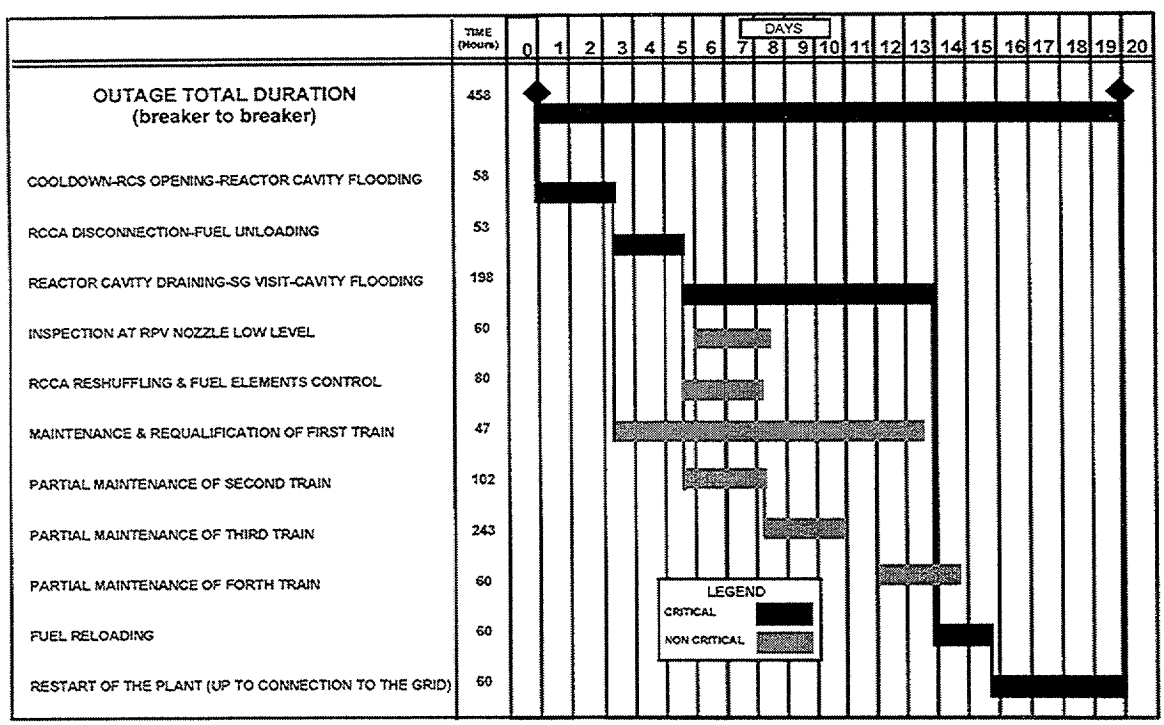


Figure 8 EPR Refueling Outage Schedule

6.4.3. Other EPR planned inspections

Turbine-Generator overhaul

The studies are not yet completed. Two scenarios are presently studied :

-general overhaul of the turbine-generator every 5 to 6 years,

-breakdown of the inspection of the generator and the turbine cylinders on each refueling outage.

Some other investigations are performed to optimize the handling and maintenance facilities. The related requirement will soon be provided.

10-Year Regulatory Inspection

The scenario proposed for the 10-year regulatory inspection outage of the EPR units uses the schedule of the shutdown and start-up phases adopted for the refueling outages.

The schedule of the works common to all these types of inspection (particularly maintenance and testing of switchboards adopted for the refueling outages) has also been reused.
For the other phases of inspection, works, testing (reactor coolant system hydrotest, containment pressure test), in the first analysis, the reference schedules for the 10-year inspection outage of 900 and 1300 MW French units have been adopted. The allocation for the EPR project is 49 days.

6.4.4. EPR availability assessment

Table I summarizes the main assumptions fixed for the availability assessment of the REP 2000/EPR project. These assumptions take into account the current practices in EDF.

Table I *EPR's Main Assumptions*

Unavailabilties	Data
10-year inspection	49 days
Turbine overhaul	34 days
Refueling outage	19 days
Yearly forced outages	2%
Outage extension for special works - 10-year inspection - turbine overhaul	 19 days 9 days
Start-up and tests : - start -up(by outage) - yearly tests	 24 hours 20 hours
Outage extension :	8 days

Table II *Three Operating Cycle of EPR*

Fuel cycle length (months)	Theoretical Availability	Target Availability	Realistic Availability
12	91,6%	89,1%	87,1%
18	93,2%	91,5%	90,2%
22	93,8%	92,3%	91,2%

Based on the hypotheses defined above, three cases corresponding to operating cycles of 12, 18, 22 months were investigated. The results are given in Table II.

6.5. Logistic Support methodology

The purpose of this methodology is to provide for systems the best balance between cost, schedule, performance and supportability.
For the future nuclear project, EDF has decided to engage an approach based on such a concept. It will be based on methods and standards adapted to the nuclear plant design. A detailed presentation of this approach is given in reference [2].

Early in the project, the CIDEM team engaged three actions :

-to define a list of main support element for a nuclear plant
-to define the methodology
-to apply during the development the methodology on a well known system to validate it.

- *List of the main support elements*

These elements represent an important cost and need perfect control of the related information.

These support elements are Maintenance Plan, Technical Data, Personnel Certification and Licensing, Tools & Test Equipment, Supply support, Computer Resources support, Packaging, Handling, Transportation and Storage, Facilities.

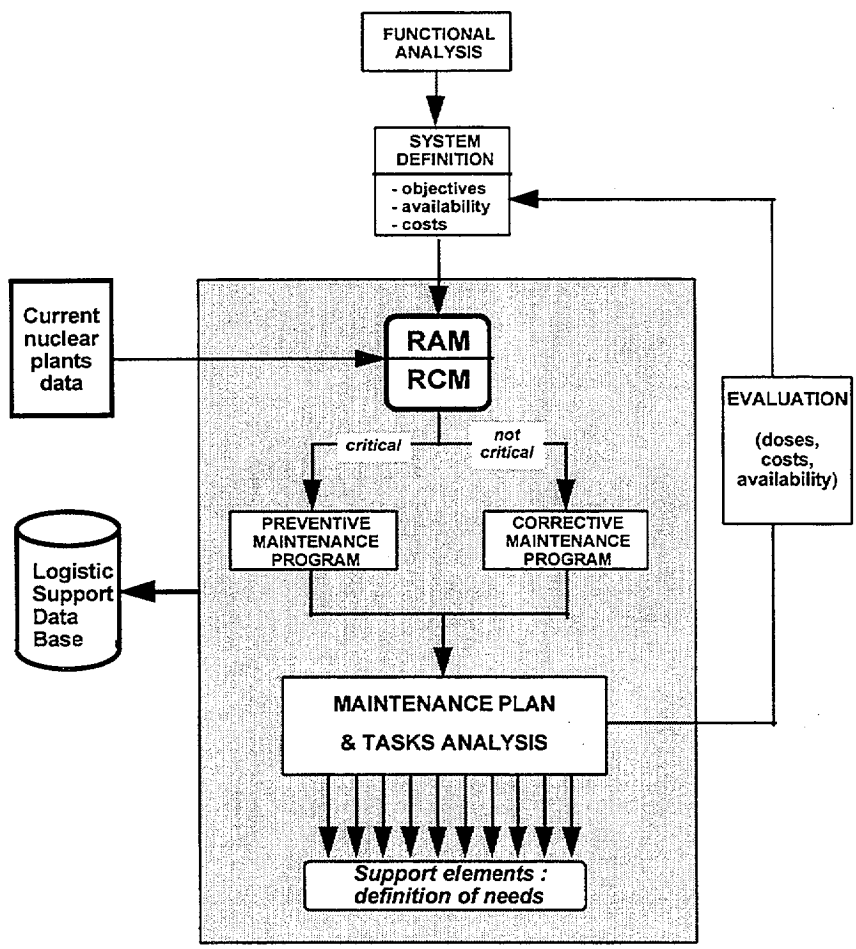


Figure 9 *Logistic Data Bases of the Main Support Elements*

- *Methodology*

The first studies implemented by EDF consist in defining the structure of a logistic data base which contains the specifications of the support elements.

The structuring of the data base in the project is a fundamental step for the process as shown in the Figure 9.

It is conducted in close relation with the methodology defining process, so that the data base is progressively filled during the design.

- *Application to a System*

The system chosen by the CIDEM team was the CVCS (Chemical and Volume Control System) of the EPR project. A RCM data base concerning this system is yet completed.

6.6. Next studies

The first studies carried out by EDF tend to prove that from a technical standpoint, the initial availability objective of 87% can be raised to 90%. On the other hand, the preliminary maintenance studies show that it is possible to control, even to decrease the maintenance costs by implementing the methodologies described above during the design process.

The next steps of the CIDEM studies will be :

-to perform a functional analysis on all critical systems of a REP 2000/EPR unit,

-to apply during the detailed design the RCM method on systems important for safety availability and cost, to define the first maintenance plan

-to build up a general program to optimize all spare parts and to integrate this program in the logistic support studies,

-to improve the unit management configuration,

-to continue studies on other support elements (training, tools, facilities, storage).

-to build and to operate a logistic data base on the REP 2000/EPR.

7. CONCLUSION

The implementation of the CIDEM process constitutes for EDF a new approach to the study of the new Nuclear Power Plant projects.

The studies conducted in the availability field have already highlighted a number of critical points and have made it possible to establish a first series of structuring specifications for the REP 2000/EPR project.

The integration in the design process of Preventive Maintenance and Logistic Support studies will allow a better control of the maintenance cost.

The competitiveness of nuclear energy greatly depends on the success of such an approach.

REFERENCES

[1] DEGRAVE C., MARTIN-ONRAET M., "Integrating availability and maintenance objectives in plant design - EDF approach", 1995, *3rd JSME/ASME Joint International Conference on Nuclear Engineering* - vol 3, pp 1483-1488, Kyoto / Japan

[2] DEGRAVE C., MARTIN-ONRAET M., MEUWISSE C. "Integrated Logistic Support concept in the design of Nuclear Power Plants", 1996, *4th JSME/ASME Joint International Conference on Nuclear Engineering* - vol 2, pp 27-31, New Orleans / USA

[3] CORDIER R., DEGRAVE C., MARTIN-ONRAET M. "CIDEM approach for improving availability and maintenance costs of future nuclear power plants", 1996, *TOPNUX'96 International Conference - vol 1, pp 222-233*, Paris / France

EPR DESIGN FOR MAINTENANCE

XA9848588

U. KRUGMANN
Siemens AG,
Erlangen, Germany

Abstract

Preventive maintenance is very important in achieving high plant availability. For the European Pressurized Reactor (EPR) preventive maintenance has been carefully addressed in the design stage. This is particularly necessary because of the traditionally different maintenance strategies employed in France and Germany. This paper emphasizes the following features introduced in the EPR design to minimize the duration of the refueling outage: (1) containment accessibility during power operation; (2) overall plant layout to facilitate inspections and maintenances within the containment; and (3) safety system design for enabling preventive maintenance during power operation.

1. Introduction

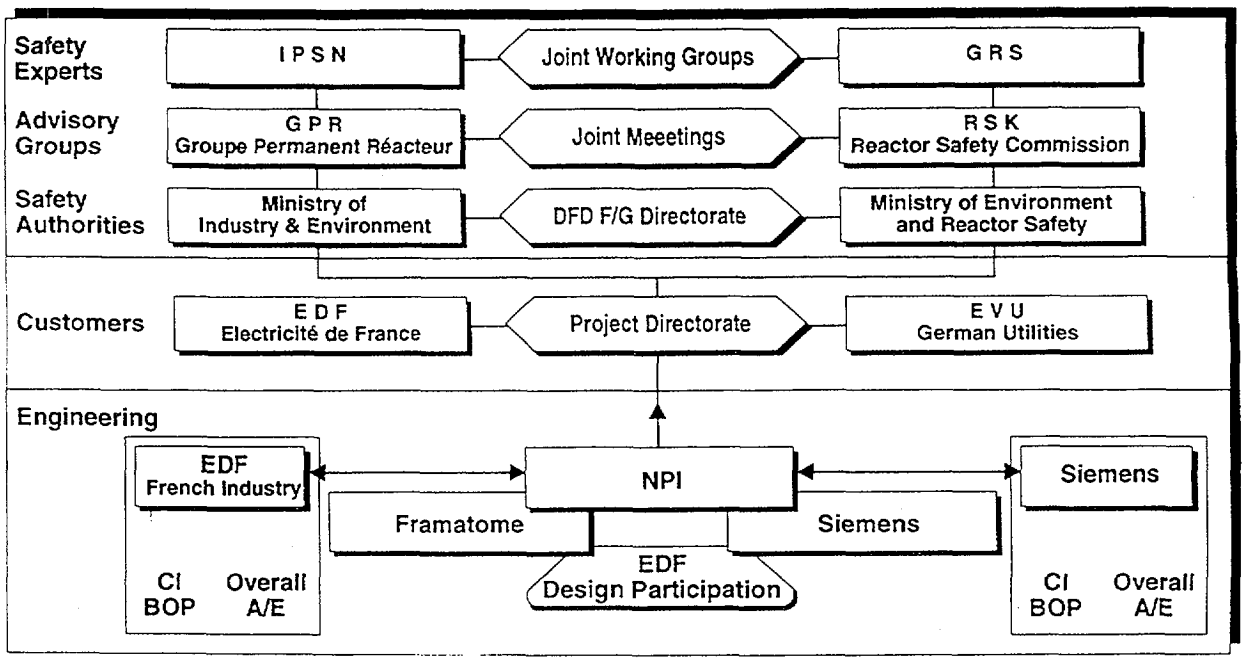
The economic objective of the EPR is competitivity with fossil power plants. This objective led beside others

- to the relatively high power output of 4250 MW_{th} which is presently again in discussion to be further increased
- to a design life of 60 years
- to the requirement of replaceability of the majority of components
- to a plant availability target of 87 % and, as a consequence
- to the objective to minimize the normal plant outage for refueling and revision works to less than 25 days.

It is obvious that these objectives can only be met if in an early design stage maintenance strategies are developed and translated into design. This is for the EPR even more important because traditionally in France and in Germany different maintenance strategies had been followed which needed to be harmonized.

For this purpose, the utilities in France and Germany have been involved since 1991 directly in the development of the EPR to ensure - beside others - that operational aspects and utility requirements in the field of maintenance enter immediately into design. Table 1 shows the partners involved in the EPR basic design.

TABLE I. EPR'S OVERALL ORGANIZATION



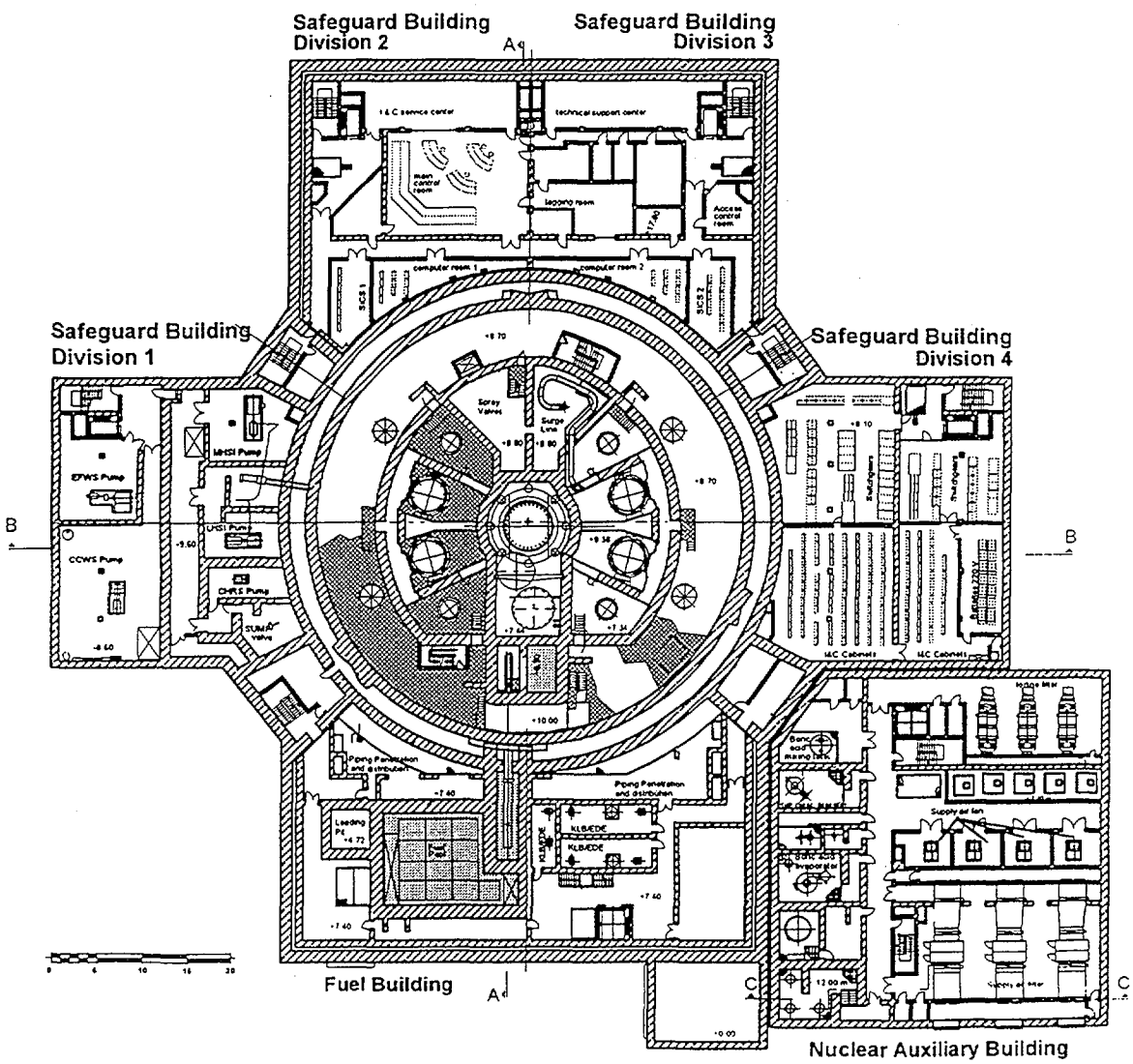


FIG. 1. EPR's Plant Layout, Nuclear Island and Plant View different Levels.

Before entering the subject of design for maintenance, let me shortly repeat some essential technical features of the EPR (Fig. 1): The EPR is an evolutionary 4 loop PWR developed on the basis of the French N4 and the German Konvoi designs. The 4-train-safeguard systems (mechanical, electrical and I&C) are allocated in 4 separated safeguard buildings. The reactor building has a double containment with a prestressed concrete inner containment without liner. Compared to existing plants containment free volume and design pressure are increased in order to cope with severe accidents. The fuel pool is allocated in a separate building outside the reactor building. The refueling water storage is allocated within the containment. The main control room is allocated on top of the safeguard buildings 2 and 3. The nuclear auxiliary systems are allocated in the Fuel Building and the Nuclear Auxiliary Building. The Diesel Buildings which belong also to the Nuclear Island, are not shown in Fig. 1.

In the following, I want to deal with some maintenance features introduced in the EPR design in order to minimize the duration of the refueling outage. The EPR standard refueling outage schedule is described in Fig. 2. Compared to the Basic Design objective mentioned in the beginning, it is furthermore shortened by roughly one week to 425 hours. With regard to this further reduction of the refueling outage duration, I want to highlight especially on

- the containment accessibility during power operation
- the overall plant layout in order to enable and improve revision works within the containment
- the safety system design for enabling preventive maintenance during power operation

2. Containment accessibility

An important improvement of the EPR compared to predecessor plants consists in an improvement of the confinement function.

This implies - as already mentioned - the consideration of severe accidents for containment design. Furthermore, a number of measures have been taken in order to improve the confinement function during normal operation.

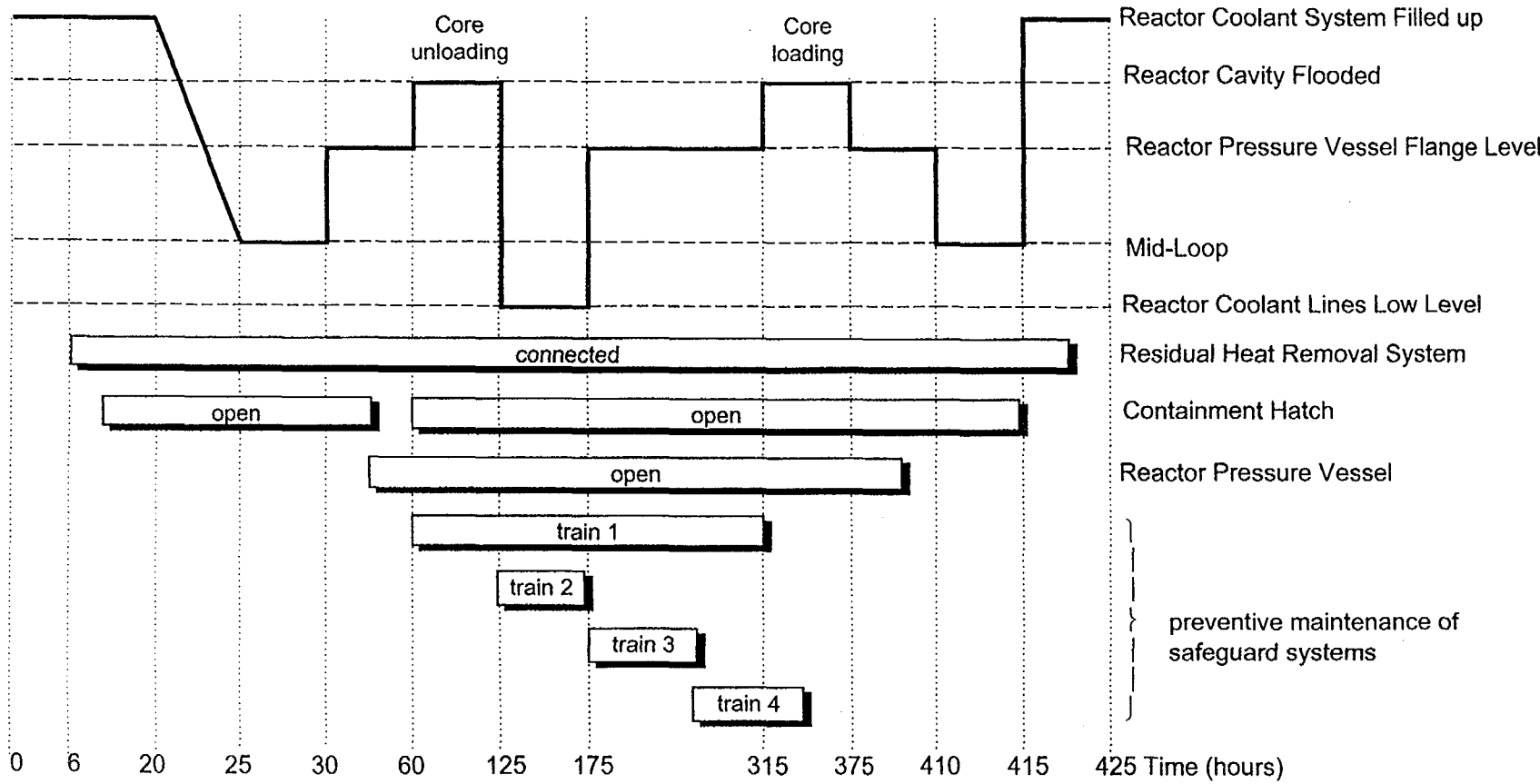


FIG. 2. EPR's Standard Refuelling Outage Schedule.

I want to mention in this context:

- The allocation of the residual heat removal system inside the reactor containment in order to reduce the containment bypass probability especially as long as the primary coolant is at temperatures above 100° C. For economical reasons, this feature is presently again under discussion.

- The closed ventilation system of the reactor containment during normal power operation.

Nevertheless, in order to relieve plant outage from preparatory functional and safety tests of lifting gears and other revision tools, as well as from final cleanup actions inside containment, the EPR containment shall be temporarily, especially about one week before and after refueling outage, accessible without need for heavy breathing apparatus. This is requested especially for the main service floor, as well as for the annular space between the missile shield cylinder and the inner containment wall (Fig. 3). It had to be investigated if for this purpose the heavy equipment compartments had to be equipped with a separated ventilation system, and had to be separated from the operating compartments, as it is the case for present German permanently accessible containments. Eventually, it turned out, that a one-room-containment is acceptable, provided sufficient containment purging capacity is available. This has advantages for accident and severe accident control with regard to equalization of pressure and homogenization of local hydrogen concentration.

3. Provision of sufficient service area on the operating floor

Because of the location of the fuel pool outside containment, there is no need for transportation of major pieces of equipment or material into or from the containment interior during power operation. However, after reactor shutdown for refueling, the multistud-tensioning device needs to be entered into the containment. It is stored immediately beside the equipment hatch in the fuel building in order to enable the common use for various units at one site (Fig. 4). For the purpose of transportation into the containment, the equipment hatch is opened at primary temperatures below 100° C (Fig. 2).

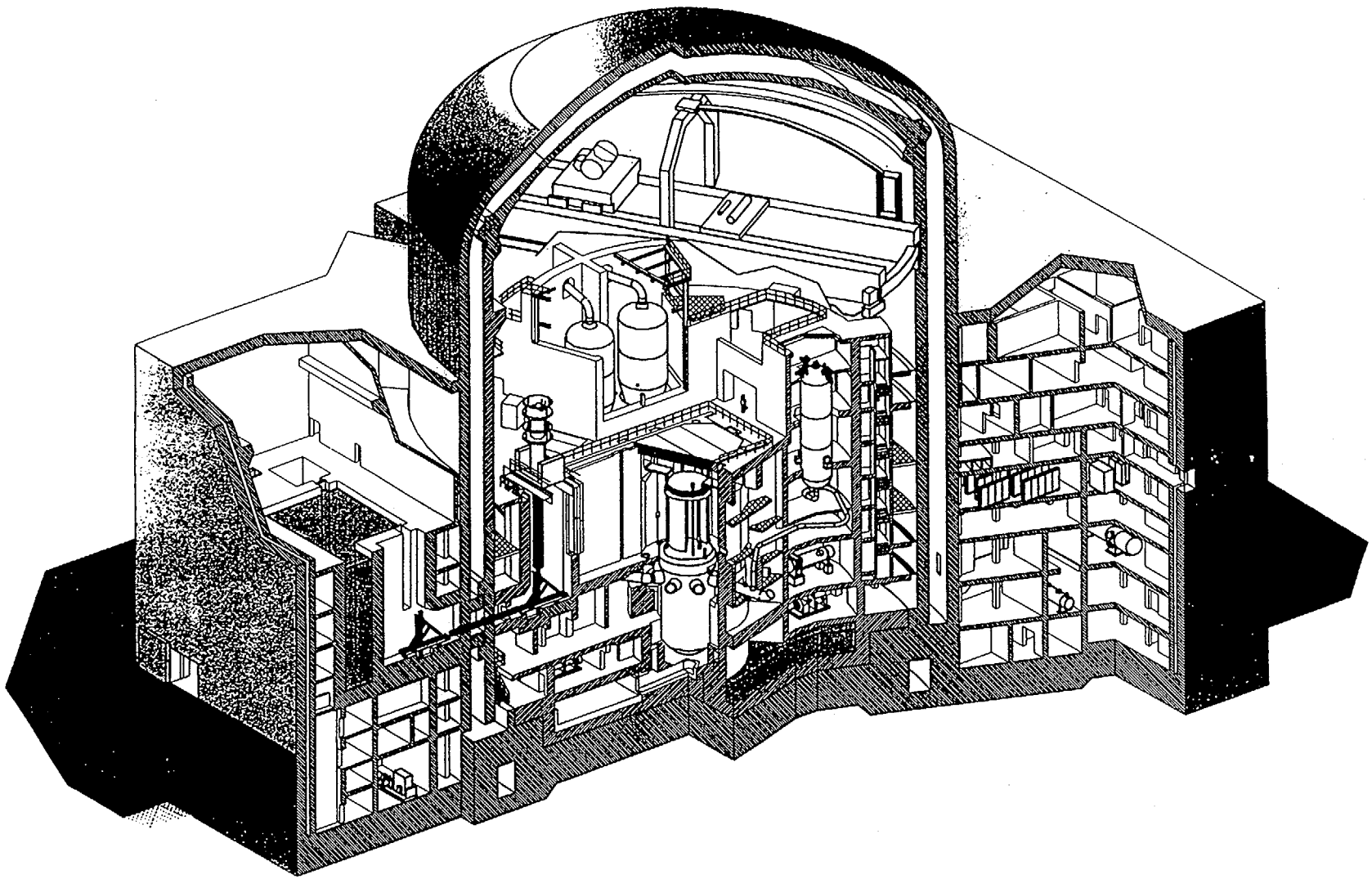
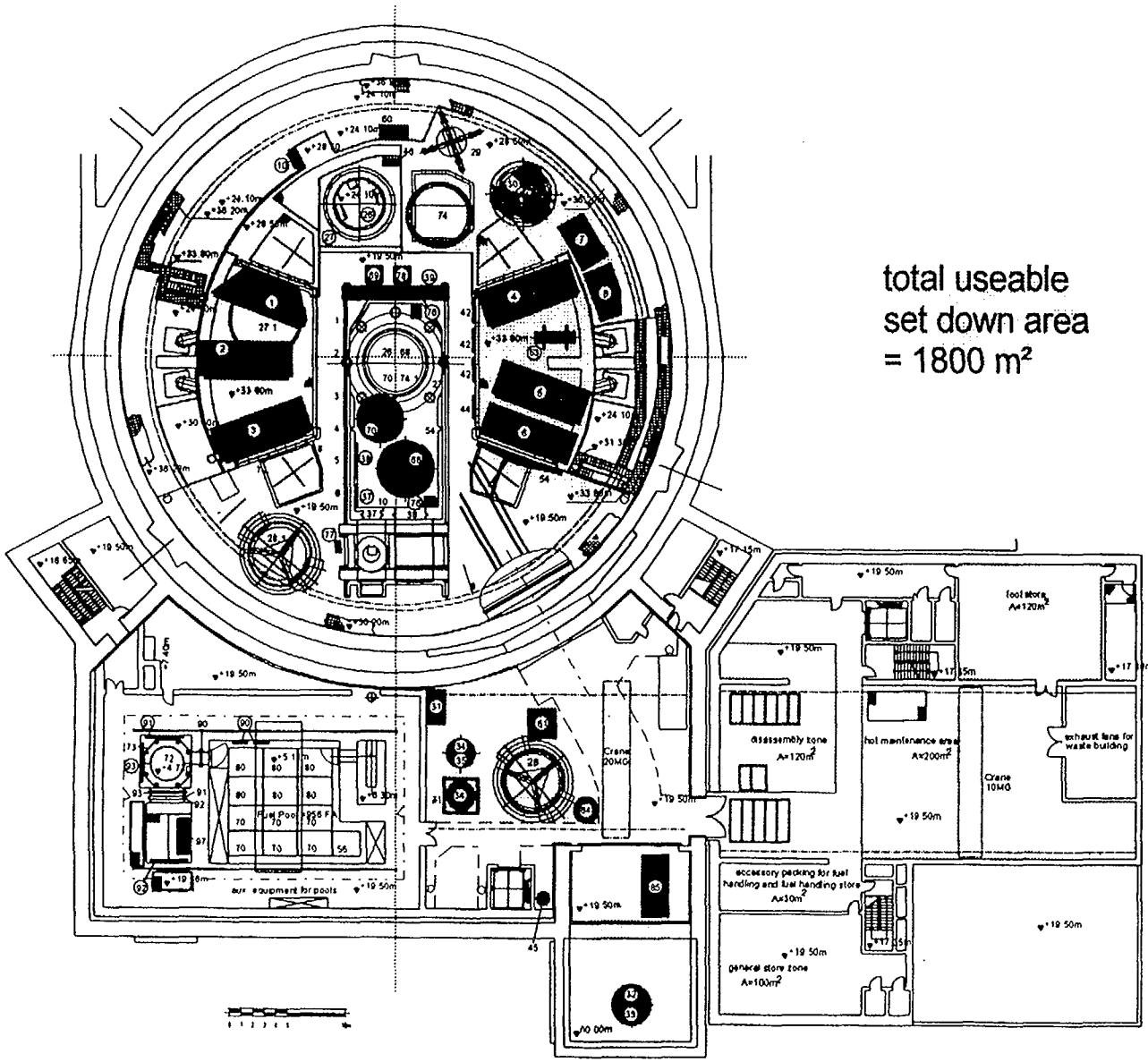


FIG. 3. EPR's Plant Layout, General Arrangement of Nuclear Island.



POS.COMPONETS AND PEACES
NR.
1 POOL SLABS
2 POOL SLABS
3 POOL SLABS
4 POOL SLABS
5 POOL SLABS
6 POOL SLABS
7 MCP SLABS
8 MCP SLABS
10 SHIELDING GATE (FOR THE TRANFER COMPARTMENT)
26 RPV CLOSURE HEAD WITH INSULATION
27 MOVING INSULATION COVER WITH ERECTION PLATFOM
27.1 TEMPORARY SET DOWN OF POS. 27
28 MULTISTUD TENSIONING DEVICE FOR RPV HEAD
28.1 TEMPORARY SET DOWN OF POS.28
29 LIFTING DIVICE FOR RPV HEAD
30 LIFTING UNIT FOR CORE INTERNALS
31 SLABS ABOVE DECONT. STATION OF MCP
32 MOTOR OF MAIN COOLANT PUMP
33 ERECTION RACK FOR MOTOR OF MCP
34 INTERNALS OF MAIN COOLANT PUMP
34.1 TEMPORARY SET DOWN OF POS. 34
35 ERECTION RACK FOR INTERNALS OF MCP
37 TRANSFER COMPARTMENT GATE
38 LANCES COMPARTMENT GATE
39 AUXILIARY PLATFORM
42 HANDLING TOOLS (FUEL LANCES,DRIVE SHAFT)
44 TRANSPORT TOOL FOR INSULATION COVER
45 HYDRAULIC BOLT TENSIONING DEVICE FOR MAN HOLE
46 SLIDING ROD AND SPARE BOLTS FOR RPV HEAD
53 LIFTING UNITS FOR CONCRETE SLABS
54 REACTOR CAVITY GATE
60 LIFTING DEVICE FOR REACTOR CAVITY GATE
61 CLEANING UNIT FOR MSTD
68 CORE INTERNALS
69 SWITCHBOARD FOR RPV MULTISTUD TENSIONING DEVICE
70 HEAVY REFLECTOR
72 CASK CONTAMINATION PROTECTION SHIRT
73 CASK FILLING PLATFORM (LOADING HALL ñ0.00m)
73.1 TEMPORARY SET DOWN FOR CASK FILLING PLATFORM
74 DUMMY RPV HEAD
74.1 TEMPORARY SET DOWN OF POS. 74
76 ELEVATOR PLATFORM
77 CONTROL DESK FOR TRANSFER
78 CONTROL DESK FOR REFUELING MACHINE
84 LIFTING DEVICE FOR MCP
85.1 MAINTENANCE AREA FOR ROTOR OF MCP MOTOR
90 SHIELDING GATE BETWEEN SFSP AND SFCP (TWO PARTS)
91 SHIELDING GATE FOR LOADING PIT (PART 1)
92 SHIELDING GATE FOR LOADING PIT (PART 2)
93 WATER GATE FOR LOADING PIT
97 LIFTING DEVICE FOR CASK

Example:
59 ERECTION PLACE
(69) SET DOWN AREA
27.1TEMPORARY SET DOWN
(7) SET DOWN AREA OF LOWER PART

POSSIBLE SET DOWN AREA

FIG. 4. EPR's Set Down Area during Outage.

At these operating conditions, the risk for fast pressure transients in the containment is relatively low, so that a continuous preservation of the containment function is not necessary, and there is no need for a material airlock.

However, because there remains a risk during reduced primary water level with open reactor pressure vessel, the equipment hatch is closed again provisionally before the reactor pressure vessel head is lifted (Fig. 2).

After flooding of the reactor cavity, the equipment hatch is kept continuously open in order to enlarge the service area at the operating floor by approximately 800 m^2 in the fuel and nuclear auxiliary buildings, e.g. for revision works like decontamination of the reactor coolant pump impeller or servicing of the reactor coolant pump motor.

During this period of time, a dynamic activity confinement is ensured in the enlarged service area. For transportation of major pieces of equipment into or from this area, e.g. of the reactor cavity concrete slabs, or of the multistud-tensioning device, the fuel building gantry is designed as an airlock.

4. Preventive maintenance of Safety Systems

It is the objective of the French and German utilities that preventive maintenance of the safety systems during refueling shutdown is not on the critical path (Fig. 2).

In one train, a full mechanical and electrical maintenance including subsequent re-qualification tests is foreseen, in the other trains, only partial mechanical and electrical inspections shall be performed. The outage of 1 safeguard system train is accepted during core loading and unloading, the outage of 2 trains is accepted with unloaded core. During this last period of time the only safety functions to be performed are fuel pool cooling by the 2-train fuel pool cooling system, and maintenance of the dynamic confinement function by the 2 train controlled area ventilation system.

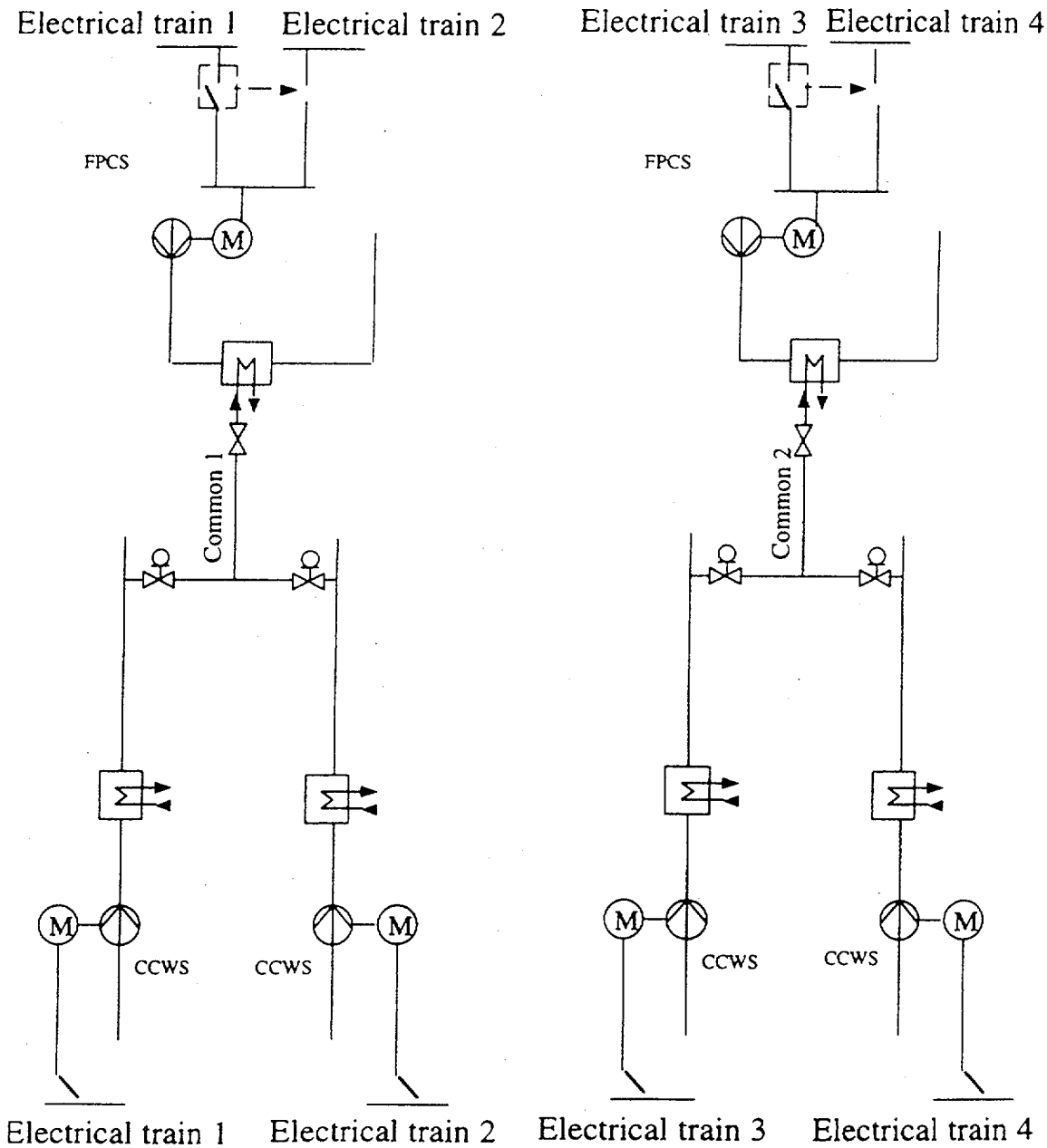


FIG. 5. Design of Fuel Pool Cooling System for Maintenance.

In order to be able to perform preventive maintenance during this period of time on 2 cooling chain and electrical trains, each fuel pool cooling train is connected via a header to 2 cooling chain trains, and via special switching elements to 2 electrical trains (Fig. 5). An equivalent cross-connection would be necessary for the electrical power supply of the controlled area ventilation.

TABLE II. EPR'S PREVENTIVE MAINTENANCE OF SAFETY SYSTEM DURING POWER OPERATION

System/Equipment	No. of trains	Preventive Maintenance Duration during Power Operation	Remarks
Safety Injection System	4	28 days/system 14 days/train	except accumulator injection
Fuel Pool Cooling System	2	28 days/system	
Component Cooling System Service Water System	4	28 days/system 14 days/train	Only for safety-classified portion; no preventive maintenance to be done for common headers except FPCS header
Emergency Feedwater System	4	28 days/system 14 days/train	
Emergency Diesel Generators	4	28 days/system 14 days/train	including support and cooling systems, as well as correlated electrical busbars

TABLE III. EPR'S UTILITY REQUIREMENTS FOR PREVENTIVE MAINTENANCE DURING POWER OPERATION

System/Equipment	No. of trains	Preventive Maintenance Duration during Power Operation	Remarks
Electrical switchboards 10 kV, 690 V, 380 V	4	coherent with systems maintenance	only interruptible power supply
Batteries	4	48 hours/train	discharge/reloading tests
Safety-classified Ventilation Systems (non-controlled area)	4	to be specified	including electrical divisions and chilled water system
Safety classified Ventilation Systems (controlled area)	2	to be specified	except annulus accident ventilation system

Behind this solution is the requirement raised by the French Group Permanent Réacteur and the German Reactor Safety Commission, that for safety systems required during all reactor states, including shutdown, scheduled maintenance has to be superposed with a single failure, taking into account the required capacity of the corresponding safety function during this maintenance.

In order to meet the requirement that the refueling schedule is not determined by safety system maintenance, the utilities requested the investigation of the possibility to do preventive maintenance during normal power operation to the extent specified in Tables II and III.

In addition the following requirements for this investigation were specified:

- the demonstration that the specified maintenance times are acceptable should be done either deterministically as above for the fuel pool cooling system, or probabilistically; preferably, major modifications as for example significant oversizing of pump flow rates or heat exchanger capacities which had been achieved on a n+1 basis, that means considering only 1 outage due to a single failure, should be avoided

- preventive maintenance on different components during plant power operation will only be performed within 1 train simultaneously

- preventive maintenance on 1 train shall not induce any reduction of the reliability and availability of remaining plant, and especially of the other safety trains

- preventive maintenance during plant power operation should not induce an unacceptable reduction of admissible repair times

Because for the EPR the majority of safety systems is designed as 4 train systems (except residual heat removal system, fuel pool cooling system and some ventilation systems) with strict train separation, the n+1 redundancy requirement determines essentially system dimensioning. In this context it has to be mentioned that beside deterministic safety requirements, availability or operational requirements have been considered for EPR safety system dimensioning.

An example is the emergency feedwater system, where for probabilistic reasons the system has been sized such that 1 train is sufficient for heat removal in case of loss of main feedwater (Fig. 6).

Another example is the medium head safety injection(Fig. 7). For operational reasons it is designed in such a way that for very small primary leaks (≤ DN 25) the water level in the reactor pressure vessel will not decrease below the main coolant line nozzles considering a single failure. This means implicitly that a (n+2)-redundancy is

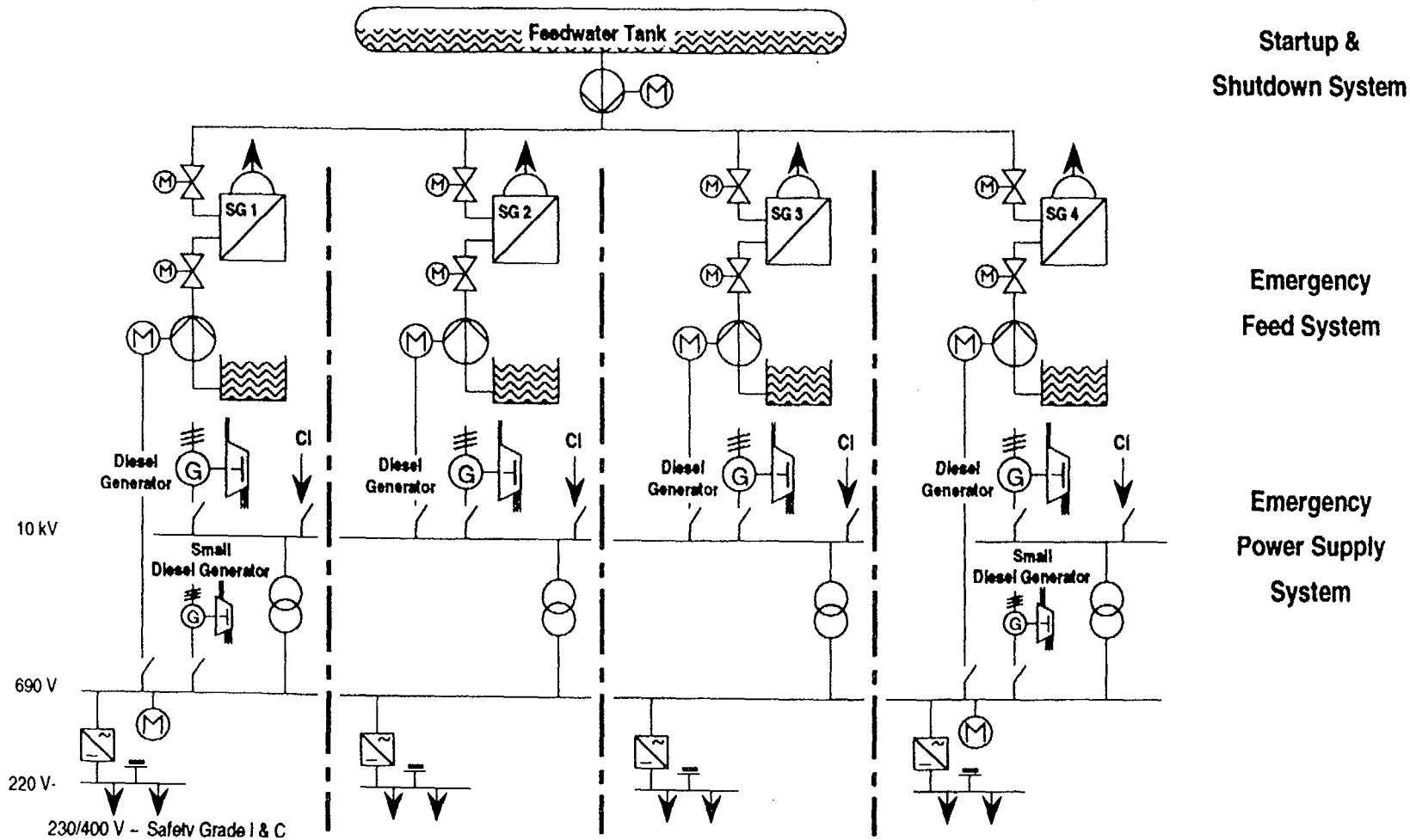


FIG. 6. EPR's Conceptual Arrangement of SG Feed Including Electrical Power Supply.

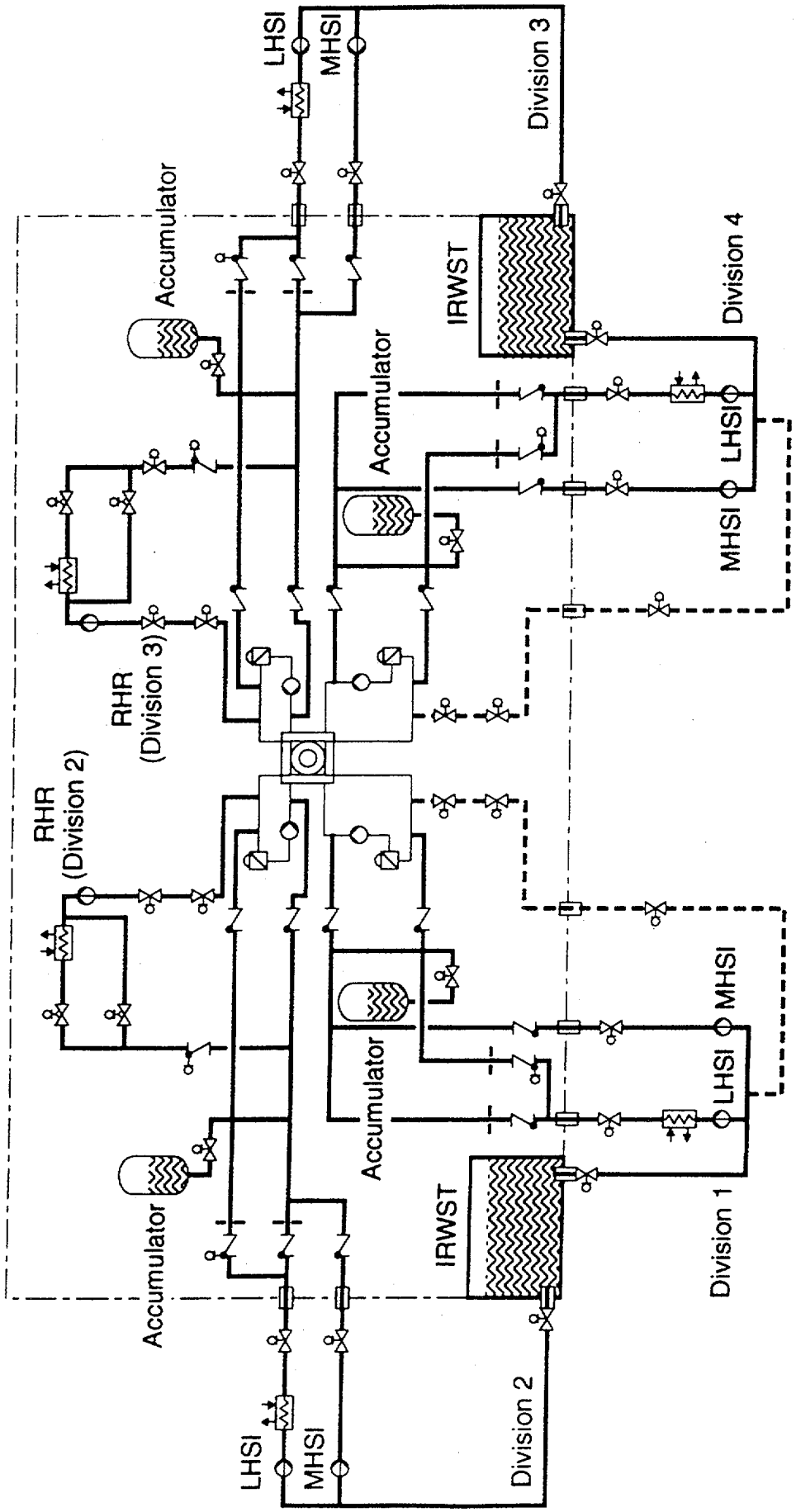


FIG. 7. EPR's Primary Side Safety Systems.

achieved for all primary leaks where the medium head safety injection is required with regard to the relevant safety criterion "limited core heat-up".

Furthermore, for a number of safety systems functionally diverse back-ups are provided which is de facto equivalent to a higher redundancy of the safety system function. An example is the 2 train residual heat removal system which can be backed-up by 2 trains of the low head safety injection system at primary temperatures below 100° C (Fig. 7).

TABLE IV. EPR'S PREVENTIVE MAINTENANCE OF SAFETY SYSTEM DURING POWER OPERATION

Maintenance has to be performed during Power Operation for:	Maintenance can be performed during Power Operation
• Fuel Pool Cooling System with the correlated Component Coolers headers • Controlled Area and Fuel Building Ventilation	• Safety Injection System • Residual Heat Removal System (although not intended) • Emergency Feedwater System • Component Cooling System (safety-classified part) and Service Water System • Non-controlled Area safety-classified HVAC Systems • Emergency Diesel and Parts of MV and LV switchgear and busbars • Main Control Room Ventilation • Safety-classified Chilled Water System

TABLE V. EPR'S PREVENTIVE MAINTENANCE OF SAFETY SYSTEM DURING POWER OPERATION

Maintenance cannot be performed during Power Operation
• RCS isolation • Containment isolation • SG isolation • RCS hot leg letdown • SG steam relief • uninterruptable LV busbars and switchgear • DC busbars • Annulus ventilation

In consequence, there was already extra redundancy available in EPR safety system design which could be used for

- doing preventive maintenance by satisfying the licensing requirement of the French and German authorities to deterministically superpose outage due to preventive maintenance with an additional single failure, and thereby for
- relieving time pressure during revision outage due to safety system maintenance work which could be done in a more relaxed manner during normal power operation.

The results of the investigation are outlined in Table IV and V. They can be summarized as follows:

Maintenance of those 2 train systems which are functionally necessary during refueling outage has to be done during power operation. For their auxiliary functions cooling and electrical power supply train cross-connections are necessary as discussed above for the fuel pool cooling system (Fig. 5).

Maintenance of the majority of safety systems which are 4-train systems is possible during power operation without any need of resizing because of existing design margins.

Not possible is preventive maintenance especially for all those safety functions which are provided by valves, in general 2 valves in series, and their power supply which is provided by the uninterruptable LV and DC power supplies, unless additional measures for ensuring redundancy in case of maintenance are provided. This is presently not foreseen for the EPR because of reasons of train separation.

Conclusions

Preventive maintenance is an essential aspect with regard to plant availability. I have tried to outline for some examples that early consideration of maintenance needs in the design is necessary and contributes to improve the overall plant performance and to optimize especially the refueling outage.

NEXT PAGE(S) left BLANK

XA9848589

AVAILABILITY AND ITS CORRELATION WITH THE COST SITUATION OF NPPs AND AN ADVANCED REACTOR AS A POSSIBLE FUTURE SOLUTION

M. FUCHS
PreussenElektra,
Hannover, Germany

Abstract

The availability depences from a lot of factors, especially from design approaches. The way for the development of design approaches for attaining the safety requirements with more redundancy and without diversity of the systems, especially of safety systems, in NPP's in the past is not acceptable for the future because of cost reasons. It is necessary to find new technical ways to achieve a better availability, reliability and safety by lower costs. The simplification of safety systems by using passive systems may be a solution in the future. The development of a new boiling water reactor BWR 1000 in Germany by Siemens which is sponsored by german utilities and supported by various European partners can be named as such example.

Introduction

Thank you, Mr. Chairman. Good afternoon, Ladies and Gentlemen. I am working for the german utility PreussenElektra in North-west of Germany. This company has the technical responsibility for four Nuclear Power Plants in Germany and it is a share holder of some other NPP's. Some slides in my presentation relate to the following PreussenElektra NPP's (Table 1).

I am very pleased to have an opportunity to present our results of availaibility and to adress some facts of the correlation between availability and the cost-situation. The availability means in this case the technical development of the NPP's during the last time. I like to show, that an extensive development with more redundancy without diversity of the systems, especially of safety systems, in NPP's is not acceptable because of cost reasons. It is necessary to find new technical ways to achieve a better availability, realibility and safety by lower costs. The present task is to verificate if the the simplification of safety systems by using passive systems may be a solution in the future. The development of a new boiling water reactor BWR 1000 in Germany by Siemens which is sponsored by german utilities and supported by various European partners can be named as such example.

Table I PreussenElektra's Nuclear Power Plants

Unit	year of start up	typ	output power in MW
Stade	1972	PWR	640
Unterweser	1978	PWR	1230
Grohnde	1984	PWR	1300
Brokdorf	1986	PWR	1307

Availability

The availability of german nuclear power plants during the last 10 years is shown on Fig.1.

It is constantly higher than 80%. A certain reducement can be noticed from 1988 to 1991. Especially during the period 1990-1991 was done a great amount of work at the pressurizer safety valves because of safety requirements. In addition as a consequence of Chernobyl a high number of modernizations-measures in the field of accident management in order to cope with severe accidents were undertaken during this period. After this time we can watch a stable operation of NPP's.

The availability depences from a variety of factors, such as:
- Design approaches and technologies,
- Behaviour in terms of normal operation and transients
- Design for optimised outages
- Optimal conditions for preparation of outages (informations about the state of components)
- Level of education and training of operators
- Relationship with the authorities

Cost situation

An intensive development of design approaches, especially with the purpose to increase the safety, took place in the past. It was required because of following circumstances:
- Design of NPP's for external hazards (aircraft crash and earthquake),
- High expenses for nuclear specific components, also outside the primary circle
- Increase of redundancy, especially for safety systems in order to control the external hazard-events (for example, four additional emergency diesel generators and four additional trains emergency feedwater systems protect against external hazards)

The final result was a much more complicater but only a little bit safer plant. Especially the probability of severe accidents was not substantially reduced, because it is not determined by external hazards, but by common mode failures.
The noticed measures caused the extreme growth of costs for NPP's.

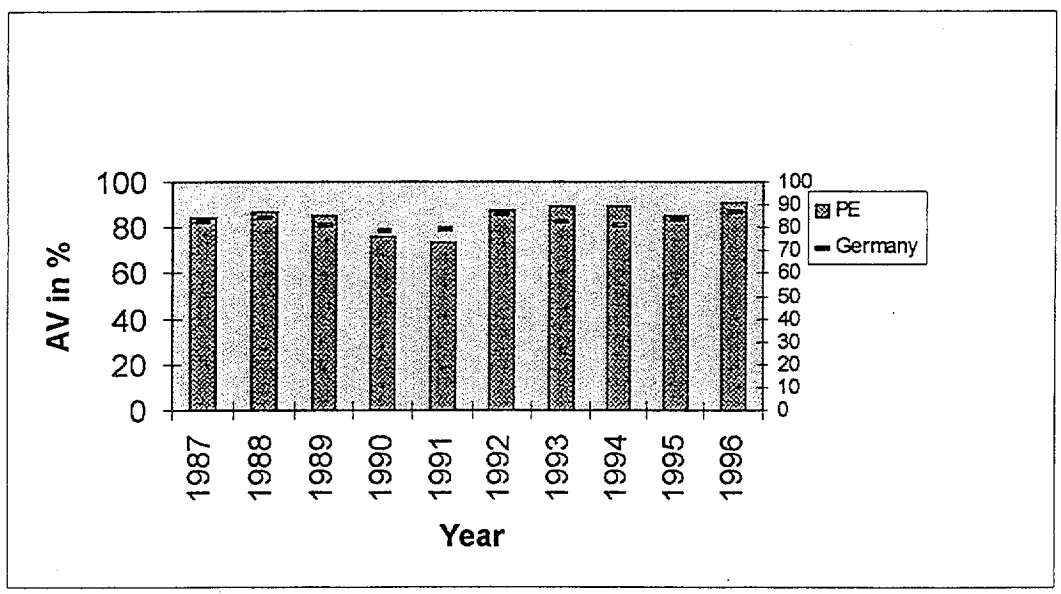


Figure 1 Availability German's NPP

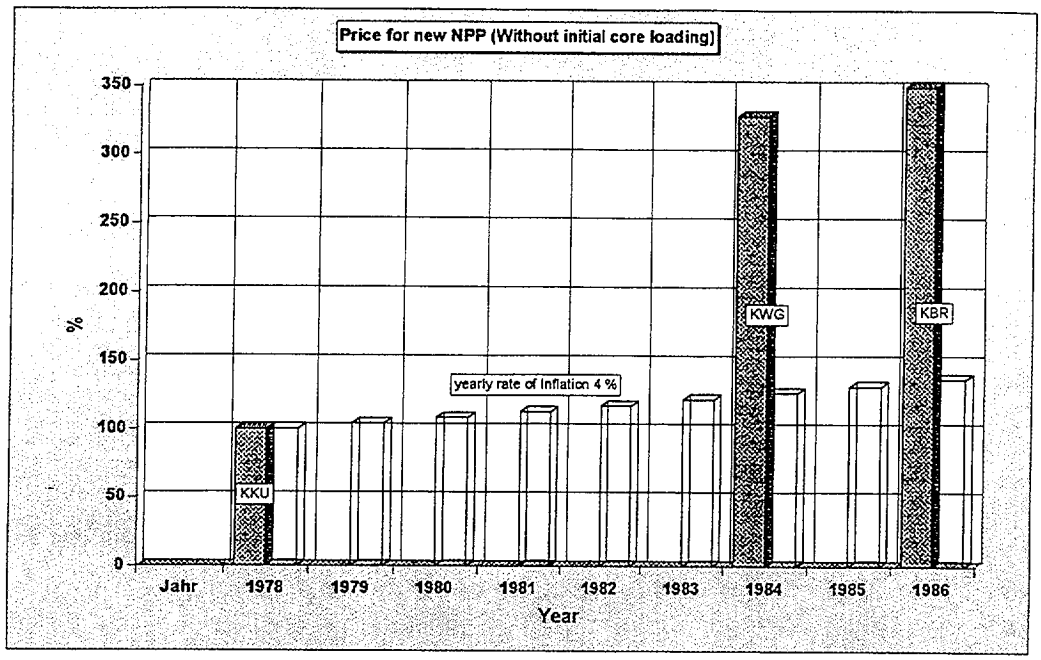


Figure 2 *Costs Compararision between three NPP of PreussenElectra Utility*

On Fig. 2 is shown a comparison between the investing costs for three NPP's of PreussenElektra.

The NPP KKU (Unterweser) was built in 1978. 6 years later the investing costs for NPP Grohnde (KWG) with approximately the same electrical output was more than three times higher. Taking the inflation-rate into account the investment costs by an equal design might have been increased only 1,3 times.

Not only the new NPP's were affected with such a growth of costs. Even the existing plants had to be additionaly improved. The Fig. 3 shows the costs, which were arisen by the additional improvements and repairs because of design lacks and material reasons.

Further expenditures for attaining of new safety regulatory requirements were generated (Fig. 4), which partly exceeded investment costs.

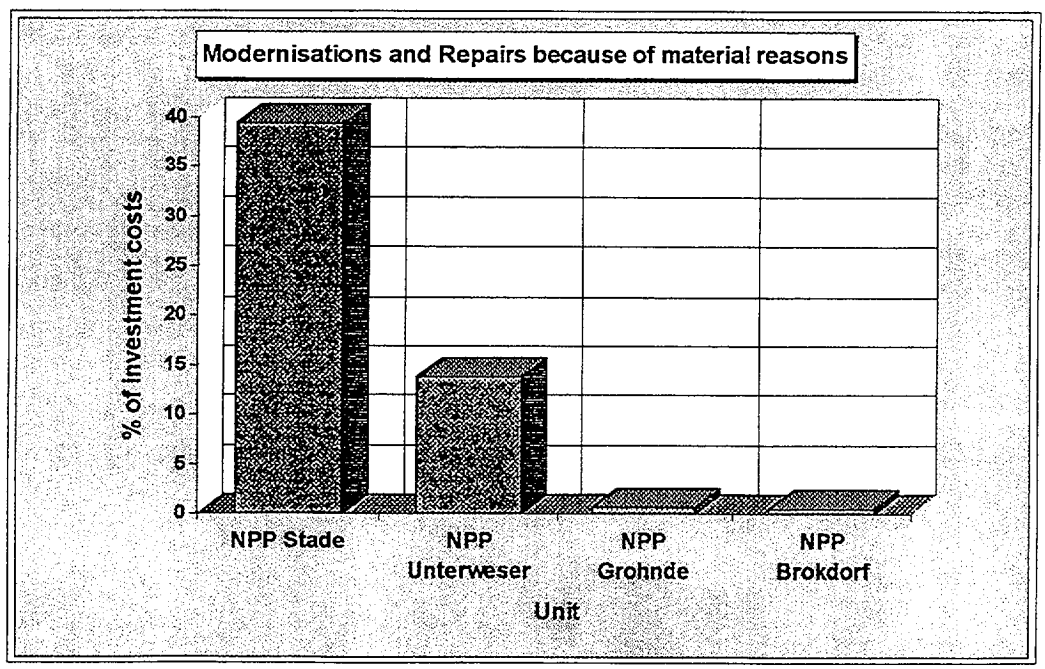


Figure 3 *Costs due to Modernisations and Repairs*

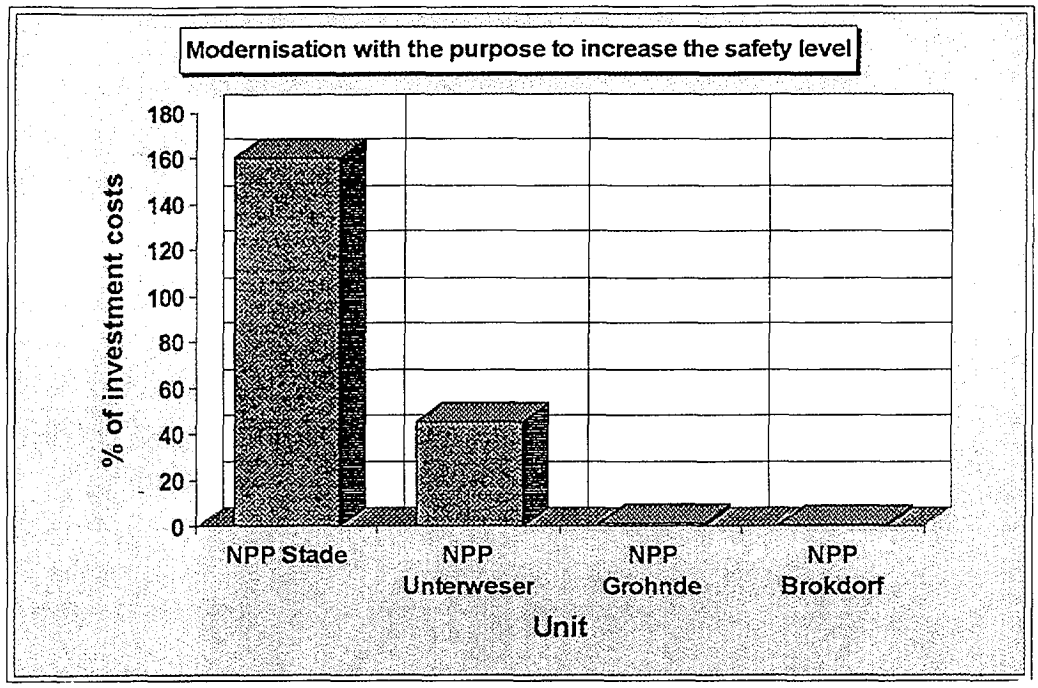


Figure 4 *Additional Costs due to the New Safety Regulatory Requirements*

Such an evolution and further cost-factors, especially in the waste management caused the situation, that nuclear energy today is not without hesitation the cheapest source of energy. The situation with the nuclear energy was additionally complicated with the fact, that the prices for coal and gas during the last years constantly decreased. Above it with the increasing of power efficiency also the investment costs for fossile-fired plants decreased. The fossile-fired technology has become more competitive with nuclear power.

On the other hand we know about the existance of some issues, which shows the advantages of nuclear energy. For example, a well operating plant produces no emissions harmful for the enviroment and the atmosphere, especially greenhouse gases.

Were is the way out?

In the present time we can watch an evolutionary and a revolutionary or innovative lines of development of nuclear plants. I think, that the optimum for the future should include the advantages of both development-lines in new projects. It means:

- For the production of energy (non safety grade systems) we should use proven technology with a high reliability. For such systems it has to be possible to use only one train without redundancy and to achieve in this case a good availability.
- The active safety systems for decay heat removal can be partly replaced and partly completed with passive features for safety. The passive systems should give the possibility for a substantial simplification for the whole system, I&C-systems and power supply.

In this case we can be sure, that we are noting an important technical requirement: Not too long development-strides from the existing technology. On the other hand, we are opening the door for a new generation of nuclear plants with a better competitive examination, higher safety level and I hope with an increased public acceptance.

Two types of NPP's are in development in Germany now. I prefer to speak about the development of the BWR 1000, because of a high number of publications about the European pressurized water reactor (EPR), which is being worked out in cooperation with France.

Development of a new BWR

As an example of a reactor, which connects the advantages of the evolutionary and a revolutionary lines, I like to present you the development of a new boiling water reactor BWR 1000 in Germany by

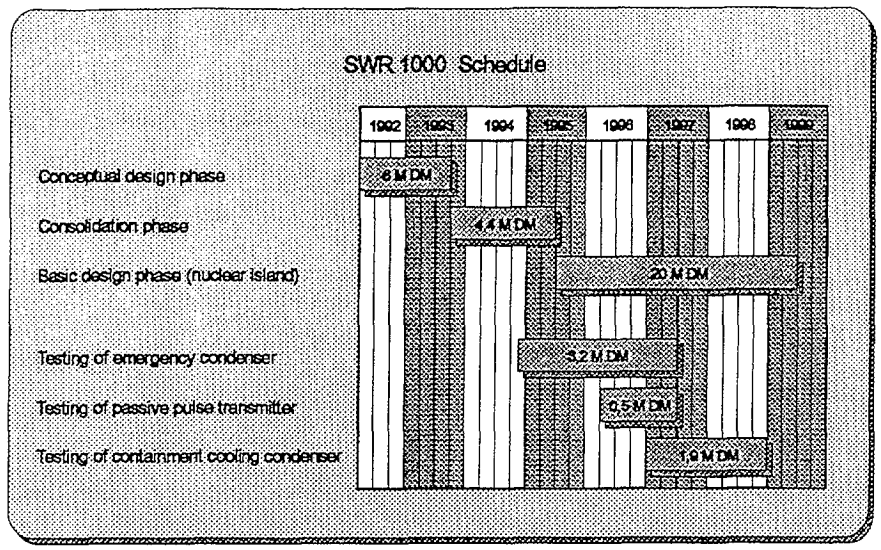


Figure 5 *Costs Resulting from Development of a New Boiling Water Reactor BWR 1000*

Siemens. The project is sponsored by German utilities and supported by various European partners. The work has been started in 1992 (Fig. 5), based on the following principal goals:
- To reduce the probability of a severe accident, especially of core melt,
- To control a core melt accident in such a way, that the consequences o f the accident remain restricted to the territory of the plant,
- To make the economy comparable with already existing large nuclear or coal-fired plants.

The following principal design-decisions were made for attaining the afore- mentioned goals:
- Low core power density will be combined with large water inventories in the reactor pressure vessel in order to achieve a good-natured behaviour in terms of normal operation, transients and accidents,
- Passive systems will be used in combination with a reduced number (combined to existing plants) of active systems. This diversity makes possible to exclude the probability of common mode failures in such safety systems and to reduce in this way the probability of severe accidents. On the other hand, the passive systems gave the possibility to simplify the technology of systems, I&C and power supply for attaining the economic goals.
- The water inventories for passive systems are calculated for a grace period of several days before manual intervention by operating personnel will become necessary. This design feature helps to control the plant after external hazards.
- The area around the reactor pressure vessel will be flooded in case of risk for a melting core, in order to ensure retention of the molten core inside the vessel and to achieve the removal of heat through cooling of the reactor pressure vessel exterior.
- Proven components and technologies with simplifications based on operating experiences in existing plants will be used in active safety systems and non safety grade systems, especially in the turbine area.

The main technical characteristics of the design concept are shown on the Table II in comparison with the parameters of the most modern existing BWR in Germany, Grundremmingen B and C.

The striking differences between existing BWR's and BWR 1000 are in the reactor internals (Fig. 6). The length of core is about one meter shorter and the average power density is probably 17 % lower. These issues in conjunction with a different fuel rod geometry decrease the average linear rod power to 44 This is the main factor contributing to the reactor's good behaviour during normal operation and transients, which also provides the basic prerequisite for achieving higher discharge burnups.

The feedwater and main steam nozzles as well are positioned higher. The diameter of the chimney above the core has been necked down in order to reduce the volume of the steam-water-mixture. All this features provide a water inventory above the core that enables the reactor to be depressurized without any feedwater make-up and without any risk of core uncovery.

Table II *Technical Characteristics of New BWR 1000*

	BWR 1000	Grundremmingen B/C
Plant		
Thermal power	2778 MW	3840 MW
Gross power output	1013 MW	1344 MW
Net power output	977 MW	1284 MW
Reactor core		
Number of fuel assemblies	684 (12 x 12)	784 (9 x 9)
Number of control rods	157	193
Length of active fuel element	2,80 m	3,76 m
Average power density	48 kW/l	56,8 kW/l
Average enrichment	5,3 %	3,14 %
Discharge burnup	65 GWd/t	35 GWd/t
Fuel cycle length	1 year	2 years

	BWR 1000	Grundremmingen B/C
Reactore pressure vessel		
Inner height	22,7 m	22,35 m
Inner diameter	7,00 m	6,62 m
Design pressure	88 bar	87,3 bar
Number of internal recirculation pumps	6	8
Containment		
Inner diameter	34 m	29 m
Inner height	28,7 m	32,5 m
Turbine		
Speed	25 s^{-1}	50 s^{-1}
Number of casings	1/3	1/3

The main innovations in the design concept has been achieved by introducing passive safety features which provide redundancy and diversity for a reduced number of active safety systems. As long as the reactor vessel is closed, the passive systems are capable to control an accident entirely by themselves for a period of several days without any need for manual intervention, even if there has been a complete loss of power. The following passive features are integrated into the concept:

- Emergency condencer for the heat removal from the reactor water,
- Gravity core flooding for core flooding depressurized reactor,
- Containment cooling condenser for heat removal from the containment atmosphere,
- Passive pressure pulse transmitter.

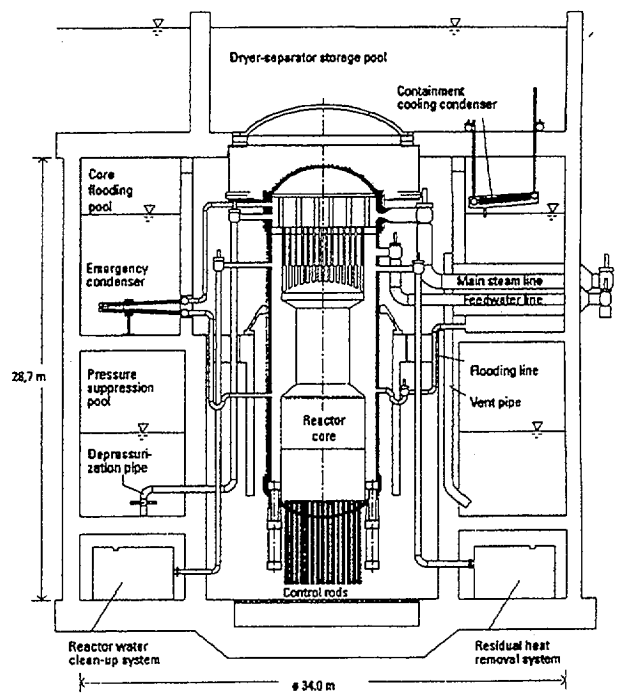


Figure 6 *Reactor Vessel of the New BWR 1000*

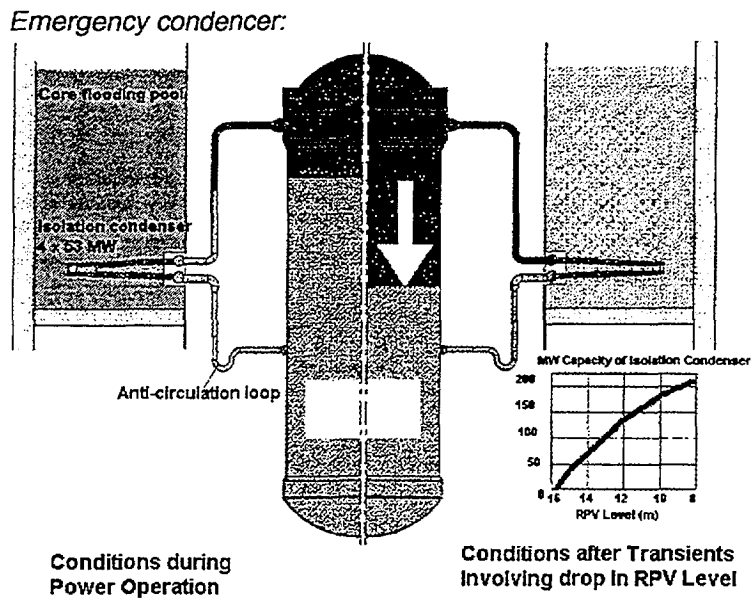


Figure 7 Passive Features of the New BWR 1000

The four emergency condencers are located in the core flooding pool and conected with the reactor pressure vessel by non-isolated steam discharge and condensate return lines (Fig. 7). Condensate lines contain an anti-circulation loop (termosiphon), so that practically no circulation of reactor water takes place through open lines by a normal water level in the reactor.

If the water level in the reactor is droping, the steam will enter the condensator and the condensate will return into the reactor vessel. The energy will transfer to the water of the core flooding pool, which will slowly raise its temperature. If the water will not be cooled, it begins to evaporate after 10 hours. The emergency condencer was tested in the Forschungszentrum Julich. The condenser showed no problems during all operation phases of the tests. Because of thermosiphon, as long as the primary water level remains higher than the heat exchanger pipes, is the convective heat transfer unpossible. The power rate depends from the water level and the pressure. It corresponds very well with the calculated rates.

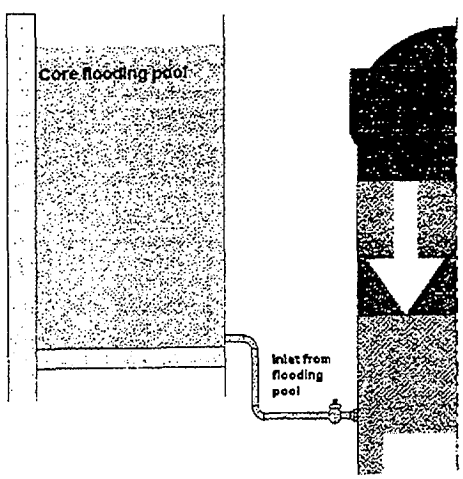


Figure 8 Gravity core flooding:

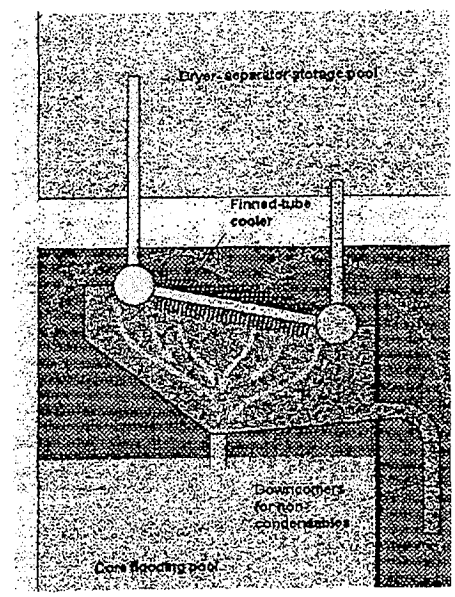


Figure 9 Containment cooling condenser.

In case of a loss-of-coolant accident (LOCA) or depressurisation of the reactor with the safety-relief valves, it is necessary to make up the water inventory in the reactor vessel. If the pressure in the vessel is lower than the geodetical pressure in the flooding pool, the water can go by gravity flow via six supply lines and self-actuated check valves into the reactor vessel (Fig. 8). The flooding pool contains a water inventory of 3600 m^3. This volume of water is sufficient to fill the reactor pressure vessel and the drywell of the containment up to a level, which is equal to that in the flooding pool. This level is higher than the emergency condenser. The flooding pool guarantees because of this issues, firstly-the existence of a water-cover over pipe breaks at lower elevations inside and outside of the reactor pressure vessel, secondly-an effective cooling of the reactor vessel exterior and thirdly-the heat transfer by the emergency condenser. Even in case of LOCA on the heat transfer pipes of the emergency condencer we don't expect problems. This situation is comparable with a small leak in a safety-relief valve.

By an accident control without the using of active heat removal systems and only with the help of passive systems, the energy is accumulated in the containment and the temperature rises up. The containment cooling condenser (Fig.9) realized the heat transfer from the inside of the containment to the outside, into the water inventory of the steam dryer and steam-water separator storage pool. The condensate from the containment condenser returns into the flooding pool. This system works also without any active components. There are no valves in the lines. The containment condenser can be in operation more than three days before it will be any need for external interference. After this period it will be necessary to make up the water inventory of the steam dryer and steam-water separator storage pool.

The existence of non condensable hydrogen and nitrogen in the containment atmosphere and aerosols during several accidents was also taken into account for the design.

The first tests of the containment cooling condenser are going on now at the PANDA test facility in Switzerland.

This switching device, which operates without any interactions with I&C systems, initiates safety functions. The transmitter (Fig.10) is like a small heat exchanger and works similar to the emergency condenser. When the water level in the reactor pressure vessel is normal, the tubes inside the transmitter are filled with cold water and don't transfer heat. If the water level drops, steam comes into the transmitter and condensates. The transferred heat during this process causes the pressure on the shell side of the heat exchanger. This pressure-signal can be used to activate pilot valves, which in turn initiate the safety functions of reactor scram, containment isolation and reactor vessel depressurization.

During the tests the transmitter works properly. The main task of the actual tests is to promote the design's optimization in order to achieve a shorter erection time.

The described passive safety systems on Figure 11 in combination.

This passive safety systems are in operation with a reduced number of trains of proven active safety systems. Table III shows how the both kinds of safety systems achieve safety functions.

It is difficult now to forsee all the peculiarities of the cost-situation. But because of the far-reaching simplifications in the basic design, we can be sure, that the BWR 1000 will achieve the sufficient level of competitivness with the other power producing technologies. Table IV shows the simplification of the most important systems in comparison with a modern standard BWR, which are in operation in Germany now.

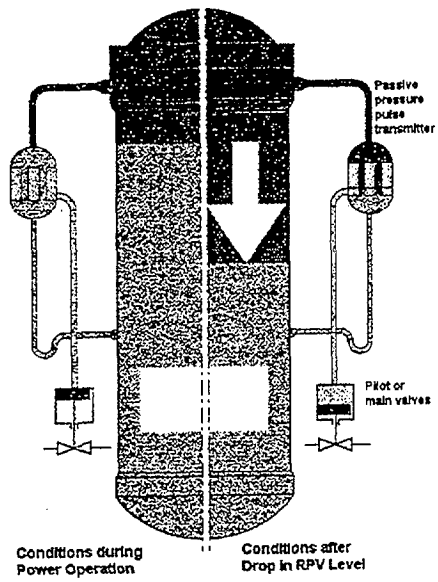
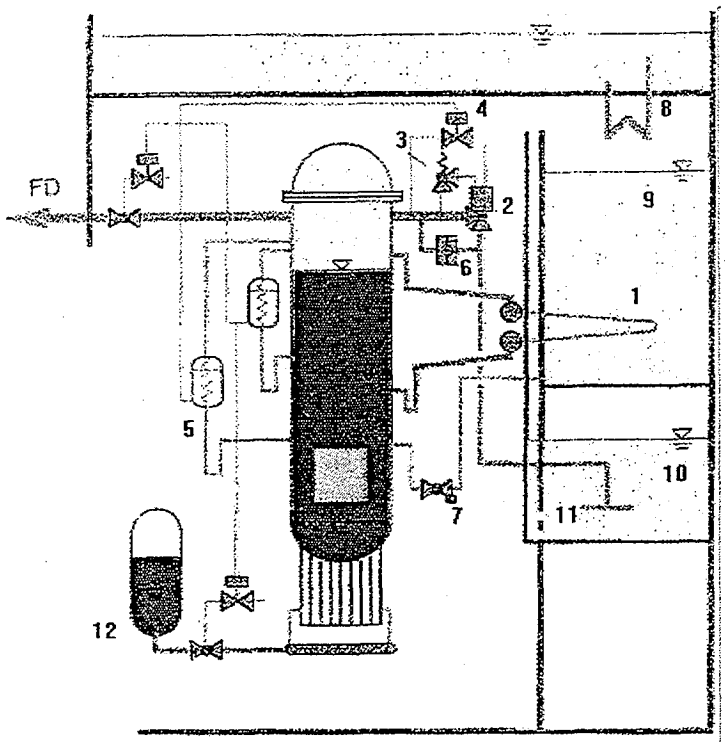


Figure 10 Passive pressure pulse transmitter.



1 Emergency condenser
2 Savety-relief valve
3 Spring-loaded pilot valve
4 Diaphragm pilot valve
5 Passive pulse transmitter
6 Rupture disk
7 Flooding line
8 Containment cooling condenser
9 Core flooding pool
10 Pressure suppression pool
11 Vent pipes
12 Scram system

Figure 11 Passive Safety System

Table III *Safety Functions of the Active and Passive Safety System*

<table>
<tr><th>Safety functions</th><th colspan="3">Active safety systems</th><th colspan="2">Passive safety systems</th></tr>
<tr><td>Reactivity control</td><td colspan="3">2 scram tanks
tripped by I&C</td><td colspan="2">tripped by passive pressure pulse transmitter</td></tr>
<tr><td></td><td colspan="3">high pressure boron injection by pumps tripped by I&C</td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3">Motor-actuated CRD tripped by I&C</td><td colspan="2"></td></tr>
<tr><td>Containment isolation (main steam line)</td><td colspan="3">3 Main steam line isolation valves per line
Solenoid pilot valves tripped by I&C</td><td colspan="2">Diaphragm pilot valves tripped by passive pressure pulse transmitter</td></tr>
<tr><td rowspan="2">Reactor pressure control</td><td colspan="5">8 Savety-relief valves</td></tr>
<tr><td>tripped by I&C</td><td rowspan="2">8 solenoid pilot valves</td><td>8 spring loaded pilot valves</td><td rowspan="2">8 rupture disks</td></tr>
<tr><td>Reactor depressurization</td><td>tripped by I&C</td><td>8 diaphr. pilot valves tripped by passive pressure pulse transmitter</td></tr>
<tr><td rowspan="2">Core cooling
- high pressure
- low pressure</td><td colspan="3"></td><td colspan="2">4 emergency condensers</td></tr>
<tr><td>low pressure core injection mode</td><td rowspan="2">2 residual heat removal systems</td><td colspan="2">6 flooding lines</td></tr>
<tr><td>Residual heat removal from containment</td><td>- low pressure core injection mode
- wet well cooling mode
- residual heat removal mode</td><td colspan="2">4 containment cooling condensers</td></tr>
</table>

Table IV *Comparison between the two BWR's Systems*

Systems	BWR today	BWR 1000
Heat removal system	3 trains for high pressure injection, 4 trains for low pressure injection and heat removal	2 trains for low pressure injection and heat removal, - Emergency condenser, - Containment cooling condenser, - Flooding pool
Cleaning systems	2 high pressure reactor water clean up systems, 2 trains for heat removal and water cleaning in the storage pools, 2 trains of gas exhausting systems	1 low pressure reactor water clean up system, 2 trains for heat removal in the storage pools, - mobil devices for water clean up in the storage pools, 1 train of gas exhausting system
Steam system	4 main steam lines, 1 auxiliary steam line, - steam lines for 2 preheater trains	3 main steam lines, - steam lines for 1 preheater train
Feedwater system	4/2 feedwater lines, 2 trains of preheaters, 3 x50% condensate- and feedwater pumps	2/1 feedwater lines, 1 train of preheaters, 2 x50% condensate- and feedwater pumps
Energy supply	6 emergency generators, - safety grade energy supply for 3 or more trains	2 emergency generators, - safety grade energy supply for 2 trains
Buildings		25 % lower volume

Conclusions

I have tried to show, how the passive and active systems together can be used for BWR 1000 and in what way it will be possible to achieve the appreciable simplification. These simplifications are visible not only in the systems themselves, but also have an impact towards the energy supply, I&C, auxiliary systems and the volume of buildings. In this way it will be possible to decrease enourmously the investment costs and the expenditure for maintenance in the whole.
The simplification is now urgent necessary from the point of high costs for the extensive development of safety systems in the NPP's, which are in operation today. From my point of view, provides BWR 1000 a interesting direction of development for increasing the safety level and probaly for decreasing the costs.

Reference

W. Brettschuh and K. Wagner, Germany's next generation of boiling water reactors. Kerntechnik 61 (1996) 5-6, p. 223-227

NEXT PAGE(S)
left BLANK

XA9848590

PLANT AVAILABILITY DESIGN ASPECTS OF KOREAN NEXT GENERATION REACTOR

WOO SANG LIM, HA CHUNG BAEK
Korean Electric Power Research Institute,
Taejun, Republic of Korea

Abstract

The purpose of this paper is to describe the KNGR design concepts adopted for reducing forced outages and refueling outages, and current design changes, to assess their availability impacts compared to existing domestic nuclear power plants, and then to identify design directions for next design stage.

1. INTRODUCTION

The KNGR project is aimed at providing the standard design of an advanced pressurized water reactor by 2001. The development consists of three phases. During the first phase from 1992 to 1994, the selection of preliminary design concepts was made and the top-tier design requirements were developed [1]. To ensure these top-tier design goals, the Center for Advanced Reactor Development (CARD) has organized the plant level analysis group which views the top levels of design verification such as safety, economics, constructability, performance, and radiation protection of the plant in the basic design stage (phase II). As one of the plant level analysis topics, the plant performance is assured in terms of power production capability (i.e. plant availability) through the RAM program.

The availability of future nuclear power plants is generally targeted to accomplish at least an 87% average during plant lifetime. The availability of existing Korean PWRs has shown an increasing trend since commercial operation of the first nuclear power plant, Kori Unit 1 and has been approaching 87% during past a few years as shown in FIG. 1 [2]. So the availability target of KNGR is established higher as 90%.

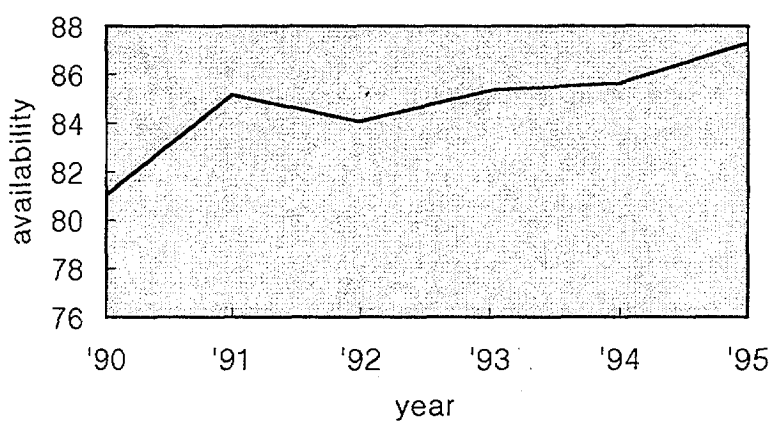


FIG. 1. Availability History of all Korean PWRs.

In order to achieve this target, it needs to improve design configuration and adopt new design feature. Overall plant availability is being assessed and its results are fed back into the design and reassessed. Availability assurance is implemented by repeating this process during the basic and the detail design stages. Each design stage has its unique feature to provide more input for availability assurance. These features are addressed in this paper.

2. FORCED OUTAGE

Forced outage is expected to be easier outage types than planned outage or extended outage type. Because existing domestic nuclear power plants have almost approached the KNGR targets during past a few years, which are;

- Trip frequency : less than 0.8 per year
- Forced outage: 2.4 days per year

2.1 Current design approach

At the basic design stage, the plant configuration is initially being settled to maximize availability, considering;

- design simplification
- amount of redundancy
- degree of diversity
- design of the support system infrastructure
- reliability and maintainability of individual components

Since the KNGR is being designed primarily based on the KSNP which has significant experience on the construction, startup and operation, it is expected to accomplish the forced outage targets. Therefore, the design is focused on the simplification to provide advantages to the economy of the KNGR by reducing the construction cost. Recent some design changes show these features well.

(a) Turbine building open cooling water system (TBOCWS)

The function of TBOCWS is to supply seawater to the turbine building closed cooling water system heat exchangers for heat removal. Seawater which is used as the source of cooling water and as a heat sink, is supplied by circulating water pumps in KNGR TBOCWS instead of TBOCW pumps as in KSNP. Thus, two 100%-capacity TBOCW pumps (TOP) are deleted compared to KSNP. This results in reducing plant unavailability as much as;

$$\Delta U = (\lambda_{TOP} \cdot \tau_{TOP})^2$$

where, λ is failure rate during a given period of time and τ is mean time to repair (MTTR).

Although the amount of the differential unavailability expected is not much large by itself, it contributes to increasing KNGR economics. Since it reduces construction and maintenance cost as well as unavailability.

(b) Main feedwater pumps

The FW system supplies feedwater from the deaerator storage tank to each of the two steam generators at the required pressure, temperature, and flow rate. The function of the system is to raise the pressure and temperature of the feedwater and to supply this preheated high-pressure water to the steam generators for conversion to steam. The system is also used to maintain proper water level in the steam generators during steady-state and transient operation.

The feedwater pump arrangement of KNGR consists of three parallel main feedwater pumps driven by variable speed steam turbine, and the parallel and identical feedwater booster pumps as shown in FIG. 2. A parallel startup feedwater pump is also provided for startup, shutdown and hot stand-by operation. All three main feedwater pumps are normally operating. The maximum capacity of each pump is 55% respectively.

The KSNP arrangement is two normally-operating pumps plus one spare pump. This arrangement also accomplish the objective of 100% power with one pump out and has the additional advantage that the pump can be run at their design point.

The KNGR arrangement requires the pumps to be run somewhat below their design point during normal three-pump operation so that the flow above design flow is not excessive during off-normal two-pump operation.

However, the KNGR arrangement, with three normally-operating pumps, is considered preferable because it provides a smoother transient following a pump trip and therefore lessens the risk of a plant trip.

The current KNGR main feedwater pump arrangement, furthermore, is being reviewed to study the feasibility of additional design change for improving reliability. One concept is to change pump drive type from steam turbine to adjustable speed motor (ASM) and the ASM driver is also used for driving main feedwater booster pump as shown in FIG. 3.

Considering that the maximum capacity of each main feedwater pump is 55%, equivalent unavailability is;

$$U(EQ) = U(100\%) + U(55\%)$$
$$= 3U_{LINE}^2 \times (1 - 0.55) + U_{LINE}^2 \times 0.55$$
$$U_{LINE} = \Sigma \lambda_i \cdot \tau_i$$

where, i is each component in one of three pump lines.

Since little operational data is available in the nuclear industry, quantification of above equation is possible by only a vendor's data at this time. Anyway, it is certainly a good design concept from an availability point of view that single ASM driver replaces two different types of drivers. So its adoption is soon to be decided after technical review on its reliability and maintainability together with some vendors.

If the ASM is adopted for KNGR, it is expected to bring another advantage. The concept is that main feedwater pump with the ASM driver can be used for startup instead of existing main feedwater startup pump.

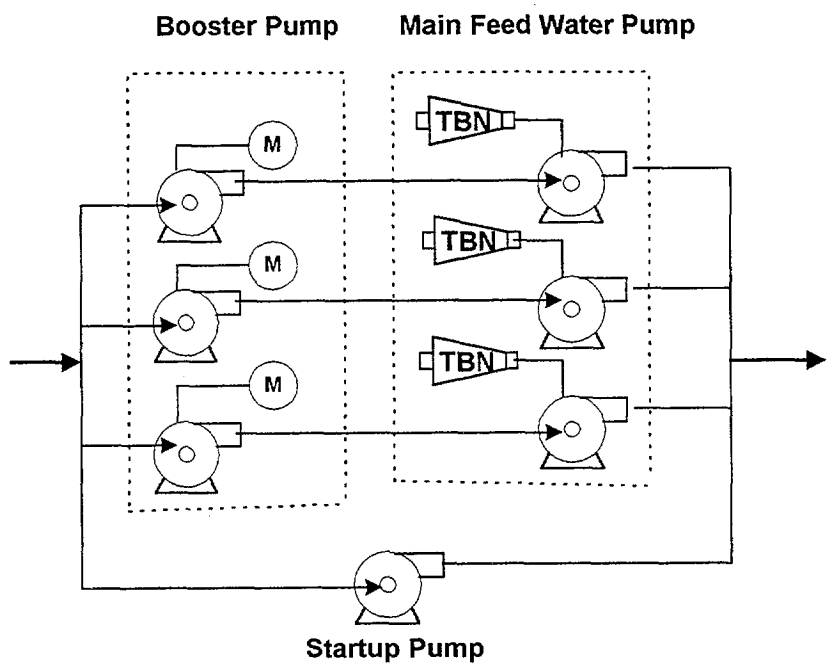


FIG. 2. Current Arrangement of Main Feedwater Pumps.

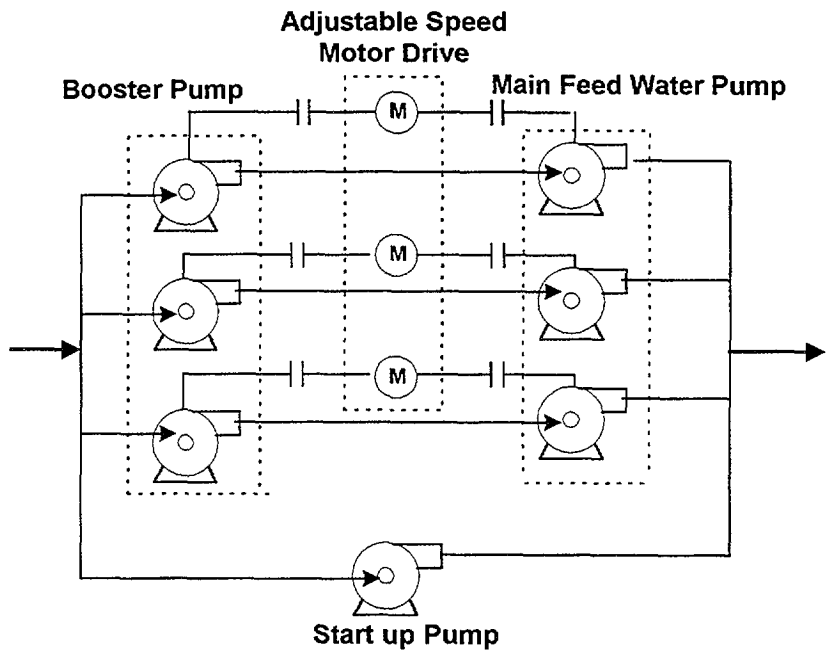


Fig. 3. New Arrangement of Main Feedwater Pumps.

2.2 Forced outage assessment

On the basis of the initial design configuration, forced outage is probabilistically assessed to identify significant systems and components. Although the assessment is not finalized at this time, it will be utilized to redesign systems, provide maintenance guidelines and implement the reliability centered maintenance (RCM).

FIG. 4 shows the work flow diagram for the analysis of unavailability caused by forced outages. The first step in the unavailability analysis is to collect plant operating experience

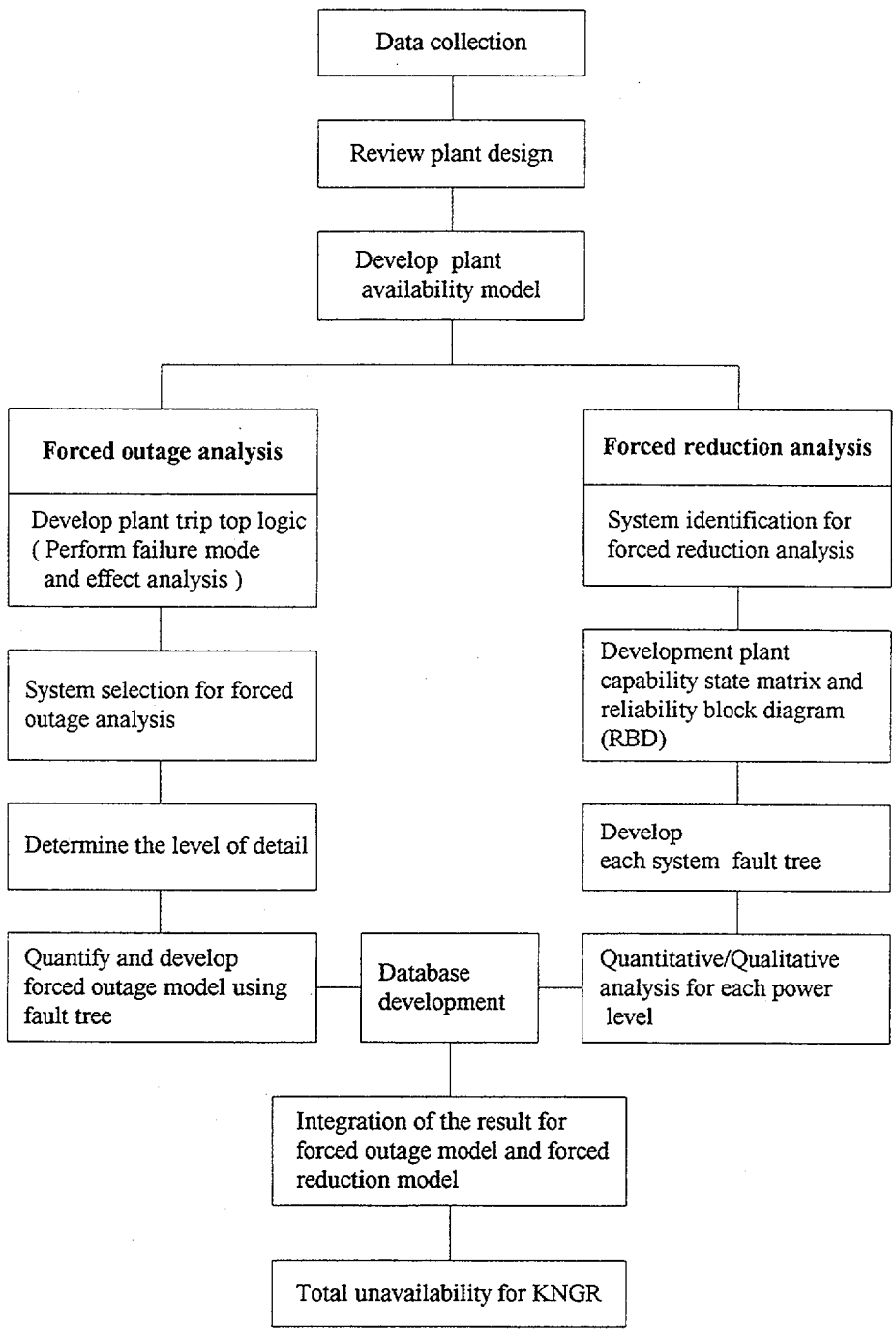


FIG. 4. Work Flow Diagram from Analysis of Unavailability Caused by Forced Outage for KNGR.

data. Since KNGR is not yet operating, however, the data are assessed based on Korean PWRs historical data and U.S. plant historical data. These data are used for producing the insights needed to predict its performance by which the level of modeling is determined.

The second step is to review the plant functional description and design documents for KNGR. At this step, the information needed, such as plant configuration, system function and operation, and the interface with other systems are reviewed. After this familiarization process, the plant availability model is developed. The plant availability model consists of two separate models, i.e., a forced outage model and a forced power reduction model.

To calculate total unavailability, these models are quantified by using the NUPRA computer code. The component failure data are used for the quantification of the plant availability model. The results quantified are represented as minimal cutsets along with their probabilities. And then the qualitative analysis is performed in order to check up to see if the results of the model are reasonable. The minimal cutsets from the availability model correspond to the component failure combinations which lead to a plant trip or a power reduction. These are ranked on the basis of their overall contribution to plant unavailability. Importance ranking of each systems and components which affects power production capability is measured in terms of Fussell-Vesely importance, Risk Reduction Worth and Risk Achievement Worth. The components of high importance thus identified need to be considered in detail.

The availability of KNGR is qualitatively checked with reference to Ulchin Unit 3 and 4, typical of Korean Standard Nuclear Power Plants (KSNP). Differences in design configurations are identified and the effects on plant availability are reviewed item by item. If a system is found to adversely affect plant availability, the system is redesigned depending on the results of the cost benefit analysis.

Some suggestions obtained from the evaluation results via each system analysis might lead to an availability improvement. These suggestions are then acceptable if they are easy to implement. After the effect on the overall KNGR availability is assessed, the suggestions are implemented and fed back into the analysis described in the previous section. This process is repeated until the target of the plant availability is met.

3. PLANNED OUTAGE

Planned outages, during which refueling and maintenance (R/M) is performed, is the most dominant factor to plant unavailability. Average planned outage duration for current nuclear power plants amounts to 47 days/unit · year, corresponding to 53 days per a planned outage during recent three-year period. Several action items have been identified to reduce planned outage duration for current domestic nuclear power plants, after the critical paths of the refueling and preventive maintenance work schedules had been analyzed in detail. Those action items shown below will be adopted in the KNGR design. As a result, outage duration is expected to be shortened about 5 days.

- Modulizing reactor head facilities
- Auxiliary crane for turbine maintenance
- Multi stud tensioner

3.1 Integrated head package (IHP)

It has been found that, prior to refueling in existing PWRs, the equipment on reactor vessel area has to be removed and temporarily stored before removing the reactor vessel head. This process has led to an increase the overall refueling time as well as the personal radiation exposure. An IHP is being designed to consolidate the following into an one-package component design: the head lifting rig; lift columns; missile shield; CEDM forced air cooling system; electrical and instrumentation cabling; insulation and reactor vessel head. The IHP lifts the reactor vessel closure head and the head area equipment at one time. Therefore, the amount of critical path time required to reach the reactor vessel internals can be reduced.

3.2 Additional design features

Furthermore, the KNGR will have advanced design features such as a permanent pool seal and a quick opening fuel transfer tube blind flange to reduce refueling work. A permanent pool seal is installed between the reactor pressure vessel and the surrounding refueling canal floor to permit flooding above the vessel during refueling. Since the leak-before-break concept is applied to the reactor coolant piping, the possibility of the local pressurization in the reactor cavity is eliminated. It becomes possible to permanently install the refueling pool cavity seal (termed as pool seal). Thus the need for assembling and disassembling temporary pool seals is eliminated.

The quick opening fuel transfer tube blind flange seals off the containment building transfer tube penetration sleeve during reactor operation. The current blind flanges are installed with bolts to be a part of the containment pressure boundary. Therefore, it takes long time to lift, and to temporarily store. The quick opening fuel transfer tube blind flange, however, can eliminate the need for lifting it from the area during refueling.

It is expected that these design features shorten refueling work as many as 2 ~ 3 days. So for the KNGR, it would take less than 45 days for refueling/maintenance (R/M) cycle per 18 months (i.e., 30 days/year). While current domestic nuclear power plants are operated with 12 ~ 18 month R/M cycle, KNGR is being designed to have a capability of operating on a 18 ~ 24 month fuel cycle, from post refueling startup to the subsequent post refueling startup as per EPRI URD [3].

4. EXTENDED OUTAGE

An extended outage is another type outage. Typical examples are;

- repair or replacement of large components
- manual trip resulted from unintended situation like steam generator tube leak

The current extended outage duration records as 2.3 day/unit · year during recent six years. Most of work performed during above extended outages is to repair major equipment such as generator, turbine, main transformer, reactor coolant pumps and so on. Kori Unit 1 has the 100 day schedule to replace steam generators (S/Gs) in 1998 including refueling and maintenance work. It is also assumed for KNGR that the S/G replacement can be performed in parallel with the refueling and maintenance outage. Assuming a 45-day R/M outage, the extension to the outage would be less than 55 days. Over the sixty-year period of the plant

lifetime, this results in an estimated contribution to plant unavailability of less than 1 day per year associated with steam generator replacement.

There are some design features to reduce outage time by reducing corrosion, which are;

- lower hot leg temperature
- Alloy 690 for SG tube material

Although the quantitative estimation of their effects are difficult, the extended outage target of KNGR is assigned conservatively as 5 days.

5. FUTURE AVAILABILITY APPROACH

5.1 Availability improvement during the detail design stage

Since the plant configuration is almost set up at this stage, component level availability improvement is required as follows;

- enhancement of maintainability to be ensured for important plant components and sub-systems during the plant construction and operation;

  - built-in testability
  - on-line diagnostic and fault detection systems
  - repairability
  - replaceability

- development of procurement requirements for critical components (purchase for reliability and maintainability levels which are commensurate with their importance to reliability)

- use of maintenance simulation of R/M outages to identify critical path components whose periodic maintenance schedule can be changed (procurement specs) to minimize impact, or, whose maintenance schedule can be shifted from refueling to "at power" or "on-line"

5.2 Availability assurance through the RAP

Reliability assurance originated with the regulatory concern SECY-89-013 dated January 1989 where "Reliability Assurance Program (RAP)" was defined as a program to ensure that the design reliability of safety SSC is maintained over the life of a plant. Based on this document, ALWR designers have been setting up their own assurance program to ensure that their own systems meet all required safety regulations and requirements. Since it was considered that plant availability goals were generally beyond the purview of the regulatory bodies in their states, the vendors have been developing their own procedures which focus on achieving an economically competitive position and satisfying customer needs.

The EPRI URD requires D-RAP to ensure that sufficient plant reliability is designed into the plant to achieve overall availability goals, as well as to assure design reliability of structures,

systems, and components whose reliability has a significant effect on core damage frequency. However, it does not detail how a reliability assurance program can be implemented throughout each stage of plant development, design, construction and operation, nor does it provide an integrated approach to incorporation of reliability and maintainability engineering in all aspects of plant decision making.

The Reliability Assurance Program which will be employed throughout design and operation of the KNGR is currently under development. Availability assurance will be continued through this RAP until the end of the commercial operation.

6. CONCLUSION

The unavailability caused from forced outages, planned outages and extended outages is assessed at the conceptual design stage to identify availability significant systems and components. As design progresses forward into detail, the assessment is also revised to reflect it. The plant availability will be ensured through RAP during all the phases of design, procurement, construction, startup, and commercial operation.

Above all things, planned outage time has to be shortened in order to improve the plant availability. It has been found that only the reduced refueling time can not reduce overall planned outage. Because turbine and generator maintenance process is of the critical path together with refueling process. Therefore, most of work will be concentrated to turbine and generator maintenance during the detail design stage to accomplish the KNGR availability target.

REFERENCES

[1] KOREA ELECTRIC POWER CORPORATION, Top Tier Design Requirements of the Next Generation Nuclear Power Plant, Korea(1994).
[2] KEPCO, Annual Report for Nuclear Power Plant Operation, Korea(1996).
[3] ELECTRIC POWER RESEARCH INSTITUTE, Advanced Light Water Reactor Utility Requirements Document, Volume II ALWR Evolutionary Plant, U.S.A(1992)

NEXT PAGE(S) left BLANK

XA9848591

ADVANCED DIGITAL TECHNOLOGY — IMPROVING NUCLEAR POWER PLANT PERFORMANCE THROUGH MAINTAINABILITY

J.L. FORD, R.R. SENECHAL, G.D. ALTENHEIN, R.P. HARVEY
ABB Combustion Engineering Nuclear Systems,
Windsor, Connecticut, United States of America

Abstract

In today's energy sector there is ever increasing pressure on utilities to operate power plants at high capacity factors. To ensure nuclear power is competitive into the next century, it is imperative that strategic design improvements be made to enhance the performance of nuclear power plants. There are a number of factors that affect a nuclear power plant's performance; lifetime maintenance is one of the major contributors. The maturing of digital technology has afforded ABB the opportunity to make significant design improvements in the area of maintainability. In keeping with ABB's evolutionary advanced nuclear plant design approach, digital technology has systematically been incorporated into the control and protection systems of the most recent Korean nuclear units in operation and under construction. One example of this was the multi-functional design team approach that was utilized for the development of ABB's Digital Plant Protection System (DPPS) The design team consisted of engineers, maintenance technicians, procurement specialists and manufacturing personnel in order to provide a complete perspective on all facets of the design. The governing design goals of increased reliability and safety, simplicity of design, use of off-the-shelf products and reduced need for periodic surveillance testing were met with the selection of proven ABB-Advant® Programmable Logic Controllers (PLCs) as the heart of the DPPS. The application of digital PLC technology allows operation for extended periods without requiring routine maintenance or re-calibration. A well documented commercial dedication program approved by the United States Nuclear Regulatory Commission (US NRC) as part of the System 80+™ Advanced Light Water Reactor Design Certification Program, allowed the use of off-the shelf products in the design of the safety protection system. In addition, a number of mechanical and electrical improvements were made which support maintainability. The result is a DPPS that has been re-designed to take full advantage of the many benefits associated with digital technology. The new design places emphasis on ease of maintenance in order to reduce operating and maintenance costs, allow greater plant availability and, ultimately, improve plant performance.

1. SYSTEM DESCRIPTION

The Plant Protection System is one of the most important systems in a nuclear power plant. Its job is to monitor the plant to ensure it is operating within safety limits. The DPPS does this by receiving inputs from critical plant sensors in the field. It monitors these inputs and compares them to the specified safety limits. If the DPPS detects that these limits are exceeded, it generates signals which initiate a plant trip and actuation of other safety features as required. Built into the DPPS is redundancy where four independent channels monitor each safety limit. Protection functions are initiated when two-out-of-four channels detect an unsafe plant condition.

The DPPS is comprised of bistable processors, local coincidence logic processors, initiation logic, and interface and test processors. Plant limits are compared by the bistable processors while the two-out-of-four trip limit coincidence logic is performed by the local

coincidence logic processors. Initiation logic provides the interface to the actuated systems and accommodates hard wired manual initiation capability downstream of the programmable logic. Interface and test processors perform system monitoring and test functions.

2. DESIGN APPROACH

Historically, nuclear power plant protection systems have been designed with electro-mechanical relays and/or solid state electronics. Systems of this type, although highly reliable, typically require extensive periodic testing and maintenance. Spurious plant trips and extended outages due to the need for system maintenance can have an adverse effect on plant performance. In response, there has been an increased awareness in the nuclear industry of the need for improving the maintainability of power plants. ABB took advantage of the opportunity to design for improved reliability and maintainability when it initiated a program to digitize the existing analog Plant Protection System (PPS). The re-designed DPPS is significantly less susceptible to these maintenance issues and therefore contributes to improved plant performance.

2.1 Design Team

A multi-functional design team was assembled which consisted of design engineers, manufacturing engineers, startup engineers, maintenance technicians and procurement specialists. The diversity of the team was instrumental in identifying areas for improved maintenance based on actual operating experience with the previous PPS designs.The team was fully empowered to make design and product selection decisions.

The DPPS design was to remain functionally the same as the System 80® analog relay PPS design, but was to take full advantage of the benefits such as high reliability and system accuracy offered by the incorporation of modern digital technology. The governing design goals for the DPPS project embodied ease of maintenance and increased plant availability. The specific goals were:

- provide for increased reliability and safety over analog systems;
- strive for simplicity of design using proven, off-the-shelf products; and
- reduce the amount of periodic surveillance testing required.

2.2 Maintainability Defined

Before addressing an issue such as maintainability, it was first necessary to define it in concrete terms that were understandable to the design team. Based on the types of activities performed during plant operation, plant outages, and the random occurrence of plant trips, the concept of maintainability was defined in two parts:

(1) the amount and frequency of required periodic maintenance, and

(2) the ease at which periodic maintenance can be performed.

By this definition, the ideal system would be one in which the need for periodic maintenance was minimal, and when necessary, was quickly performed with ease. This two part definition was the basis for the advanced design improvements made on the DPPS.

3. DIGITAL TECHNOLOGY ALLOWS A SIMPLER DESIGN WITH FEWER PARTS

An essential ingredient in anything that is designed for maintainability is simplicity. In striving for simplicity, fewer parts are better. Because the DPPS incorporates a modular design, component types were able to be standardized resulting in few unique parts.This attribute provides multiple benefits including:

- Equipment Familiarity - Personnel who work with and perform maintenance on the DPPS are more familiar with the makeup of the system. There are fewer parts that need unique maintenance procedures and less time is required to perform routine service and system checks.

- Reduced Spares Inventory - The need to stock numerous parts for use in the event of component failure is greatly reduced. The standardized design allows interchanging of hardware.

- Fewer Equipment Suppliers - Procurement is made easier by dealing with fewer equipment suppliers since there are fewer equipment supplier qualification and QA programs to review and fewer files to maintain.

3.1 Product Selection

Critical to achieving the goal of simplicity was the selection of the proper technology and products. Product selection was focused on finding a cost-effective replacement platform based on new technology which offered the added benefits of improved functionality, reliability and maintainability. After a comprehensive evaluation program was completed, the ABB-Advant® Programmable Logic Controller (PLC) was selected as the technology of choice for the "heart" of the DPPS. The ABB-Advant PLC was chosen in part due to its high reliability and use in nuclear applications worldwide. Versatility and ease of programming added to the long list of positives for the ABB-Advant PLC. In keeping with the design goal of off-the-shelf products, the ABB-Advant PLC was subject to an extensive verification phase prior to acceptance as a "Dedicated Commercial Grade Item" to be used in safety-related applications. Although the product selection process implemented by the design team was used for the selection of all components in the system, the PLC had the greatest impact on the simplicity of the design by replacing numerous electro-mechanical relays.

PLCs have an excellent reputation as being very reliable and simple to maintain which is supported by their extensive use in critical control and safety function applications in the petrochemical, pharmaceutical and fossil power industries. PLCs are capable of extended operation without the need for periodic maintenance or calibration. Use of PLC technology eliminates the custom made analog PC boards and the majority of the electro-mechanical relays associated with analog PPS systems. All of the relays associated with performing logic functions have been replaced by PLCs. Nine electro-mechanical relays still exist in the system. These nine remaining relays are off-the-shelf, commercially dedicated parts which are used as interposing devices. The elimination of the majority of electro-mechanical relays is a large contributor to reducing the overall number of parts in the DPPS by a factor of ten over the previous analog design. This reduction in parts means that fewer spares are required to be kept in inventory. Because all parts in the system are off-the-shelf, it is no longer necessary to be highly dependent on custom replacement parts and their associated long lead times. Off-the-shelf parts offer high availability as well as a reduced likelihood of equipment obsolescence.

Adding to the product selection decision is the ABB-Advant PLCs hardware and software upward compatibility. This means that as new hardware and/or software is developed, it will be

compatible with the hardware and software that is utilized in the DPPS today. This is a major improvement to a situation that has historically rendered digital equipment platforms obsolete and has resulted in significant replacement costs.

3.2 Reduced Number of Power Supplies

It is typical for analog systems to require many different power types whereas digital systems can be configured to run on very few. ABB took advantage of the fact that digital systems are less power dependent than analog systems and used it to simplify the DPPS. All equipment in the DPPS is designed to operate at a common 24 VDC voltage. As a result, there are only two redundant power supply pairs in each channel of the DPPS; one pair of redundant Input/Output (I/O) external power and one pair of redundant internal equipment power. This improved configuration replaces the thirty power supplies with various voltages and currents in each channel of the older analog PPS system.

3.3 Reduced Cabling

Digital design is conducive to the usage of fiber optics. The DPPS utilizes fiber optics for transmission and isolation of signals that are required to pass between safety channels. Fiber optic isolation replaces the complex relays and multiple fuse isolation of the older analog PPS design. Fiber optics improve the isolation protection of the DPPS while reducing the quantity of equipment that is needed to perform this function. Additionally, the use of fiber optic isolation cables results in an overall reduction in the required amount of internal cabinet cabling from more than 1000 hard wires to approximately twenty four fiber optic cables.

4.0 DIGITAL TECHNOLOGY INCREASES THE TIME BETWEEN REQUIRED MAINTENANCE

ABB's first definition of maintainability; the amount and frequency of required periodic maintenance, is directly impacted by how reliable the system is. The design improvements discussed in this section all contribute to the reliability of the DPPS.

4.1 Software Development

ABB has a long and successful history developing high quality software for the nuclear industry. In 1978, ABB delivered the world's first safety grade software to the Arkansas Nuclear One Generating Station Unit 2, and since then has been involved in numerous software development projects. It is this extensive experience which provides the basis for the software development program on the DPPS.

Because PLCs are software based, they are capable of extended operation without the need for periodic maintenance or calibration. Trip setpoint limits on the DPPS are no longer set mechanically, but are now accomplished by digital software code. Built in automatic tests and diagnostics are also performed by software. Well-designed software can be expected to run indefinitely without the likelihood of failure. In order to assure that the DPPS software is designed with a high degree of quality and reliability, an extensive verification and validation program exists.

ABB has made significant progress defining the codes, standards and regulatory guides required to address the software design and qualification process. The software design,

development, verification and validation process for the DPPS was performed in accordance with ABB's Quality Program Instructions [1] and Software Program Manual for ABB's Advanced Control Complex, Nuplex 80+ [2]. This software program approach was developed by ABB in accordance with industry standards and approved by the USNRC during the licensing of System 80+™. The program includes phases for requirements, design, implementation, testing and installation and checkout, operations and maintenance, and retirement.

4.2 Digital Setpoints

One of the major differences between analog systems and digital systems is how setpoints are programmed. Analog systems rely on mechanical potentiometers which convert a particular setting into corresponding voltage values. These voltage values are prone to "drift" which must be compensated for in order not to exceed regulatory safety limits. Digital systems allow the operator to program in a value which does not change. No longer is it necessary to routinely verify and re-calibrate setpoints monthly as was the case with analog systems. The elimination of these operations increases plant availability due to unnecessary, spurious trips resulting from human error. Digitally programmed setpoints also increase system accuracy and improve the margin to trip. The ABB Advant PLC analog-to-digital (A/D) conversion is self-checking, thus the calibration verification interval is extended from every month in the old analog PPS design to once every refueling outage (i.e., 12 - 24 months).

4.3 On-Line Diagnostics and Test

The DPPS design includes a comprehensive on-line diagnostics and test program which automatically provides health status monitoring on a system as well as component level. At the system level, the automatic testing programs test both the hardware and the software greatly reducing the time needed to perform NRC required surveillance testing of the DPPS. This on-line testing also identifies random hardware failures which previously went undetected between normally scheduled outages and tests. The diagnostics program can identify failures at a module level. If a failure were detected and the system was brought off-line for maintenance, an extensive diagnostic search would not be necessary because the problem would already be categorized. This process improvement results in a typical Mean Time To Repair (MTTR) of less than 30 minutes. Reducing the amount of manual troubleshooting performed reduces the potential for human error which can be the cause of spurious trips.

4.4 Redundant Power Supplies

The fully redundant 24VDC power supplies also add to the DPPS's reliability in that any single power failure will not result in the loss of the DPPS operation. "Hot Swap" capability, the ability to change out components without the need to take the system off-line, was provided for the power supplies further increasing channel availability. The decision to use the 24VDC power supplies also supported the DPPS's total design against Electro-Mechanical Interference and Radio Frequency Interference (EMI/RFI).

4.5 Early Warning Features

Other design features that contribute to the reliability of the DPPS are built in cabinet temperature and smoke detectors. The cabinet temperature detectors monitor the environment inside the cabinet and provide alarms to the operators. The setpoint for these temperature detectors is such that a high temperature alarm is provided before equipment availability would be affected. Each channel of the DPPS is outfitted with its own smoke detector that provides

input to the fire protection system in the plant. Both of these design features add to the maintainability of the system by providing early warning of potentially serious problems.

5. DIGITAL TECHNOLOGY MAKES MAINTENANCE EASIER

ABB's second definition of maintainability - the ease at which periodic maintenance can be performed, is a more tangible subject. There are a number of design improvements in the DPPS which decrease the mean time to repair and reduce the amount of down time for the system.

5.1 PLC Rack Design

Digital technology has allowed the DPPS to accommodate future expansion of system capabilities if the need arises. The racks (backplanes) which mount the required PLC modules have spare capacity beyond that which is necessary to operate the system. Until the empty PLC slots are used, a full complement of "dummy" modules are incorporated into the design as place holders. Having the entire rack full provides additional structural strength and also prevents replacement of a module in the wrong location after performing maintenance. In the event an incorrect type PLC module were inadvertently installed in a rack during maintenance, the built in software diagnostics would provide automatic error notification.

Further adding to the structural integrity of the PLC rack is a patented seismic support bracket designed to hold the PLC modules in place. For ease of maintenance, the seismic support bracket requires no tools to remove. Additionally, all loose parts are attached to lanyards to prevent loss within the cabinet.

The ABB-Advant® PLC module and rack design are perfectly suited to "hot swapping" in that the modules are back plane hinged into the rack so that they can be "hot-swapped" without power spiking of the modules. This is made possible by the fact that power is not introduced to the module until it is screwed in. In addition, the module design allows the replacement of failed modules without the removal of terminated wires. The edge connector is able to be disconnected from the PLC module in one piece. This process helps avoid any potential rewiring errors.

5.2 Four Channel Methodology

ABB has always incorporated a four channel methodology into the design of all plant protection systems. The DPPS is no different in this respect. All four channels monitor the plant for operation within specified safety limits. A two-out-of-four coincidence logic is employed to send actuation signals to the safety features systems. The decision to incorporate four channels was made with maintainability in mind. US NRC regulations require that nuclear plant safety systems be single failure proof. ABB's two-out-of-four logic not only allows one channel to fail but additionally allows one channel to be bypassed during plant operation for testing or replacement and still satisfy regulatory requirements.

5.3 Cabinet Arrangement

Some simple design improvements have been made to the cabinet arrangement of the DPPS. Power distribution terminal block strips on the DPPS are all located next to their respective PLC I/O racks for ease of maintenance and operator familiarity. These terminal blocks have also been color coded for quick identification of the power circuit's polarity.

The DPPS cabinet has been designed to be immune from the effects of the EMI/RFI present in a nuclear power plant application. The doors have been gasketed, there are no sharp edges, the flanges on the cabinet are outwardly curving, and EMI filters have been installed.

5.4 Blown Fuse Indication

Sometimes even the simplest design improvements are the most effective. The time spent attempting to diagnose a system problem has often taken hours with prior systems when it may have been as simple as a blown fuse. ABB has incorporated L.E.D. blown fuse indicators on all the fuses in the DPPS. With this feature, any blown fuse can be identified by a red light which is located in plain sight on the inside of the cabinet. This may allow the operator to quickly and easily correct the problem or at least will have led him to the problem circuit.

5.5 Reduced Risk of Electrical Shock

The move to digital technology allowed the use of 24VDC for all components and wiring in the cabinet. The result is a greatly reduced threat of electrical shock to personnel while performing maintenance activities on the DPPS. This is a human factors engineering improvement which makes maintenance safer and more efficient

6. CONCLUSION

The advanced design features made possible by the migration to digital technology in the DPPS have resulted in a number of improvements in the area of maintainability. The DPPS is proof positive that with proper planning, simple maintainable designs are possible. The nuclear industry can benefit from the lessons learned in ABB's digitization of the plant protection system. The DPPS has been designed to:

- Provide high reliability
- Require less periodic surveillance testing
- Reduce the incidence of random, undetected failures
- Reduce the spares inventory
- Simplify maintenance
- Increase personnel safety
- Attain higher system accuracy
- Improve the margin to trip
- Improve plant performance

The DPPS will be first deployed to an operating nuclear power plant as part of the Oskershamm 1 modernization in Sweden. This application will be followed shortly thereafter by the initial startups of Ulchin Units 5 and 6 in the Republic of Korea.

REFERENCES

[1] ABB's Quality Program Instructions, QPM-1.1

[2] Software Program Manual for ABB's Advanced Control Complex, Nuplex 80+, NPX80-SQP-0101.0

NEXT PAGE(S) left BLANK

XA9848592

THE DESIGN RELIABILITY ASSURANCE PROGRAM FOR THE WESTINGHOUSE AP600 REACTOR

M.H. CANTON
Westinghouse Electric Corporation,
Pittsburgh, Pennsylvania, United States of America

Abstract

The mission of the Westinghouse AP600 is to provide a safe, simple, standardized and economically competitive design with a high degree of operability and ease of maintenance. To meet these goals, the AP600 Reliability, Availability and Maintainability program (RAM) and Design Reliability Assurance Program (D-RAP) were established. These programs, from the outset of the design process, systematically identified the safety and availability goals of the plant, defined the associated performance goals of the plant's critical systems, and provided insights to the design process to improve component reliability. The result is a documented list of risk-significant and availability-significant structures, systems and components (SSCs) whose reliability values must be established during manufacture and maintained throughout the life of the plant.

1. INTRODUCTION

The Westinghouse AP600 is an advanced 2-loop nuclear power electrical generating station design with passive safety features. It has been designed to meet the EPRI Utility Requirements Document (URD) [1], which establishes standards for safety, availability and maintainability for advanced passive and evolutionary plants. The AP600 features passive emergency reactor core cooling, canned motor reactor coolant pumps that eliminate pump seals and increase reliability, and digital instrumentation and control in proven applications.

The AP600 draws upon the operating experience of and lessons learned from the utility community via design workshops and design review interaction, as well as operating plant data from utility and Westinghouse-maintained databases.

2. OVERVIEW OF RAM AND D-RAP

From the early stages of the design, the AP600 program has executed a comprehensive RAM program that focuses on the assessment and improvement of plant availability. This program was developed in accordance with MIL STDs 785B [2] and 470A [3]. Parallel to this effort, a Probabilistic Risk Assessment (PRA) [4] was submitted to the NRC with the Standard Safety Analysis Report (SSAR) [5] in 1992. The RAM and PRA efforts have shared failure information and historical data, but have been deliberately kept separate to ensure that safety was not compromised by the availability goals.

The Design Reliability Assurance Program (D-RAP), as defined by the URD, considers both the safety and the availability of the AP600. However, the D-RAP objectives of the NRC, as guided by Reference 6, focus on safety. Westinghouse has produced separate D-RAP plans/programs to satisfy both guidelines. This paper focuses upon on the D-RAP that meets the NRC requirements, as well as on the RAM program that emphasizes plant availability.

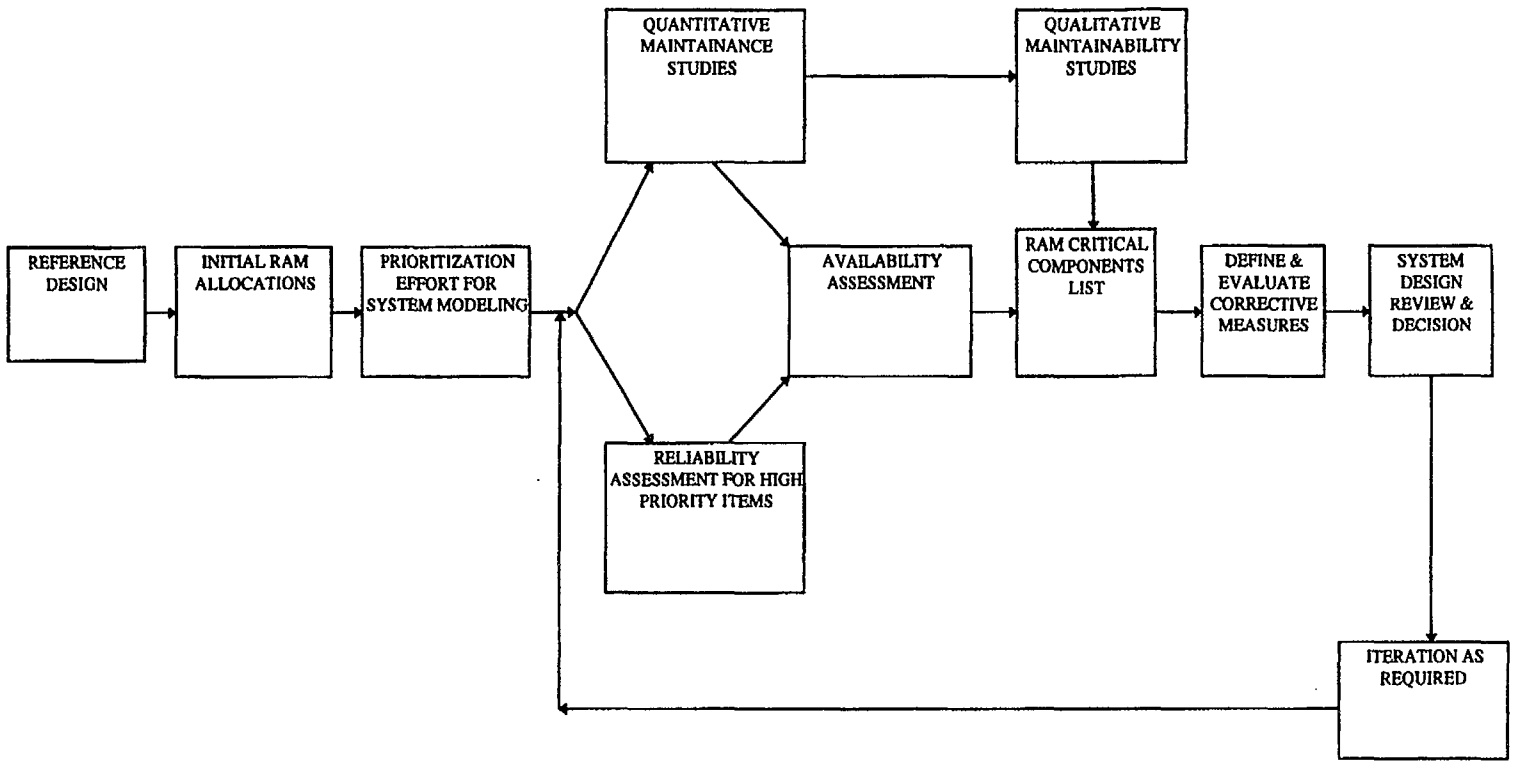


Figure 1. AP600 RAM Program

3. AP600 RAM PROGRAM

The AP600 Reliability, Availability and Maintainability Program was instituted early in the design process. Its overall mission was to achieve a design capable of 90% availability as well as increased operability and maintainability. Three objectives were pursued:

1) to lead the design evolution process toward meeting the RAM performance objectives through independent verification of the RAM characteristics of the reference design and evaluation of proposed design changes.

2) to provide periodic assessments of program progress toward meeting plant RAM requirements, permitting the AP600 project to effectively allocate resources.

3) to support the AP600 test, PRA and Design Certification activities. PRA studies were conducted with inputs from the RAM program to confirm that the design meets public safety and investor protection objectives. The extensive test program utilized information from the RAM program:

   - large-scale containment cooling tests
   - automatic depressurization system test
   - full-height, full-pressure integral system test
   - low-pressure integral system test
   - core makeup tank test

Figure 1 is a flowchart of the program.

The reference design represents the first iteration of the design. It is a combination of the best features from existing designs with the new, improved features unique to the AP600. Utilizing the RAM database, which documents utility experience to identify failure mechanisms, an initial RAM system-by-system allocation evaluation is performed. This list estimates and ranks system contributions to plant unavailability based upon historical experience of similar (Westinghouse 2-loop) plants as well as deterministic evaluation of new design information. An example of the list is provided in Table I.

For the systems determined to contribute most to plant unavailability, detailed availability analyses are performed to refine the estimates and to identify critical components within those systems. An example critical component list is provided in Table II. The primary tools used in this process are fault tree modeling, FMECAs, quantitative maintenance studies and quantitative estimates of plant, system and component failure rates. As potential design improvements are identified by these analyses, they are considered for implementation based upon cost/benefit, ease of implementation and perceived need to improve the plant in that area. The impacts of the implemented changes are fed back into the availability tally. This iteration process is continued until the plant availability goal is estimated to be achieved. Over a six-year period, the availability estimate for the AP600 plant has improved from 88.6% to 90.6% using conservative evaluations and assumptions. A large fraction of the increase is due to improvements in the refueling and maintenance outage times.

4. AP600 D-RAP

The Design Reliability Assurance program was developed to provide confidence that the reliability assumptions made as part of the PRA remain valid throughout plant life. It follows the guidance of Reference 6. Originally, one intention of the program was to combine results of both the availability and safety analyses to generate a joint list of critical SSCs for consideration in design, operation and maintenance. Through NRC direction and due to practical issues regarding

TABLE I. AP600 UNAVAILABILITY ESTIMATES AND ALLOCATIONS FOR AP600 SYSTEMS (EXAMPLE)

SYSTEM	HISTORIC 3/4 LOOPS DOWNTIME (1980-89) (hrs/yr)	HISTORIC 3/4 LOOPS DOWNTIME (1986-89) (hrs/yr)	HISTORIC 2 LOOPS DOWNTIME (COD-89) (hrs/yr)	ALLOCATED AP600 DOWNTIME GOALS (hrs/yr)	AP600 ESTIMATE (hrs/yr)
REACTOR COOLANT SYSTEM					
- Reactor Coolant Pumps	48.1	26.4	26.3	8.0	10.5
- Steam Generators	171.2	77.7	144.9	70.0	47.3
- Other RCS Components	86.7	82.5	24.1	20.0	14.3
TOTAL RCS	306.0	186.6	195.3	98.0	72.1
CORE INTERNALS	0.0	0.0	0.0	0.0	0.0
CONTROL ROD DRIVE MECHANISMS	10.4	16.6	0.5	0.0	0.0
PASSIVE CORE COOLING SYSTEM (ECCS of operating plants)	40.6	41.9	9.7	8.0	10.3
CHEMICAL & VOLUME CONTROL SYSTEM	11.3	15.8	4.8	1.4	2.04
CONTAINMENT COOLING AND PURIFICATION SYSTEM	28.4	12.6	1.0	0.0	0.0
SERVICE WATER SYSTEM	4.5	3.1	0.0	1.5	1.5
COMPONENT COOLING WATER SYSTEM	9.6	6.8	0.3	1.5	1.5
WASTE PROCESSING SYSTEM					
- Liquid Waste Processing	0.0	0.0	0.0	0.0	0.0
- Solid Waste Processing	0.0	0.0	0.0	0.0	0.0
- Gaseous Waste Processing	0.0	0.0	0.0	0.0	0.0
TOTAL WPS	0.0	0.0	0.0	0.0	0.0
INTEGRATED PROTECTION SYSTEM	13.6	17.0	6.2	3.0	5.0
INTEGRATED CONTROL SYSTEM	12.1	11.5	4.8	2.0	2.5
INCORE INSTRUMENTATION SYSTEM	2.7	0.5	0.9	1.0	1.0
STEAM GENERATOR SYSTEM	38.7	33.7	35.0	8.0	16.6
MAIN STEAM SYSTEM	18.3	18.5	3.8	2.0	3.4
MAIN & STARTUP FEEDWATER SYSTEM	40.7	33.6	10.9	2.0	0.14
HEATER DRAIN SYSTEM	3.6	4.8	1.6	1.6	1.6
MAIN CONDENSATE SYSTEM	26.4	27.5	5.3	2.5	0.44
CIRCULATING WATER SYSTEM	13.2	9.8	0.9	0.9	0.9

TABLE II. AP600 CRITICAL COMPONENT LIST (EXAMPLE)

COMP NO.	EQUIPMENT NAME	COMP. FAIL. RATE (hrs/yr)	COMP. FAIL RATE GOAL (hrs/yr)
1	Main Turbine	56.6	50.0
2	Steam Generator A	23.65	35.0
3	Steam Generator B	23.65	35.0
4	Main Step-up Transformer	4.6	5.0
5	Main Feed Reg Valve-A & Valvop	4.17	2.0
6	Main Feed Reg Valve-B & Valvop	4.17	2.0
7	Main Generator/Exciter/Voltage Reg	3.20	2.0
8	Pressurizer Spray Valve-A & Valvop	2.74	2.7
9	Pressurizer Spray Valve-B & Valvop	2.74	2.7
10	Reactor Coolant Pump	2.62	2.0
11	Reactor Coolant Pump	2.62	2.0
12	Reactor Coolant Pump	2.62	2.0
13	Reactor Coolant Pump	2.62	2.0
14	Main Steam Isol Valve-A & Valvop	2.43	1.0
15	Main Steam Isol Valve-B & Valvop	2.43	1.0
16	Pressurizer Code Safety A	2.28	2.3
17	Pressurizer Code Safety B	2.28	2.3
18	Pressurizer	2.16	2.2
19	PRHR Actuation Valve-A (Air)	1.79	1.7
20	PRHR Actuation Valve-B (Air)	1.79	1.7
21	Reactor Vessel	1.40	1.4
22	PRHR Heat Exchanger	1.12	1.1
23	Extraction Steam Piping	1.06	1.0

prioritization of SSCs, the D-RAP was refocused exclusively upon safety considerations. Specifically, the following goals were established:

Provide reasonable assurance that

- the AP600 is designed, procured, constructed, maintained and operated in a manner consistent with the PRA assumptions and risk insights for the risk-significant SSCs
- the risk-significant SSCs do not degrade to an unacceptable level during plant operations

- the frequency of transients that challenge the AP600 risk-significant SSCs are minimized
- the risk-significant SSCs function reliably when they are challenged
- a mechanism is provided for establishing baseline reliability values for implementation of the NRC Maintenance Rule [7].
- design and operational information is available to be used by the combined license applicant for ongoing plant reliability assurance activities

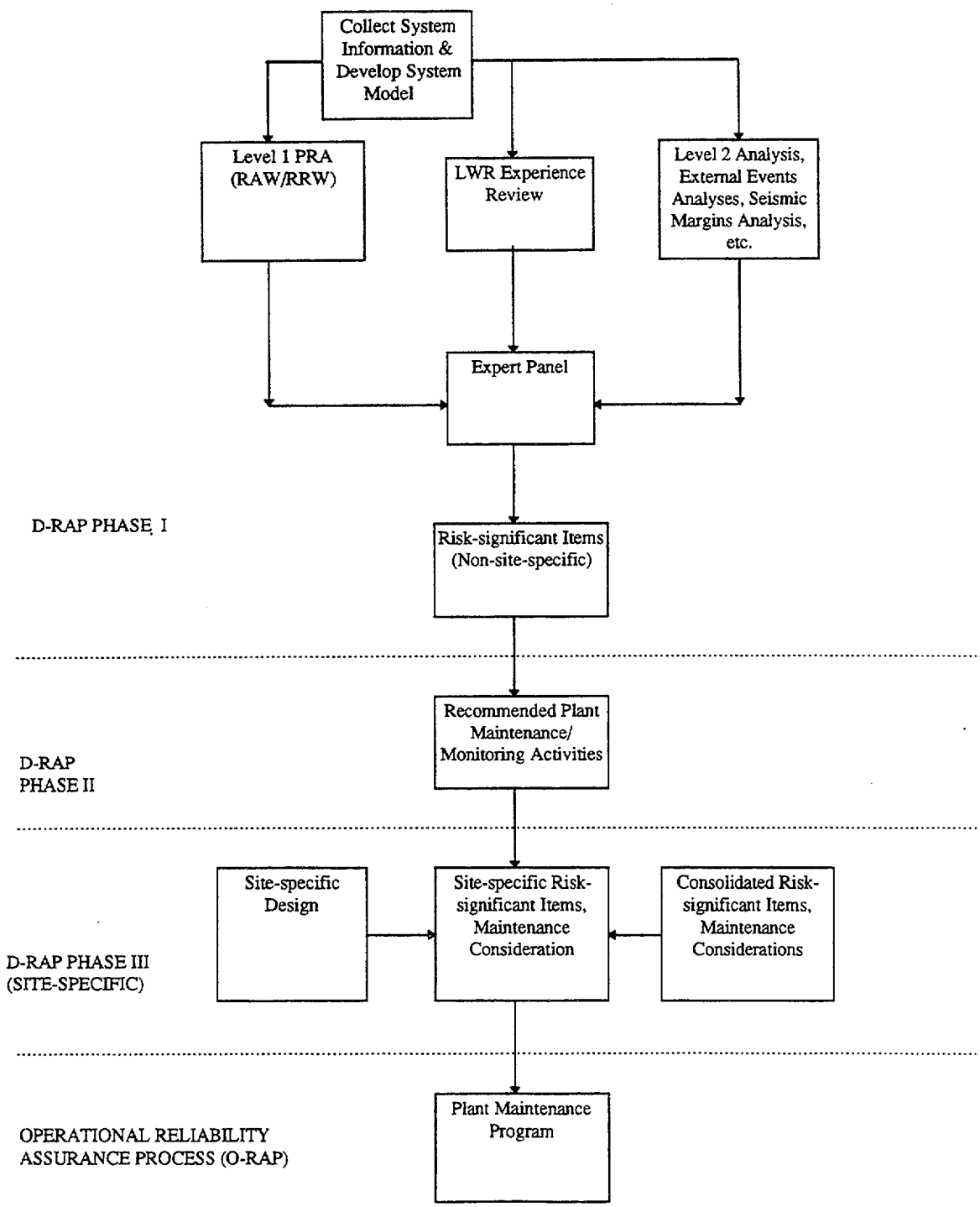


Figure 2. AP600 Design Reliability Assurance Program (D-RAP)

Figure 2 shows the elements of the program.

The program is established in three phases. Phase I is primarily concerned with the design process. During this phase, the risk-significant SSCs are identified for inclusion in the program using probabilistic, deterministic and other methods. Phase II develops maintenance recommendations for the plant's operations and maintenance activities related to the risk-significant SSCs. Phase III incorporates the site-specific considerations (climate, location, etc.) into the process.

Phases I through III feed into the Combined License applicant's Operational Reliability Assurance Process. This process includes the Maintenance Rule -related activities relative to the risk-significant SSCs.

The Phase I selection process for non-site-specific risk-significant SSCs utilizes the Level 1 PRA as a screening tool. The Level 1 PRA evaluates accident sequences from initiating events and failures of safety functions to core damage events. The probability of core damage and the identification of dominant contributors to that state are also considered in the analysis. The Level 1 PRA generates component importance measures for the events/hardware that are modeled. Two of these measures are Risk Achievement Worth and Risk Reduction Worth. A component's risk achievement worth (RAW) is the factor by which the plant's core damage frequency increases if the component reliability is assigned the value 0.0. A RAW value of 2 or greater has been chosen as the criterion for inclusion consideration. This is consistent with the threshold used in the industry implementation (NEI 93-01) [8] of the Maintenance Rule [7]. The program is implemented in three phases. Phase I is primarily concerned with the design process. During this phase, the risk-significant SSCs are identified for inclusion in the program using probabilistic, deterministic and other methods. Phase II develops maintenance recommendations for the plant's operations and maintenance activities related to the risk-significant SSCs. Phase III incorporates the site-specific considerations (climate, location, etc.) into the process.

Risk Reduction Worth (RRW) is the factor by which the plant's core damage frequency decreases if a particular component's reliability is assigned the value 1.0, or perfect reliability. Consistent with NEI 93-01, SSCs with RRW values greater than or equal to 1.005 have been considered for inclusion in the AP600 D-RAP.

Fussel Vesely Worth (FVW) is defined as the component/event's percentage contribution to the total core damage frequency. Consistent with NEI 93-01, SSCs with FVW values greater than or equal to 0.005 have been considered for inclusion in the AP600 D-RAP.

Level 2 PRA results are also considered in the selection process for risk-significant SSCs. The Level 2 analysis predicts the plant response to severe accidents and offsite fission product releases. The equipment that prevents severe accidents and severe accident boundary conditions, as well as the equipment that mitigates the threat to containment from severe accident phenomena, are considered for inclusion in the D-RAP list of risk-significant SSCs.

The results of the following analyses are also used in the SSC selection process:

Internal flood	identifies, analyzes and quantifies the core damage risk contribution as a result of internal flooding during at-power and shutdown conditions
Seismic margins analysis	identifies potential vulnerabilities and demonstrates seismic margin beyond the safe shutdown earthquake.
External events evaluations	(high winds, tornadoes, external floods, transportation accidents, etc.)

An important element of the SSC selection process is the expert panel. This panel consists of personnel from Systems Engineering , PRA and Reliability Engineering. Its purpose is to develop a final risk-significant SSC list using engineering judgment and industry-wide information sources. This panel brings the following insights to the process:

- knowledge of limitations in the PRA and other models
- design insights
- assumptions used in the design/maintainability decision-making process
- identification and interpretation of industry history
- other deterministic considerations

The expert panel makes final inclusion/exclusion decisions on the SSCs that have been identified for consideration based upon the Level 1 component importance measures. Rationale for any exclusion decisions is documented. Additionally, the expert panel uses the semi-quantitative and qualitative information from the other analyses to select the remaining risk-significant SSCs.

Table III provides an example of the D-RAP risk-significant items list.

TABLE III. RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP (EXAMPLE)

System, Structure, or Component (SSC)	Rationale	Insights and Assumptions
System: Component Cooling Water (CCS)		
CCS Pumps	EP	These pumps provide cooling of the normal residual heat removal system (RNS) and the spent fuel pool heat exchanger. Cooling the RNS heat exchanger is RTNSS-important during shutdown reduced-inventory conditions. CCS valve realignment is not required for reduced-inventory conditions.
System: Containment System (CNS)		
Containment Vessel	EP, L2	The containment vessel provides a barrier to steam and radioactivity released to the atmosphere following accidents.
Hydrogen Igniters	EP, L2, Regulations	The hydrogen igniters provide a means to control H2 concentration in the containment atmosphere, consistent with the hydrogen control requirements of 10 CFR 50.34f.
System: Chemical and Volume Control System (CVS)		
CVS Makeup Pump Suction and Discharge Check Valves	RAW	These CVS check valves are normally closed and have to open to allow makeup pump operation.
CVS Makeup Pumps	RAW/CCF	These pumps provide makeup to the RCS to accommodate leaks and to provide negative reactivity for shutdowns, steam line breaks, and ATWS.

During Phase II of the D-RAP, maintenance assessments and recommendations are developed to enhance the reliability of the plant risk-significant components. These activities are shown in Figure 2 as "Recommended Plant Maintenance Monitoring Activities." The recommendations can take the form of monitoring activities or preventive, predictive or corrective maintenance, and are dependent upon the types of failure modes that a component may experience. These modes are generally determined by a failure modes, effects and criticality analysis. The maintenance recommendations address the most significant failure modes of the component.

This information, along with the list of risk-significant SSCs , are provided to the Combined License applicant to support the applicant's D-RAP Phase III and O-RAP activities.

The third phase of D-RAP is the responsibility of the Combined License applicant. At this stage of the process, the D-RAP package is modified or appended based upon factors specific to the site. It is expected that to perform this activity, the Combined License applicant will assemble an expert panel knowledgeable in the systems, operations and maintenance of a plant, with the experience necessary to perform the site-specific SSC selections and evaluations.

The Operational Reliability Assurance Process (O-RAP) is the responsibility of the Combined License applicant. It includes the tasks necessary to maintain the reliability of risk-significant SSCs. This process is expected to be an integral part of the plant's Quality Assurance program, Maintenance Rule program and maintenance plan. The O-RAP activities should incorporate a reliability database with historical data on equipment performance. The compilation and reduction of this data will provide the plant with a source of equipment reliability information. Surveillance and testing should also be included in the process as other means of attaining a high degree of reliability.

The Combined License applicant is responsible for performing the tasks necessary to maintain the reliability of risk-significant SSCs from core loading through the life of the plant.

5. CURRENT STATUS OF PROGRAMS

The Westinghouse AP600 RAM program report was submitted to the Utility Sponsor Group (USG) of the Advanced Reactor Corporation (ARC) in the fall of 1996. The USG requested additional clarification of some of the analysis results, and an updated submittal is currently under review.

The Design Reliability Assurance program is currently under review by the NRC. The program has undergone significant modifications to support the NRC's position of closely aligning the D-RAP outputs with the Maintenance Rule.

6. CONCLUSIONS

The Westinghouse AP600 RAM and D-RAP programs were instituted early in the design process to identify structures, systems and components that are critical to plant safety and reliability, respectively. Although these programs share the use of historical databases, they have remained programmatically separate to ensure that plant safety is not compromised by availability improvement efforts.

The RAM program identifies SSCs that are critical to plant availability by using historical information and deterministic evaluations to produce an initial system-by-system availability allocation. The systems with the highest allocations are analyzed in detail to determine design and maintainability improvements down to the component level, and the information is fed back to the design process. The resulting design improvements have resulted in a projected 90.6% plant availability.

The purpose of the Design Reliability Assurance Program is to ensure that SSCs critical to the plant safety goals are designed with adequate reliability to support future plant operation activities that maintain their reliability throughout the life of the plant. Using results from the PRA in conjunction with deterministic methods and expert panel review, a list of risk-significant SSCs has been developed. The D-RAP studies have resulted in design improvements that reduce plant safety risk. Furthermore, the documented list of risk-significant SSCs provide the future Combined License applicant with information to support the lifelong upkeep of the equipment via QA, Maintenance Rule and other plant Operational Reliability Assurance Process activities.

Although the D-RAP and RAM programs remain separate throughout the design process, it is noted that many Combined License applicants will incorporate the information packages from both programs into an integrated reliability-centered maintenance program.

REFERENCES

[1] EPRI ALWR Utility Requirements Document, Volume III - ALWR Passive Plant

[2] Military Standard 785B, "Reliability Program for Systems and Equipment Development and Production"

[3] Military Standard 470A, "Maintainability Program Requirements for Systems and Equipment"

[4] DE-AC03-90F18495, Westinghouse AP600 Probabilistic Risk Assessment

[5] Westinghouse AP600 Standard Safety Analysis Report

[6] SECY-89-013, "Design Requirements Related to the Evolutionary Advanced Light Water Reactors (ALWRs)," 1989

[7] Code of Federal Regulations 10CFR50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants"

[8] NEI 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," 1993

LIST OF PARTICIPANTS

Allen, P.J.	Atomic Energy of Canada Limited, 2251 Speakman Drive, Mississauga, Ontario L5K 1B2, Canada
Anahara, N.	Electrical & Mechanical Engineering, Nuclear Power Engineering Department, Tokyo Electric Power Company, 1-3 Uchisaiwai-cho 1 Chome, Chiyoda-ku, Tokyo 100, Japan
Angus, V.T.	PECO Energy Co., Limerick Generating Station, P.O. Box 2300, M/C SSB3-1, Sanatoga, PA 19464, USA
Apostolakis, G.E.	Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Bell, R.	Nuclear Energy Institute, 1776 I Street NW, Washington, DC 20006-3708, USA
Blanchat, T.K.	Reactor Safety Experiments, Sandia National Laboratory, Albuquerque, NM 87185-1137, USA
Bliss, H.	Argonne National Laboratory, 9700 South Cass Avenue, Argonne, Illinois 60439, USA
Bowman, M.D.	Engineering and Technical Services, Tennessee Valley Authority Nuclear, 1101 Market Street LP 4H-C, Chattanooga, TN 37402, USA
Brodeur, D.L.	Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Canton, M.	Westinghouse Electric Corporation, P.O. Box 355, Pittsburgh, Pennsylvania 15230-0355, USA
Clauss, J.M.	Sandia National Laboratory, Albuquerque, NM 87185-1137, USA
Cleveland, J.	International Atomic Energy Agency, P.O. Box 100, A-1400 Vienna, Austria

Degrave, C.	Electricité de France, 12-14 Avenue Dutrievoz, F-69628 Villeurbanne Cedex, France
Deitrich, W.	Argonne National Laboratory, 9700 South Cass Avenue, Argonne, Illinois 60439, USA
DeVerno, M.	Atomic Energy of Canada Limited, c/o Centre for Nuclear Energy Research, University of New Brunswick, Fredericton, NB E3B 6C2, Canada
Ford, J.	ABB Combustion Engineering Nuclear Power, P.O. Box 500, 1000 Prospect Hill Road, Windsor, Connecticut, USA
Fuchs, M.	PreussenElektra, Tresckowstr. 5, D-30457 Hannover, Germany
Golay, M.	Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Gotoh, N.	Nuclear Plant Constuction & Engineering Department, Hitachi Works, Hitachi, Ltd, 1-1, Saiwai-cho, 3-chome,Hitachi-shi Ibaraki-ken 317, Japan
Gross, K.	Argonne National Laboratory, 9700 South Cass Avenue, Argonne, Illinois 60439, USA
Hawkins, F.	Office of International Health Programs, US Department of Energy, 19901 Germantown Road, Germantown, Maryland 20874-1290, USA
Herczeg, J.	Office of Nuclear Energy, Science and Technology, US Department of Energy, Washington, DC 20585, USA
Hill, D.	Argonne National Laboratory, 9700 South Cass Avenue, Argonne, Illinois 60439, USA
Jones, B.G.	University of Illinois, At Urbana-Champaign, Department of Nuclear Engineering, 103 South Goodwin Avenue, Urbana, Illinois 61801, USA
Karr, K.N.	ComEd, P.O. Box 428, Chicago, Illinois 60690, USA

Kaushal, N.N. ComEd,
P.O. Box 428, Chicago, Illinois 60690, USA

Kerak, J. Bohunice NPP,
Nuclear Regulatory Authority of the Slovak Republic,
Okruzna 5, 918 64,
Trnva, Slovak Republic

Klickman, A. Argonne National Laboratory,
9700 South Cass Avenue, Argonne, Illinois 60439, USA

Krugmann, U. Siemens AG,
P.O. Box 3220,
D-91050 Erlangen, Germany

Kuk, W. CRC/ComEd,
P.O. Box 428, Chicago, Illinois 60690, USA

Lim, W.S. Korea Electric Power Research Institute,
103-16, Yusung-gu, Munji-dong,
Postal No. 305-380,
Taejun, Republic of Korea

Lyon, R. International Atomic Energy Agency,
P.O. Box 100, A-1400 Vienna, Austria

Magwood, W. US Department of Energy,
1000 Independece Ave. SW,
Washington, DC 20585, USA

Martin-Onraet, M. Electricité de France,
EPN — Mission REP 2000, 12–14 Avenue Dutrievoz,
F-69628 Villeurbanne Cedex, France

Morman, J. Argonne National Laboratory,
9700 South Cass Avenue, Argonne, Illinois 60439, USA

Pedersen, T.J. Department PM,
Nuclear Systems Division,
ABB ATOM AB, S-721-63 Västerås, Sweden

Quiroz, H. Division of Nuclear Reactor and Power Plant Activities,
Argentine Atomic Energy Commission (CNEA),
Ave. Libertador 8250, 1429 Buenos Aires, Argentina

Reifman, J. Argonne National Laboratory,
9700 South Cass Avenue, Argonne, Illinois 60439, USA

Reising, D.V. Department of Mechanical & Industrial Engineering,
University of Illinois, 1206 E. Green Street,
Urbana, IL 61801, USA

Rochau, G.E.	Nuclear Reactor Safety Department, Sandia National Laboratories, P.O. Box 5800, Albuquerque, NM 87185-0742, USA
Rohar, S.	Slovakian Nuclear Regulatory Authority, Bajkalska 27, P.O. Box 24, 820 07 Bratislava 27, Slovak Republic
Rupani, B.B.	Bhabha Atomic Research Centre, Reactor Engineering Division, Hall No. 7, BARC, Mumbai - 400 085, India
Shah, D.	Consolidated Edison Company of New York, Inc., Indian Point 2, Buchanan, NY 10511, USA
Shimamura, K.	Systems Safety Department, Nuclear Power Engineering Corporation, Fujita Kanko Toranomon Bldg 5F, 17-1, 3 Chome Toranomon, Minato-ku, Tokyo 105, Japan
Singer, R.	Argonne National Laboratory, 9700 South Cass Avenue, Argonne, Illinois 60439, USA
Staunton, R.H.	Oak Ridge National Laboroatory, P.O. Box 2009, Oak Ridge, Tennessee 37831-8038, USA
Stubbins, J.F.	Department of Nuclear Engineering, University of Illinois, 214 NEL, 103 South Goodwin Avenue, Urbana, IL 61801, USA
Todreas, N.E.	Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Wei, T.Y.C.	Argonne National Laboratory, 9700 South Cass Avenue, Argonne, Illinois 60439, USA
Wittich, K.	Atomic Energy of Canada Limited, Chalk River Laboratories, Chalk River, Ontario K0J 1J0, Canada
Wyman, R.	Lawrence Livermore National Laboratory, 7000 East Avenue, Livermore, CA 94550, USA

98-02826