IAEA-TECDOC-CD-1749

IAEA TECDOC SERIES

IAEA-TECDOC-CD-1749

International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety

Proceedings of an International Conference Held in Vienna, Austria, 21–24 October 2013

IAEA
International Atomic Energy Agency

INTERNATIONAL CONFERENCE ON TOPICAL ISSUES IN NUCLEAR INSTALLATION SAFETY: DEFENCE IN DEPTH — ADVANCES AND CHALLENGES FOR NUCLEAR INSTALLATION SAFETY

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA, ISLAMIC REPUBLIC OF
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

IAEA-TECDOC-CD-1749

INTERNATIONAL CONFERENCE ON TOPICAL ISSUES IN NUCLEAR INSTALLATION SAFETY: DEFENCE IN DEPTH — ADVANCES AND CHALLENGES FOR NUCLEAR INSTALLATION SAFETY

PROCEEDINGS OF AN INTERNATIONAL CONFERENCE
HELD IN VIENNA, AUSTRIA, 21–24 OCTOBER 2013

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2014

COPYRIGHT NOTICE

For further information on this publication, please contact:

Safety Assessment Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
October 2014

IAEA Library Cataloguing in Publication Data

International Conference on Topical Issues in Nuclear Installation Safety : Defence in Depth – Advances and Challenges for Nuclear Installation Safety. — Vienna : International Atomic Energy Agency, 2014.
p. ; cm. — (IAEA-TECDOC-CD series, ISSN 1684–2073 ; no. 1749)
ISBN 978–92–0–158214–0
Includes bibliographical references.

1. Nuclear facilities — Security measures. 2. Nuclear facilities — Safety measures. 3. Nuclear facilities — Defense measures.
I. International Atomic Energy Agency. II. Series.

IAEAL 14–00933

FOREWORD

The first International Conference on Topical Issues in the area of nuclear safety was held by the IAEA in 1998 in Vienna, Austria, with three further conferences held in 2001 (Vienna), 2004 (Beijing) and 2008 (Mumbai), which all focused on different topics. The issues discussed, and the recommendations made, have provided valuable insights as to where future activities should be focused. These activities have included the development of guidance on safety performance indicators and the development of new IAEA safety standards, for example on probabilistic safety assessment and establishing safety infrastructure for new nuclear power programmes. They have also highlighted the important roles of national regulators and international organizations in harmonizing global nuclear safety and in developing the relationship between safety and security requirements.

At the International Experts' Meeting (IEM) on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, held in Vienna, 19–22 March 2012, the important elements of the broadened safety agenda were the concerted, but independent, efforts by Member States to establish additional layers of protection to prevent severe accidents, coupled with an increased priority on mitigation and a focus on the preservation of containment to enhance defence in depth (DID). The full report of the IEM was presented to the Fukushima Ministerial Conference on Nuclear Safety, in December 2012. In order to further strengthen DID, the Ministerial Conference re-emphasized the importance of measures for the prevention and mitigation of severe accidents.

The International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety was held at the IAEA, in Vienna, 21-24 October 2013. The conference continued the work done in this area so far and focused on the concept of DID and its implementation at nuclear installations. The essential philosophy of DID is to provide multiple levels of protection so that potential failures are compensated in a manner that ensures the protection of the workers, the public and the environment. DID is fundamental to the safety of nuclear installations and needs to be implemented during all stages of their life cycle — from the design phase through operation and eventual decommissioning. While the DID concept has been implemented largely successfully in the nuclear industry, recent events such as the Fukushima Daiichi nuclear accident have highlighted potential vulnerabilities exposed by extreme external events. Recent national and international actions in response to the Fukushima Daiichi accident to address rare, but credible, events with significant adverse safety consequences suggest that the implementation of the DID concept needs to be revisited and strengthened. It is important for the international nuclear community to exchange ideas and information on how the application of the DID concept is evolving, and on the challenges that are being encountered.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

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 IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

ADVANCES AND CHALLENGES IN THE IMPLEMENTATION OF DEFENCE IN DEPTH IN ACCIDENT MANAGEMENT AND EMERGENCY PREPAREDNESS AND RESPONSE (TOPICAL SESSION 3)

CROSS-CUTTING ISSUES IN THE IMPLEMENTATION OF DEFENCE IN DEPTH (TOPICAL SESSION 4)

SUMMARY

The IAEA Safety Glossary defines defence in depth (DID) as "a hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions." The objectives of defence in depth are to: (a) compensate for potential human and component failures, (b) maintain the effectiveness of the barriers by averting damage to the facility and to the barriers themselves, and (c) protect workers, members of the public and the environment from harm in accident conditions in the event that these barriers are not fully effective.

The objective of this conference was to foster the exchange of information on the latest thinking and advances in the implementation of the concept of DID in nuclear installations, and the associated challenges. The focus was on operating nuclear installations, including nuclear power plants, research reactors and fuel cycle facilities, and on how lessons learned from operating experience and recent events were used to enhance safety.

The conference covered four topical issues to cover the different states and phases of a nuclear facility: (1) Advances and challenges in the implementation of DID in siting, design, and construction, (2) Advances and challenges in the implementation of DID in commissioning and operation, (3) Advances and challenges in the implementation of DID in accident management and emergency preparedness and response, and (4) Cross-cutting issues in the implementation of DID (e.g. safety culture, regulatory oversight, human factors, etc.)

The conference consisted of an opening session, four sessions dedicated to the four topical issues mentioned above, and a closing session to summarize the conference findings, conclusions and recommendations for further actions. The conference president presented the following conclusions in the closing session:

- Although the DID concept remains valid after the Fukushima accident, it has to be strengthened and extensively applied in order to meet most recent safety objectives for nuclear plants, such as the ones adopted by the Contracting Parties during the extraordinary meeting of the Convention for Nuclear Safety. DID is not only relevant for the design of new installations, but should also be maintained/improved by periodic safety reviews over the entire life of installations.
- While DID remains an essential tool for safety and should continue to be applied, further development and guidance are required on several subjects such as:
  - Consistent application of design basis definitions at the international level;
  - Postulation of multiple failures in reactor design;
  - Practical elimination of sequences, in relation with the use of deterministic and probabilistic approaches;
  - Assessment of independence and reliability of different levels of DID;
  - Approach to be adopted for very low probability events leading to very large health and societal consequences;
  - Tools to be based on already developed methodologies to ensure that safety provisions are comprehensive enough to ensure DID.
- One important lesson from the Fukushima Daiichi accident is that extreme external hazards can result in common cause failures jeopardizing simultaneously several levels of defence. Such common cause failures can result in complete loss of the instrumentation of the plant, inducing extreme difficulties in the management of a

severe accident. Special attention should be given to these risks when implementing DID.

- Hazards, as well as combination of hazards, to be taken into account in relation to DID need further work and international guidance.
- Effective implementation of DID requires that the most recent knowledge resulting from operational experience feedback as well as research and development are taken into account. Human factors and reliability of instrumentation and control systems are subjects that require further development and guidance.
- Approaches have already been developed and efforts are underway to improve robustness of plants, taking into account the current lessons learned from the Fukushima Daiichi accident. However, such approaches still need to be matured on several topics such as:
    - Criteria to choose between fixed and mobile equipment;
    - Design approach for equipment or hardened safety core of equipment ensuring fulfilment of safety functions under extreme conditions.
- As already highlighted by IAEA, WANO and NEA, mitigation levels of DID should be enhanced in operational safety, while prevention should also be maintained. OSART missions and WANO peer reviews have already been extended to cover some design aspects related to continuous improvement of operating plants.
- Wider use of IAEA review services, especially those related to siting, design and emergency preparedness, should be promoted and established, contributing to the prevention of nuclear accidents and emergency management. Peer pressure should be extended to ensure the implementation of their recommendations. The topics of these peer reviews could be chosen in light of operating experience feedback.
- Realistic drills are essential for the effectiveness of emergency preparedness. They should involve all the key players, at all levels, in decision making and communication. They should be designed, as much as possible, to train individuals and prepare organizations to react in a flexible manner to unexpected situations.
- An idea was proposed that the technical concept of DID is necessary but not sufficient to ensure safety. Effective institutional systems need to be set up, applying the same DID concept and principles, involving all stakeholders (operators, regulators, industry, etc.). To address this issue, a peer-review service was suggested to be established jointly by IAEA and WANO, using the expertise of NEA, with initial self-assessment feeding into Nuclear Safety Convention review meetings.
- Following the Fukushima accident, WANO adopted a strategic orientation to increase its strength and its focus on nuclear safety. It improved its peer review process and expended its scope to integrate some design aspects, as well as corporate peer reviews. Overall, the peer pressure was increased in order to enhance commitment to safety of the operators worldwide.
- The safety of nuclear and non-nuclear industries would benefit from a closer collaboration allowing better sharing of experience feedback, as well as education and training methods. Nuclear safety could also benefit from the experience of first response organizations, such as police or fire brigades.

OPENING SESSION

OPENNING ADDRESS

D. FLORY
Deputy Director General,
Head of the Department of Nuclear Safety and Security,
International Atomic Energy Agency

Good morning ladies and gentlemen, dear colleagues.

- Welcome to the 5th International Conference on Topical Issues in Nuclear Installation Safety, covering the advances and challenges in implementing Defence in Depth (DID). This topic has received much attention since the Fukushima Nuclear Accident and the resulting IAEA Action Plan for Nuclear Safety. Indeed, the nuclear community has made significant progress in examining many DID-related safety matters, aimed at improving nuclear safety in general.
- The outcome of these activities suggests that the concept of DID may be undergoing re-evaluation.
- Particular to this conference, is the focus on better implementation of defence in depth strategies to further strengthen safety of nuclear installations for the future.
- The concept set out in the strategy for defence in depth—a layered approach to safety, remains sound and the application of it has been widely successful in industry, but like any good concept or philosophy, implementation may not always be adequate. Its implementation, I would even say its effective implementation, in all phases: from design through operation to eventual decommissioning requires further analysis and strengthening, to address challenges identified following the Fukushima accident.
- Examples can be provided of additional provisions to add more “layers” of defence (for example, enhancements that were implemented worldwide following “stress tests” to prevent severe accidents and to place increased priority on mitigation with a focus on the preservation of containment).
- We anticipate that the working sessions of this conference will allow us to share experience and enhance our understanding on safety measures on the implementation of DID in siting, design and construction; commissioning and operation; accident management and emergency preparedness and response; as well as the cross cutting organizational, technical and human factors issues that underlie defence in depth.
- While substantial efforts and resources have been invested to gain an understanding of what happened and why in the Fukushima Daiichi accident and much progress has been made, additional lessons learned will need to be taken forward. Learning and sharing lessons learned, and implementing the activities necessary for progress to be ongoing, is a quest for improvement that must never cease.
- I wish you a productive conference as your additional efforts into focusing on these topics will improve and enhance the implementation of defence in depth going forward.
- Thank you for your attention.

KEYNOTE PRESENTATION

NEA AND ITS ROLE IN ENHANCING THE IMPLEMENTATION OF DEFENCE IN DEPTH (DID) IN LIGHT OF THE FUKUSHIMA DAI-ICHI ACCIDENT

K. SHIMOMURA
OECD Nuclear Energy Agency (NEA), Issy-Les-Moulineaux,
France
Email: Kazuo.SHIMOMURA@oecd.org

This keynote speech will give an overview of NEA Activities to Enhance Global Nuclear Safety both those core to its work and those that have been initiated after the Fukushima Accident. In particular it will highlight the outcomes of the recently published "NEA report on the Fukushima Daiichi Nuclear Power Plant Accident".

The speech will specifically point out those lessons learnt related to Defence in Depth, and how those were fed into the NEA's one day workshop on "Challenges and Enhancements to DiD in light of the Fukushima Dai-ichi Accident", that took place on 5th June 2013.

A workshop that brought together the member countries represented on the NEA's three major standing committees for safety to not only discuss the lessons learnt from the accident but also what the NEA members considered could be done to enhance the understanding and implementation of defence in depth within nuclear safety.

Members of these three standing committees, the Committee for Nuclear Regulatory Activities (CNRA), The Committee for Safety of Nuclear Installations (CSNI) and the Committee on Radiation Protection and Public Health (CRPPH) represent a considerable body of knowledge on the application of DiD within the countries using nuclear energy.

The outcome of the workshop was the identification of a number of key tasks that NEA would take forward to assist in harmonising and enhancing globally the implementation of the DiD philosophy.

The speech will in addition detail how the discussions ranged across the whole of the nuclear safety framework, what conclusions were derived and the process the NEA followed to incorporate those tasks within its future programme of work either by enhancing current activities or creating new ones.

KEYNOTE PRESENTATION

CNS ORIENTATIONS, SAFETY OBJECTIVES AND IMPLEMENTATION OF THE DEFENCE IN DEPTH CONCEPT

A.C. LACOSTE
Autorité de Sureté Nucléaire, Montrouge,
France
Email: Andre-Claude.LACOSTE@asn.fr

The 6th Review Meeting of the Convention on Nuclear Safety (CNS) is convened in Vienna next year for two weeks from Monday March 24th to Friday April 4th 2014. The consequences and the lessons learnt from the accident that occurred at the Fukushima Daiichi nuclear power plant will be a major issue.

The 2nd Extraordinary Meeting of the CNS in August 2012 was totally devoted to the Fukushima Daiichi accident. One of its main conclusions was Conclusion 17 included in the summary report which says:

"*Nuclear power plants should be designed, constructed and operated with the objectives of preventing accidents and, should an accident occur, mitigating its effects and avoiding off-site contamination. The Contracting Parties also noted that regulatory authorities should ensure that these objectives are applied in order to identify and implement appropriate safety improvements at existing plants*".

The wording of the sentences of Conclusion 17 dedicated, the first one to new built reactors, the second one to existing plants, can be improved and clarified. But obviously the issue of the off-site consequences of an accident is fundamental.

So the in-depth question comes: what can and should be done to achieve these safety objectives? And in particular how to improve the definition and then the implementation of the Defence in Depth Concept?

From my point of view, this is clearly the main issue of this Conference.

KEYNOTE PRESENTATION

NUCLEAR SAFETY R&D FOR THE KNOWLEDGE-BASED IMPLEMENTATION OF DEFENCE IN DEPTH

W-P. BAEK
Korea Atomic Energy Research Institute (KAERI), Department of Nuclear Safety Research, Yuseong-gu, Daejeon, Republic of Korea
Email: wpbaek@kaeri.re.kr

Assuring a high level of safety is a pre-requisite for the development and utilization of nuclear technology. The most fundamental approach for nuclear power plant (NPP) safety is "defence in depth (DiD)," which is a combination of multiple physical barriers and multiple (generally 5) levels of protection, with the aim of accident prevention and mitigation [1]. NPPs around the world have shown excellent safety records for over 14,500 cumulative reactor years, compared with other electricity sources, by properly implementing DiD. However, the occurrence and severe consequences of the Fukushima accident have provoked controversy on the completeness of the DiD concept.

There have been active discussions on DiD with respect to the Fukushima accident. A general consensus has been arrived that the concept of DiD is still valid but its implementation was incomplete for the Fukushima NPP [2]. Had DiD been properly implemented during the design, construction and operation, much better provisioning against the extreme earthquake and tsunami would have been available and the accident consequences would not have been so disastrous.

Figure 1 illustrates the overall progression of the Fukushima accident [3]. The severe consequences of the accident were mainly due to the incomplete preparation before the accident rather than improper reactions during accident progression with the worst working environment. It is represented in Fig.1 as "Incomplete Design, Siting & Emergency Preparedness with respect to site characteristics, severe accident, and procedures & training."

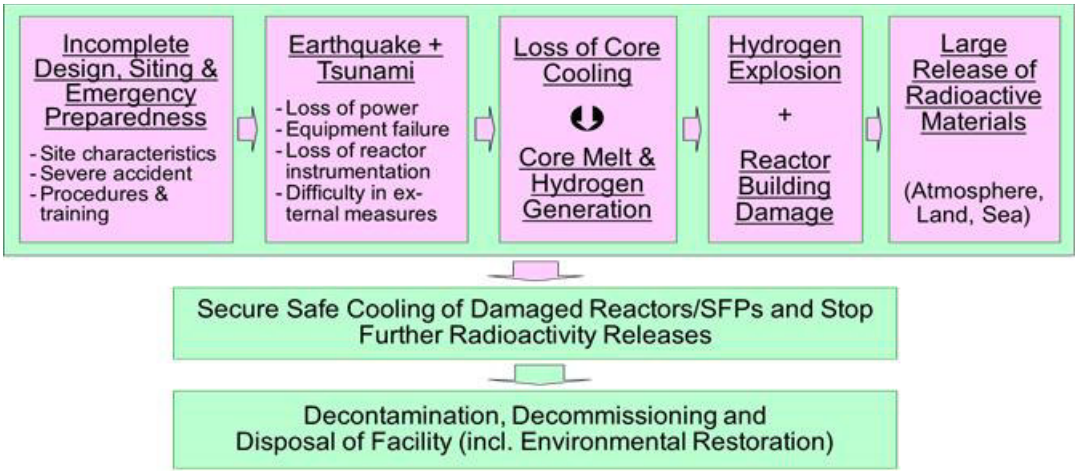

FIG. 1. Overall progression of the Fukushima accident.

The KNS Committee on Fukushima Accident pointed out the following as fundamental causes of the Fukushima accident [3]:

- Incomplete consideration of Japan-specific site characteristics (i.e. geological environment), during the processes of design, construction and operation of the U.S. designed BWRs.
- Safety-critical decision making based on a vague belief and over-confidence of NPP safety, without fully utilizing the best available knowledge and information.
- Problems in safety culture, governmental structure and decision making processes related to nuclear energy development and utilization.

The first two causes are related to the need for decision making based on reliable and best-available scientific knowledge; nuclear safety R&D is the primary tool for fulfilling this need, i.e. "knowledge-based decision making".

Figure 2 illustrates the role of nuclear safety R&D for knowledge-based decision making. Major outputs from R&D would be (a) original knowledge, (b) infrastructure for safety assessment & verification, and (c) nuclear safety experts. They are used for knowledge-based decision making in many areas/applications, enhancing the safety, reliability, and economics of nuclear technology utilization.

There exist technical safety issues with knowledge gaps for each level of DiD. In particular, the Fukushima accident highlighted some issues, including the following:

- Design basis site characteristics.
- Robustness of electrical systems and ultimate heat sinks.
- Severe accident phenomena (hydrogen, fission products, etc.) and mitigation measures.
- Role of passive systems for prevention and mitigation of severe accidents.
- Instrumentation and monitoring deteriorated plant conditions.
- Safety of spent fuel storage facilities.
- Effects of low-level radiation exposure.

The above issues are related to single or multiple levels of DiD.

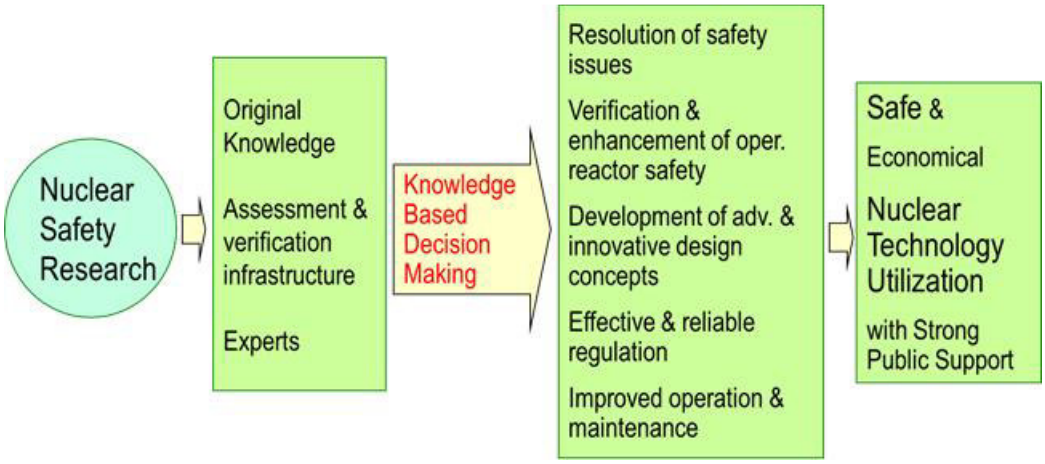

FIG. 2. Role of nuclear safety research [4].

After briefly describing the DiD concept, the Fukushima accident, and the role of nuclear safety R&D, this presentation will discuss safety issues, important phenomena, knowledge gaps, and typical R&D programmes relevant to each level of DiD. Some discussion will also be made on how Korea has established nuclear safety R&D programs for knowledge-based decision making in safety related matters. The aspects of information sharing and communication among stakeholders will also be discussed.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).

[2] OECD NUCLEAR ENERGY AGENCY, The Fukushima Daiichi Nuclear Power Plant Accident: OECD/NEA Nuclear Safety Response and Lessons Learnt, OECD/NEA No. 7161 (2013).

[3] KNS Committee on the Fukushima Accident, KNS Report on the Fukushima Accident – Characteristics, Consequences, Causes and Lessons of the Accident, Korean Nuclear Society (2013) (in Korean).

[4] BAEK, W.P., "Nuclear Safety Research in Korea in Light of Fukushima Accident", U.S. NRC's 25th Regulatory Information Conference, Rockville, MD (2013).

ADVANCES AND CHALLENGES IN THE IMPLEMENTATION OF DEFENCE IN DEPTH IN SITING, DESIGN, AND CONSTRUCTION (TOPICAL SESSION 1)

INVITED PRESENTATION

THE DEFENCE IN DEPTH CONCEPT APPLIED TO THE NEW REGULATORY REQUIREMENTS IN JAPAN

H. YAMAGATA
Nuclear Regulation Authority, Minato-ku, Tokyo,
Japan
Email: hiroshi_yamagata@nsr.go.jp

The new regulatory requirements based on lessons learnt from Fukushima Daiichi accident, which places emphasis on Defense-in-Depth concept, was put into effect in Japan on 8th July, 2013. It is required to prepare multi-layered protective measures. Each layer should achieve the objective only in that layer regardless of the measures in the other layers. The challenge is how to enhance independence of measures between layers.

In the third layer, the current concept of design regarding safety relies on “single failure”, whose condition is elimination of common cause failure (CCF). To eliminate CCFs we introduced a more accurate approach in assessment of earthquake and tsunami, and introduction of measures against tsunami inundation. Redundancy of safety systems could not eliminate CCF by extreme natural hazards. Safety system should be designed by due consideration of diversity and independence including spatial dispersement.

In the fourth layer, multi-layered protective measures are also applied for severe accidents, which consists of “prevention of core damage” under multiple failure, “prevention of containment failure”, and “prevention of large release, that is controlled release by venting”.

In the fifth layer, we also require operators to prepare measures for “suppression of radioactive materials dispersion”. Of course, off-site emergency preparedness and response has been enhanced by introduction of PAZ and UPZ.

Introduction of “Specialized Safety Facility” against intentional aircraft crash will contribute enhancement of some layers by providing electricity and water under extremely severe conditions.

The new regulatory requirements are not our goal, just a first step. It is expected for regulator and operators to improve safety continuously by periodic comprehensive safety assessments including IPE, IPEEE, Margin test, and etc. We have to make an upward spiral of nuclear safety.

THE DESIGN OPTIONS AND PROVISION FILE AND THE ROLE OF DEFENCE IN DEPTH WITHIN THE PRE-LICENSING OF THE MYRRHA PROJECT

G.L. FIORINI[*], N. HAKIMI[*], B. TOMBUYSES[**], C. DAMS[**], A. WERTELAERS[**], M. SCHRAUBEN[**], R. DRESSELAERS[**]
[*]Nuclear Safety Consultant on behalf of FANC
[**]Federal Agency for Nuclear Control (FANC),
Bruxelles, Belgium
E-mail: Gian-Luigi.fiorini@fanc.fgov.be

Abstract
The Belgian Federal Agency for Nuclear Control (FANC) is engaged in a process of pre-licensing for the experimental reactor MYRRHA. The regulatory framework applicable for the implementation of the MYRRHA project and the expected safety, security and safeguards philosophy are described by FANC in a Strategic Note. This document presents a logical flow chart which defines the steps required to design a basic nuclear installation and ensure compliance with the requirements of nuclear safety, security and safeguards. Using this flow chart, the content of a set of volumes (Design Options and Provision File - DOPF) is defined; the DOPF will serve as a basis for the evaluation of the concept with the acceptability of the selected design options. Defence in depth (DiD) and its fundamental principles remain the foundation of the whole process. The paper summarizes the contents of the Strategic Note and the DOPF and focuses more specifically on aspects relating to changes in the concept of defence in depth and on practices for their integration in the process of design / assessment of the MYRRHA reactor.

1. INTRODUCTION

The SCK-CEN, the Belgian Nuclear Research Centre in Mol is currently working on the design of MYRRHA (Multi-purpose Hybrid Research Reactor for High-tech Applications), a multi-purpose irradiation facility which will replace the BR2 reactor, a materials testing reactor (MTR), in operation since 1962. MYRRHA is a flexible fast spectrum research reactor (50-100 MW_{th}); it is conceived as an accelerator driven system (ADS), able to operate in sub-critical and critical modes. It comprises a proton accelerator of 600 MeV, a spallation target and a multiplying core with MOX fuel, cooled by liquid lead-bismuth (Pb-Bi). The installation should be operational at full power around 2023 [1].

For the establishment and operation of a nuclear facility the future operator must request permission to the Belgian Federal Agency for Nuclear Control (FANC) in accordance with the procedures specified in RGPRI, Section 6 for installation of Class 1 [2]. The documents to be submitted to the authority are indicated; they include, among others, the description of the installation, the technology retained by the applicant for the facility and a Preliminary Safety Report. Upon submission of the application for authorization, it is assumed that the safety options are fixed and the safety architecture of the installation is frozen.

For nuclear projects using new technologies, such as MYRRHA, it is desirable that a pre-licensing process be implemented to follow the pre-project so that the regulator can communicate in time expectations about the level of safety and security that it expects for the future installation. As part of this pre-licensing action, documents issued by the regulator are organized in a hierarchical manner; for each new project a Strategic Note identifies safety goals and safety objectives as well as regulations and standards applicable to the project. In the case of MYRRHA, this Strategic Note [3] is followed in this hierarchy, by a document that describes the contents of the Design Options and Provision File (DOPF – [4]): a set of volumes whose main objective is to organize the presentation and the discussion between the designer and the safety authority on the basis of a predefined Table of contents. A series of thematic Guidance will describe in more detail the expectations of the regulator in relation to the project (e.g. on earthquake, aircraft crash, etc.).

The Defence in depth (DiD) and its fundamental principles remain the foundation of the whole process which is described by the Strategic Note and materialized by the DOPF. Following the FANC position, the DiD principles shall be fully implemented for the design of MYRRHA and it will be, among others, on the basis of compliance with these principles that the concept will be assessed. In this regard, the designer attention is drawn on the availability of recent references which formulate proposals for refinements of the concept of DiD, as well as recommendations on how to incorporate these refinements within the design.

Below, the contents of the Strategic Note and DOPF are succinctly described and discussed. Preliminary indications are provided on a specific subject – the deterministic safety demonstration – which is in direct relation with the DOPF content.

2. THE MYRRHA STRATEGIC NOTE

The objectives of the MYRRHA strategic note [3] are:

- to recall and resume the regulatory framework applicable for the implementation (design, construction, operation, etc.) of the MYRRHA project (Class 1 nuclear facility);
- to present and comment the safety, security and safeguard philosophy (e.g. goals and objectives, requirements, principles and guidelines) which has to be considered in order to conceive and implement a safe and secure design for MYRRHA;
- to shortly comment and present the content of the Design Options and Provisions File (DOPF) which is expected to be prepared by the designer and submitted to the FANC for assessment within the context of the "pre-licensing process". In the view of FANC, the DOPF incorporates both the "*dossier d'options de sûreté (DOS)*" and the "*dossier d'options de sécurité (DOSEC)*" referred to in the pre-licensing note [2].

The document is written for the MYRRHA project taking into account that this installation would be an experimental facility, using a liquid metal cooled fast reactor (LFR) which is considered as a Gen-IV technology. Within the following sections only the two latter objectives are shortly presented and commented (the Safety, Security and Safeguard philosophy & the DOPF content).

2.1. The safety philosophy

The safety philosophy includes the information necessary to translate the safety principles, requirements and guidelines into safety options and into design and operational specifications needed to select the technical and operational provisions (e.g. equipment and operational procedures); high-level safety goals and objectives are developed into quantitative targets for use by the designer. The MYRRHA design and its safety architecture are materialized by this set of technical and operational provisions; the latter has to meet the qualitative and quantitative safety objectives and aims at reaching the safety goals. This demonstration goes through an iterative process and has to be provided with a preliminary safety assessment carried out by the designer and documented in the DOPF.

2.1.1. Safety principles, requirements and guidelines

Safety Fundamental Principles are defined by IAEA Safety Standards [5]. Requirements are available within the collection of IAEA Safety Standards (e.g. [6] [7]) or from other sources (e.g. [8]) even if they are not systematically fully applicable to new installations like MYRRHA. This is why a specific effort may be needed to adapt or develop specific documents to finalize the regulatory framework. The designer shall provide the

documentation sources to prove that the retained MYRRHA design requirements will comply, with due consideration for plant specificities, to the above references.

Several IAEA Safety Guides provide recommendations and guidance on how to comply with the IAEA safety requirements. In that context, general and specific IAEA safety guides shall be considered by the designer as the first option when compared to alternative guidance, taking into account the specificity of MYRRHA. Other complementary guidance documents may be followed, provided a justification is presented.

2.1.2. Safety goals and safety objectives

Safety goals and objectives, applicable to a hybrid research reactor such as MYRRHA and endorsed internationally are not available at this moment, in particular because proposals in this domain address mainly electricity producing reactors, with a standardized design, and not a unique irradiation facility like MYRRHA. Nevertheless the design and operation of MYRRHA should warrant a high level of safety. This means that the expected level of safety should:

- Reach, as a minimum, a level as high as the level of the (best) installations according to the WENRA objectives for new nuclear power plants [9].
- Tend to the highest level that can be expected for new reactor designs – i.e. the Generation IV safety goals [10].

Concerning the safety objectives, the designer shall provide a justification demonstrating that they are met or exceeded by the safety architecture and document this justification in the DOPF. The achievement of the safety goals should not be considered as mandatory but if the goals are not met, the designer shall provide a justification which will be documented in the DOPF.

2.2. The security and safeguards philosophy

The security philosophy is based on objectives principles and requirements. The objectives stress the need to prevent, detect, delay and intervene in case of malevolent event. The twelve fundamental security principles cover [11]: *Responsibility of the State; Responsibilities During International Transport; Legislative and Regulatory Framework; Competent Authority; Responsibility of the License Holders; Security Culture; Threat; Graded Approach;* ***Defence in Depth****; Quality Assurance; Contingency Plans; Confidentiality.* These principles are the basis of the regulation concerning the physical protection and will lead to the security requirements which motivate the need for the identification and categorization of Design Basis Threat (DBT).

2.2.1. The safeguards philosophy

The safeguard philosophy is based on objectives and obligation. The safeguards objectives are defined to verify that nuclear material are not diverted to non-peaceful applications, that the declared basic technical characteristics of an installation correspond to the reality on the field and the absence of undeclared nuclear materials and activities. The "obligation" addresses the need for transparency through a predefined set of declaration or formal engagements.

2.2.2. Safety, security and safeguards integrated approach: basic principles

Coherently with the WENRA safety objective O5[1], the safety architecture reached at the end of the safety design process should not be in contradiction with any of the security fundamentals and safeguards obligations. Thus, in order to reach a safe and secure architecture, a security process should be initiated that aims to fully comply with the security requirements and safeguards obligations: any measures taken in order to satisfy at the same time safety and security requirements should in a first step ensure safety and then be checked and assessed against the security requirements.

2.3. Design options and provisions file (DOPF)

Following the indication of the Strategic Note the designer will present, within the DOPF, the selected safety and security provisions implemented within the design, the operational safety specifications as well as the technical and operational security requirements taking into account the safeguards obligations. The safety design and operational specifications are themselves derived from the safety options proposed by the designer. The DOPF will also provide indications about the measures implemented to approach the safety goals and to achieve the defined safety objectives.

A top tier template is proposed for the DOPF; it is organized in different volumes to ease the presentation and the analysis: *Volume 1: Purpose and description of the facility; Volume 2: Approach to the nuclear safety; Volume 3: Design Options and selected provisions and their justification against the objectives, goals, principles, requirements and guidelines; Volume 4: Management system for safety of the installation; Volume 5: Security and Safeguards Integrated Approach*

To avoid, or at least reduce, the risk of ambiguity in the interpretation of the DOPF it seemed important to explain as much as possible the meaning of a number of terms used in the documents. Terms such as *safety, security and safeguard objectives,* as well as *safety options* were already commented, in a very generic manner, within [2]. Additional terms are discussed within [3] to help understanding the concatenation of the DOPF's content: *Safety Goals; Safety Objectives; Decoupling Criteria; Safety principles; Safety Requirements; Safety guidelines; Safety options; Security Fundamentals and requirements; Safeguards obligation; Design and Operational Safety Specifications; Technical and operational security requirements; Provisions; Safety, Security and Safeguards Architecture.*

2.3.1. The flowchart for the terms of the design

Figure 1 resumes the logic and the links between the different steps as they are detailed within the DOPF commented template [4].

2.3.2. The objectives for the different volumes and the concatenation within the DOPF

Hereafter the objectives of each single volume of the DOPF are shortly presented and commented.

---

[1] WENRA O5: *"On Safety and security interfaces, ensuring that safety measures and security measures are designed and implemented in an integrated manner. Synergies between safety and security enhancements should be sought".*

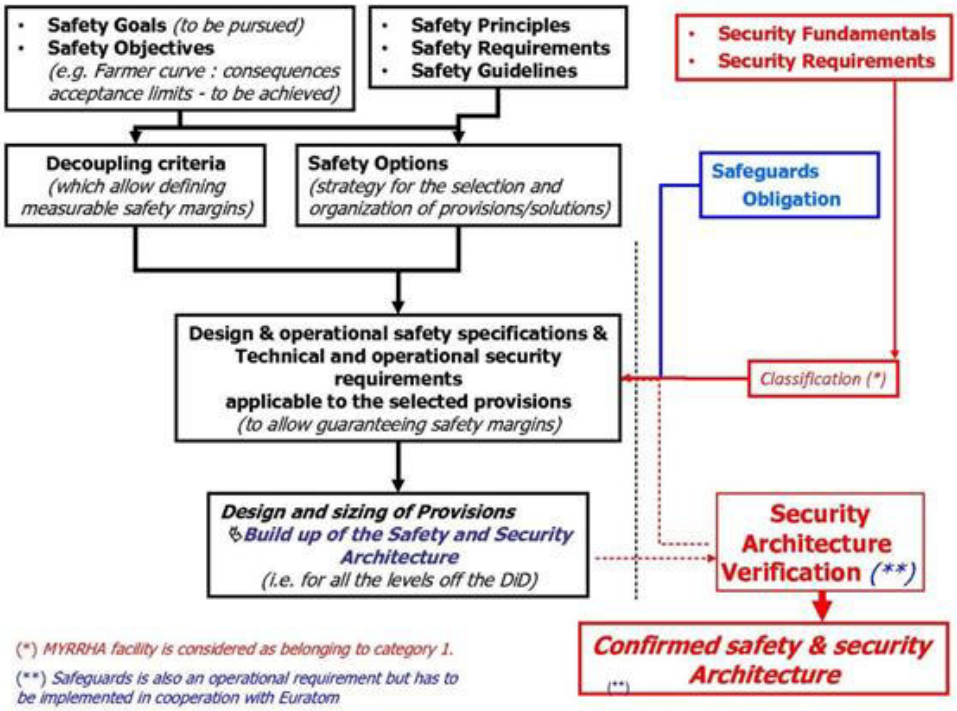

FIG. 1. Relationship between the different steps and terms for the DOPF.

2.3.2.1. Objectives of the volume 1 "purpose and description of the facility"

Apart from the presentation of the general purpose of the installation within the context of the nuclear R&D, the objectives of Volume 1 of the DOPF are: to present the description and characteristics of the site; to present the installation both in terms of its overall architecture and the description of its different components; to provide information on operation modes (critical, sub critical, irradiation for commercial purposes, etc.); and finally to present the interactions of the plant with its environment (offsite power supply, cold source, management of effluents / waste, others (e.g. transports)). Estimations of the potential source term for the different plant conditions (normal and abnormal) should also be indicated.

The level of detail will obviously be compatible with the stage of the design at the time of presentation of the DOPF.

2.3.2.2. Objectives of the volume 2 "approach to nuclear safety"

The key objective of the volume 2 of the DOPF is to describe and discuss the safety goals, objectives, principles and the general design requirements selected by the designer and applicable to the safety architecture of the installation considering its specificities. Indications should be provided to positions the choice of the designer versus the goals objectives and requirements elaborated by international organization such the Generation IV International Forum, (GIF), the IAEA/INPRO, etc.

The description of the different steps of the design, as well as indications about the process used by designers to practically implement the principles, requirements and the guidelines in order to ensure nuclear safety shall be provided. Analogously, the designer shall demonstrate that the safety principles, requirements and guidelines adopted for the design of the installation are adequately translated into safety options and further into design and operational specifications, to achieve a design that will be able to fulfil the safety functions and both meet the objectives and tend towards the goals.

2.3.2.3. Objectives of the volume 3 “design options and selected provisions and their justification against the objectives, goals, principles, requirements and guidelines”

The objective of the volume 3 of the DOPF is to show how the safety approach presented in volume 2 is implemented within the MYRRHA design (safety options, design and operational specifications, provisions) and to present the justification of the compliance / consistency of the design on one side versus the principles, requirements, guidelines and, on the other side, versus the goals and objectives.

Safety options and corresponding provisions shall cover all the probable plant conditions, including construction, operation, maintenance, waste management as well as the decommissioning of MYRRHA. Once the safety options are defined, the provisions should be selected and sized according to principles and guidelines presented within the Volume 2 to get close to the safety goals and to meet the safety objectives; such provisions are implemented within the safety architecture which is structured coherently with the principles of DiD: prevention, surveillance, control and consequences mitigation of all abnormal plant conditions.

An essential corollary to the justification is the proof of the feasibility of the safety demonstration in terms, for example, of available qualified tools (including codes and standards), adequate R&D support, adequate knowledge, skills and resources (cf. also §5).

2.3.2.4. Objectives of the volume 4 “Management system for safety of the installation”

The objective of Volume 4 of the DOPF is to present the management system in connexion to safety aspects of the installation during the project phase as well as during the operation of the installation. The designer, as well as the operator, shall ensure that the management system is compatible with the importance of the concerns raised by the installation and that it will be implemented and maintained for the planned operating conditions. To this end, the management system defines: the needed level of quality, the means to achieve and maintain this quality, the means to verify this achievement and maintenance and, finally, the means to analyse and resolve possible discrepancies.

2.3.2.5. Objectives of the volume 5 “security and safeguards integrated approach”

The objectives of the volume 5 of the DOPF are: to recall the security fundamentals, requirements and safeguards obligation; to present the detail of the implementation of the provisions important to security; to justify the categorization of the facility; to present the detail of all the security measures in respect with the categorization of the facility and the site specific DBT; to present information that allows Euratom to set the needed measures; to argue that the security measures taken don’t jeopardize the safety of the facility; to present the part of the management system dealing with security; to present the provisions taken to satisfy the safeguards obligation. In parallel, an adequate methodology should be presented to prove that, coherently with the WENRA objective O5, “*safety measures and security measures are designed and implemented in an integrated manner*”.

2.3.3. The concatenation among the DOPF volumes

Considering on one side the logic which is sketched within the figure 1 and, on the other side, the objectives for the different DOPF volumes, figure 2 shows the relationship with the content of these volumes and particularly the Volume 2, the Volume 3 and the Volume 5.

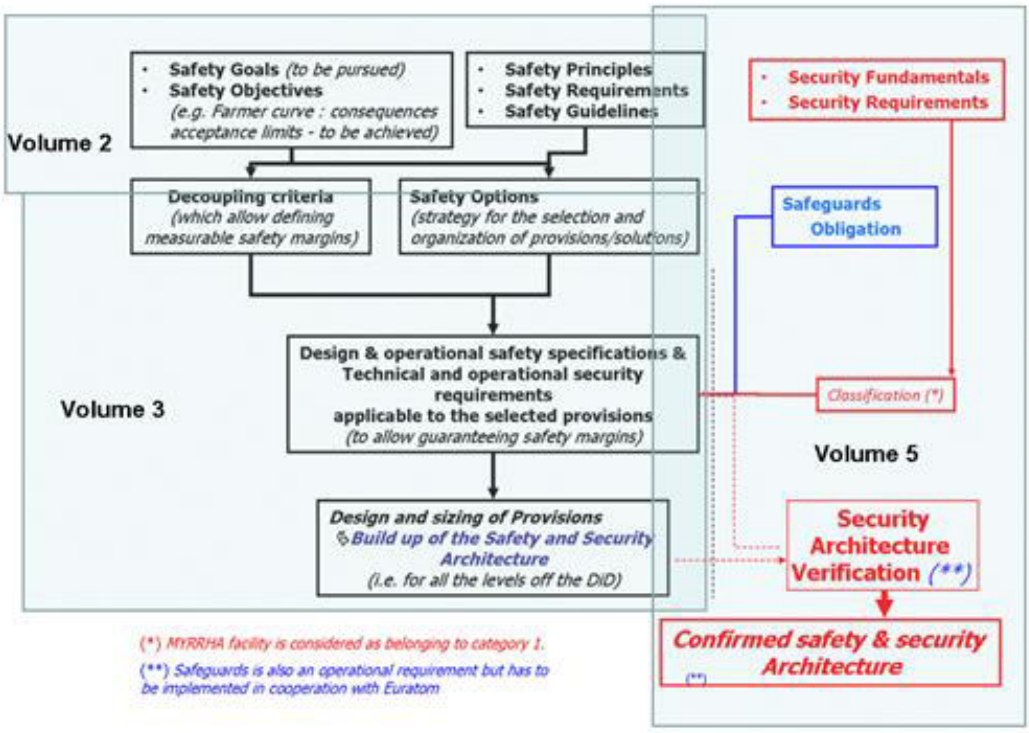

FIG. 2. Content and concatenation for the volumes 2, 3 and 5 of the DOPF.

2.4. Concluding remarks on the strategic note

The strategic note recalls the regulatory framework and presents the expected outline of the safety, security and safeguard philosophy to be presented by the designer during the "pre-licensing" phase. A way forward for the designer to show adherence to this Strategic Note is to present a DOPF which correspond to the different phases of the project as and when it progresses. Below, following the suggested template for the volumes 2 and 3, as they are presented within [4], the content and the expectations of these volumes are shortly discussed in order to stress the role of DiD.

3. VOLUME 2: APPROACH TO NUCLEAR SAFETY

3.1. Introduction

The content of Volume 2 focuses on methodologies and approaches while that of Volume 3 (cf. § 4) gives insights about the findings and results. The text below focuses more specifically on the DiD and its role within the general context for the design and the assessment of the safety architecture.

3.2. Approach and steps of the design process

3.2.1. Implementation of the principles of defence in depth

The designer is requested to describe his/her approach in relation to the DID principles and justifying this approach versus references which can be considered as representative of the state of the art in terms of reflections on this subject. The document issued by WENRA [12] is certainly among the most representative. The refined structure of the DID levels proposed by WENRA/RHWG is presented in Figure 3.

Figure 3 provides clues for several concerns that are important for the design and the assessment of innovative installations. First it shows a one to one correspondence between the third level of the DID and all events / situations without core melting, including both the "selected single initiating events" and the "selected multiple failure events". Similarly the Figure shows the correspondence between the fourth level and the "postulated core melt accidents". The proposal of WENRA/RHWG confirms that there is a direct relationship between the defence in depth and the "allowable risk domain" (column "Radiological consequences"). This relationship is essential for the designer who can so superpose the levels of defence in depth within the area of allowable risk, and simultaneously, to give explicit targets (success criteria, both in terms of performances and reliability) for these levels. These targets are essential to size the provisions that are associated with each level of the DID. This is perfectly coherent with the position expressed by the GIF/RSWG [13].

3.2.1.1. Structure and content of different levels of defence in depth

Following the logic shortly introduced within the previous section, the designer is requested to give insights – even if roughly described - about the way(s) for building the whole safety architecture of the installations in a manner that guarantees the compatibility with the principles of DID. The description should demonstrate that the selected approach will allow characterizing each level of DID: identifying the corresponding plant condition categories; defining the objectives of the DID level; identifying the means/provisions relied on to reach the objectives of the DID levels; defining de maximum expected radiological consequences (on the workers, the public and on the environment).

3.2.1.2. Approach to the design of the safety architecture to integrate defence in depth

As indicated by Figure 4, the design process for innovative systems should be iterative. For each of the fundamental safety functions (left side of Figure 4 – possibly developed in several sub functions if needed) the designer should identify possible challenges, as well as the mechanisms that can, given the characteristics of the installation, materialize these challenges. The next step is to identify provisions that should be implemented within the DID level to address these mechanisms (layer of provisions – IAEA terminology [6]), i.e. to control and minimize their consequences and to avoid further deterioration while ensuring the achievement and the keeping of a controlled and safe plant state. The iterations continue for each level of defence in depth by integrating, at each step, both specific initiating events and the additional possibility of failure introduced by the implementation of new provisions.

3.2.2. Categorization of the "plant conditions" or "plant states" used for the design

The designer shall select the methodology for the event categorization. Figure 5 shows the consistency between the methods suggested by the IAEA Glossary[2], by WENRA [12] and by the EUR [14] for the categorization of the "plant conditions" or "plant states" (i.e. the postulated initiating events) which are used for the design of the installation.

[2] IAEA Glossary Ed. 2007

Levels of defence in depth	Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)	Normal operation
Level 2	Control of abnormal operation and failures	Control and limiting systems and other surveillance features		Anticipated operational occurrences
Level 3 (1) 3.a	Control of accident to limit radiological releases and prevent escalation to core melt conditions (2)	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact (4)	Postulated single initiating events
3.b		Additional safety features(3), accident procedures		Postulated multiple failure events
Level 4	Control of accidents with core melt to limit off-site releases	Complementary safety features(3) to mitigate core melt, Management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off site radiological impact necessitating protective measures(5)	-

FIG. 3. WENRA / RHWG: Refined structure of the levels of did [12].

3.2.3. Stages of the design process

Finally the designer shall discuss its approach for the different stages of the design process which can be resumed as follows: definition, for each level of defence in depth, of quantitative objectives and goals of nuclear safety of the installation and radiation protection; for each level of defence in depth, identification of phenomena (challenges) and failure mechanisms (initiating events) for the safety functions; consideration of the internal and external hazards; categorization of initiating events and hazards retained for the design. The designer is invited to comment each of these stages and to present the corresponding engaged or planned efforts.

3.2.4. Principles for selecting design options and sizing provisions for the different levels of DID

The basic idea for this DOPF section is to provide insights about the methodology implemented by the designer to translate the goals and objectives of the various levels of the defence in depth, as well as generic principles, requirements and guidelines, first into safety design options and later - i.e., once selected the due solution/provision - into design and operational safety specifications/ criteria applicable to the design. The regulator should be able to appreciate how far safety is "*built in*" rather than *"added on"* (cf. [13], [15]). The section provides the list of generic and technology neutral requirements selected among those

available within the available references (IAEA, INSAG, others), applicable to improve the prevention, the surveillance, the accident management and the severe accident management for future installations; it should also present how the designer develops such requirements in order to obtain design and operational safety specifications.

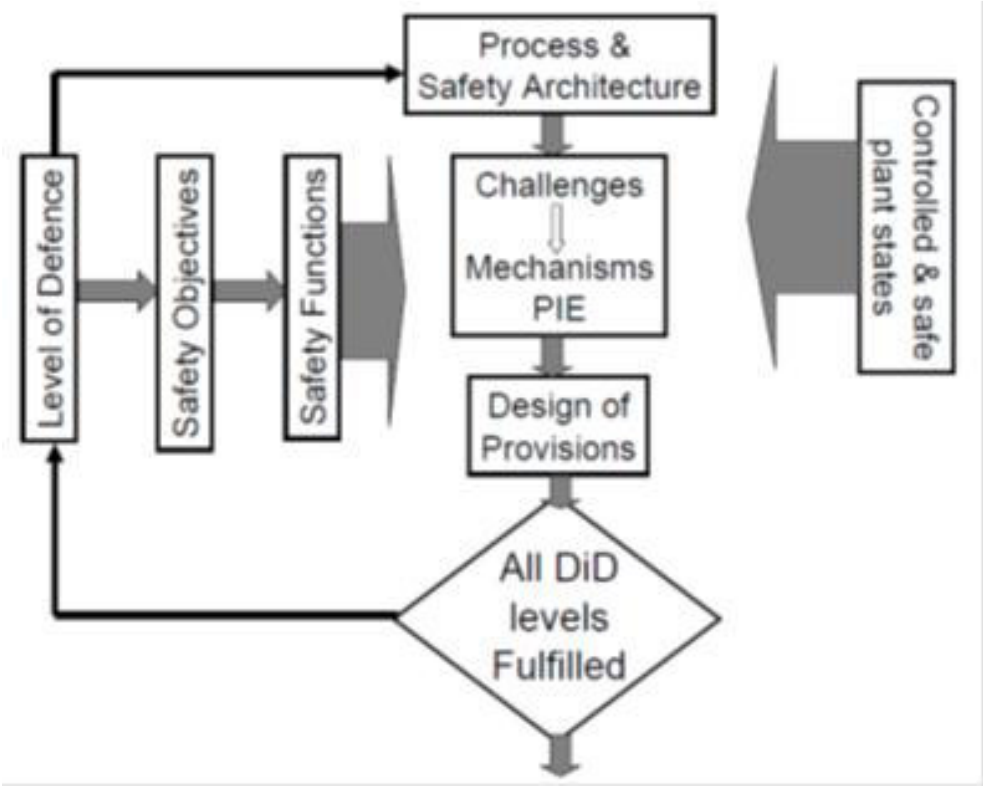

FIG. 4. Iterative process for the construction of the safety architecture [3].

IAEA Glossary	**Plant States**					
	Operational States		Accident Conditions			
			Within Design Basis Accidents		Beyond Design Basis Accident	
	Normal Operation	Anticipated Operational Occurrences	Accident conditions that are not Design Basis Accidents as explicitly considered but which are encompassed by them	Design basis Accidents	Beyond Design Basis Accidents without significant core degradation	Severe Accidents
WENRA Proposal	**Plant Conditions categories**					
	Normal Operation	Anticipated Operational Occurrences	DID Level 3a - Postulated Single Initiating Events		DID Level 3b - Selected Multiple Failures including possible failures or inefficiency of safety systems involved in DiD level 3a	Postulated Core Melt Accident (short and long term)
EUR	**Plant Conditions**					
	Design basis Categories				Design Extension Conditions	
	1st	2nd	3rd	4th		
	Normal Operation	Incidents	Accidents (low frequency)	Accidents (very low frequency)	Complex Sequences	Severe Accidents

FIG. 5. Possible categorization of the plant states.

3.2.5. Rules for plant operation

As for the previous section, the basic idea is to discuss how the content of the various levels of defence in depth is translated into design and operational safety specifications / criteria applicable to the selection of operating procedures for normal, abnormal as well as accidental conditions.

3.2.6. Crosscutting themes for the design

The designer is requested to present and comment his strategy on different safety related themes such as: *Classification of provisions important to safety; Consideration of the human factor; Consideration of Common Cause Failures; Reliability and availability of SSCs; Consideration of feedback experience; Consideration of maintenance conditions; Consideration of inadequate accessibility for testing and maintenance; Consideration of dismantling conditions; Consideration of the state of the art and R & D programs*.

3.3. Design and operational safety specifications and criteria for nuclear safety

The presentation of detailed design and operational safety specifications is not the primary purpose of the DOPF. Such request is only limited to most important safety relevant provisions (e.g. barriers) to illustrate and assess the feasibility/demonstration. In that context, the different parts of the installations (Reactor; Target/Window; Accelerator; Experimental devices) and their safety related characteristics shall be succinctly reviewed in order to indicate more precisely the risks and concerns which are raised by the different components, and how generic principles, requirements and guidelines are practically taken into account to address such risks and concerns. The DOPF section's subdivisions should provide the necessary preliminary information to indicate how these generic principles, requirements and guidelines adopted for the design of the installation are translated, with due consideration of the safety design options and the selected decoupling criteria, into design and operational safety specifications, or interpreted to select adequate criteria. The set of specifications and criteria will allow obtaining a design (through provisions) that, in turn, will be able to fulfill the safety functions and to meet the retained objectives.

3.4. The concept of safety architecture and the objective provision tree (OPT)

The safety architecture is the set of provisions/layers of provisions that are set-up by the designer to: ensure the achievement of tasks allocated to the process in satisfactory conditions of safety; prevent the degradation of the facility, i.e. the exceeding of operational limits; in case of failure: to restore and keep the facility in a safe shutdown condition for the short and long term. In practice, the guarantee of keeping in safe conditions corresponds to simultaneously achieving and satisfying the full set of safety functions.

The Objective Provision Tree (OPT) which is part of the Integrated Safety Assessment Methodology (ISAM) promoted by the GIF / RSWG [15] is a tool that can help in the iterative approach of definition / design of the safety architecture. The originality of the OPT, with regard to the conventional methods of representation of the safety architecture, lies on the fact that all the systems, independently of their nature (i.e. active or passive), as well as all the intrinsic characteristics or the procedures which participate to the achievement of the required safety function, are considered among the provisions and grouped, for each level of DiD, within the layers of provisions.

4. VOLUME 3: DESIGN OPTIONS AND SELECTED PROVISIONS AND THEIR JUSTIFICATION AGAINST THE OBJECTIVES, GOALS, PRINCIPLES, REQUIREMENTS AND GUIDELINES

4.1. Introduction

After having defined the methodologies within volume 2, the designer shall provide insights and findings about the preliminary results. The detailed objectives of the volume 3 of the DOPF can be summarized as follows: *To present the design options (with indication of possible corresponding provisions); To present the justification of the design options and selected provisions against the goals, objectives, principles, requirements and guidelines; To present the design and operational safety specifications for the most important safety relevant provisions; To present the feasibility of the safety analyses within the licensing phase.*

4.2. Design options and selected provisions for nuclear safety and radiation protection

The designer should start defining, for each safety function, challenges and mechanisms. The logic for the presentation within the DOPF could be: Safety function ⇨ Challenges ⇨ *Mechanisms*

4.3. Identification of initiating events and their categorization into "plant states"

The designer should detail the list of *Operating conditions*[3] ; *Accident conditions*; *Situations "practically eliminated"*, as well as the justification of the retained list of "*Plant states*"; the way to address internal and external hazards, should be presented within the DOPF.

4.4. Design options and selected provisions for nuclear safety

The DOPF should contain the descriptions of the design options selected to fulfil at the same time the principles of the DID and to address the challenges and mechanisms/initiating events identified and categorized for the different safety functions and the different levels of the defence in depth, as well as the considered hazards. Indications about the practical solutions (provisions) implemented within the safety architecture should be given when available. It has to be pointed out that the variety of conditions of operation for the installation could justify selecting specific strategies for the construction / organization of the safety architecture. If this is the case such specificities have to be described.

The presentation follows simultaneously the structure of defence in depth and the logic of the safety functions allowing succinctly presenting the skeleton and the rationale of the safety architecture. In this context, it is important to describe how independence is guaranteed between different levels of defence in depth. Also it is important to show how the provisions are protected vis-à-vis of the environmental conditions in which they are supposed to achieve their mission during the accidents. When describing the selected design options, the role of the operator should be systematically presented in order to appreciate the strategy adopted by the designer to manage the human factor. Design and operational safety specifications and criteria for the sizing of the most important safety relevant provisions are also presented. Similarly, insights should be provided on implementation of the principle of multiple

[3] See Glossary IAEA 2007

independent barriers for the main components of the installation; consideration of hazards; consideration of situations practically eliminated ; classification of provisions important to safety; interaction between provisions.

4.5. Design options and selected provisions for radiation protection

This DOPF section should present the design options and selected provisions (if available) to minimize the radiological impact on the workers, the public and the environment. The following items should be addressed: approach to radiation protection during normal operation; management of radioactive effluents and waste; options for the replacement and the repair; options to facilitate the dismantling.

4.6. Summary table of design options and design provisions

It is expected that, within the DOPF, a summary table will provide, for each safety function, information on the selected design option and provisions.

4.7. Justification of the design options and selected provisions against the goals, objectives, principles, requirements and guidelines (Safety Assessment[4])

As an essential contribution to the safety assessment, the DOPF should allow checking that the goals, objectives, principles, requirements and guidelines, as defined and presented by the designer within the Volume 2, are correctly translated into design and operational safety specifications in order to build the safety architecture. As matter of examples, the themes which allow addressing key principles, requirements and guidelines are provided as an indicative guideline – not necessarily exhaustive - for the preparation of the sections' content: *implementation of the Defence in Depth (DID); innovative provisions; classification of provisions important to safety; Codes and Standards; redundancy, diversification and physical separation; In service inspection (ISI) and the principles of maintenance; qualification of the safety provisions; system/provisions interactions; radiological consequences.*

The DOPF should present the preliminary safety studies which anticipate the full scope safety analysis. The scope and level of detail of the preliminary safety studies should increase as the design program progresses so that the studies reflect the status of the plant design (cf. §5).

4.8. Design and operational safety specifications

This DOPF should provide the details concerning the design and operational safety specifications and criteria applicable for the safety and radiation protection aspects for the most relevant safety provisions of the installation. Safety and radiation protection aspects will be presented for the Reactor, the Target/Window, the Accelerator, and the Experimental devices.

[4] Cf. the definition of Safety assessment within the IAEA No. NS-G-1.2

4.9. Feasibility of safety analyses during the licensing phase

An essential aspect for the justification of design options and corresponding provisions is related to the availability of an adequate support to conduct, during the licensing phase, a comprehensive safety analysis. This support can be expressed and commented within the DOPF in terms of: availability of selected equipment / technologies / materials; appropriate degree of verification and qualification of codes and methodologies; availability of human and financial resources.

5. DETERMINISTIC SAFETY DEMONSTRATION

The safety demonstration, whose premises have to be presented within the DOPF volume 3, covers [12]: Events considered occurring and consequences considered in the design; Events which have to be practically eliminated, as they would lead to large or early radioactive release.

5.1. Events considered to occur and consequences considered in the design

The safety analysis, as part of the safety assessment, should proceed in parallel with the design process, with iteration between the two activities. The scope and level of detail of the safety analysis should increase as the design process progresses, so that the final safety analysis reflects the final design of the reactor as constructed.

5.1.1. Analysis of postulated single initiating events

The postulated single initiating events are those corresponding to the DiD Level 3.a (cf. Table1). The associated radiological consequences shall meet safety objective O2 of WENRA. The response of the research reactor to the postulated initiating event should be predicted by conservative deterministic safety analyses.

5.1.2. Analysis of postulated multiple failure events without core melt

The postulated multiple failure events addressed in this section are those corresponding to the DID Level 3.b (cf. Table1). The associated radiological consequences shall meet safety objective O2 of WENRA. The response of the research reactor to the postulated multiple failure events may be predicted by a best estimate plus uncertainty safety analyses.

5.1.3. Analysis of core melt accidents

The postulated “core melt” accidents addressed in this section are those corresponding to the DID Level 4 (cf. Figure 3). The associated radiological consequences shall meet safety objective O3 of WENRA. The response of the research reactor to the “core melt” accidents may be predicted by a best estimate plus uncertainty safety analyses.

5.2. Events which have to be practically eliminated, as would lead to large or early radioactive release

Initiators, consequential faults, fuel melt sequences challenging the confinement resulting in accidental situations with a large or early release could be rejected and excluded from further analysis of radiological consequences provided that an acceptable justification is given by the designer to the regulatory authority. An acceptable justification is to demonstrate

that any accident sequence with a large or early release is practically eliminated, i.e. if it is physically impossible for the accident sequence to occur or if the accident sequence can be considered with a high degree of confidence to be extremely unlikely to arise.

In order to quantify the notion of "extremely unlikely" it is important to give insights concerning the order of magnitude of acceptable reliability for the different upstream DiD levels. The residual risk of having early and large releases should be pushed to very low probabilities being aware that the demonstration cannot be claimed solely based on compliance with a general cut-off probabilistic value. Because of the existence of unpredictable common mode failures there is a limit to the reliability that can be allocated to the layers of provisions which materialize the DID levels. Other criteria will be considered as for example the simplicity of the safety architecture or the demonstrated degree of knowledge for the phenomena involved in the accident sequence. The final assessment will be done on a case by case basis.

6. CONCLUSIONS

The Belgian Federal Agency for Nuclear Control (FANC) is engaged in a process of pre-licensing for the experimental reactor MYRRHA. The regulatory framework applicable for the implementation of this project is described by FANC in a Strategic Note. The steps required to design a basic nuclear installation and to ensure compliance with the requirements of nuclear safety, security and safeguards are described and commented within a complementary document which present the template of a Design Options and Provision File (DOPF) which shall be prepared by the designer to engage the exchanges with the regulator.

The DID represents a pillar for both Strategic Note and the DOPF template. The two documents focus more specifically on aspects relating to refinements in the concept of DID and on practices for their integration in the process of design / assessment of the MYRRHA reactor.

REFERENCES

[1] MYRRHA: Multi-purpose Hybrid Research Reactor for High-tech Applications, http://myrrha.sckcen.be/

[2] FANC, 2011-04-09-MSC-5-3-2-FR, Description d'un processus de pre-licensing pour un projet de construction d'une installation nucléaire nouvelle et complexe, Révision 1.

[3] HAKIMI, N., MYRRHA Strategic Note, AFCN 2011-10-13-NH-5-4-3-EN, Revision 2.

[4] FIORINI, G.L., Guidance for the format and content of the Design Options and Provisions File, AFCN 2011-10-12-NH-5-4-3-EN, Revision 1.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards, Safety Requirements No. NS-R-4, IAEA, Vienna (2005).

[8] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), WENRA Reactor Safety Reference Levels, January (2008).

[9] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), WENRA Statement on Safety Objectives for New Nuclear Power Plants, November (2010)

[10] US DEPARTMENT OF ENERGY (DOE), A Technology Roadmap for Generation IV Nuclear Energy Systems, GIF-002-00, USDOE, Washington (2002).
[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Facilities, IAEA Nuclear Security Series No. 13, INFCIRC/225/revision 5, IAEA, Vienna (2011).
[12] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), WENRA Booklet: Safety of New NPP Designs, October (2012).
[13] GENERATION IV INTERNATIONAL FORUM (GIF), Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems, GIF/RSWG/2007/002 Revision 1, November (2008).
[14] EUROPEAN UTILITY REQUIREMENTS for LWR Nuclear Power Plants, Revision C, April (2001). http://www.europeanutilityrequirements.org/
[15] GENERATION IV INTERNATIONAL FORUM (GIF), An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems, GIF - Risk and Safety Working Group (RSWG), Version 1.1, June (2011).

REINFORCEMENT OF DEFENCE-IN-DEPTH: MODIFICATION PRACTICE AFTER THE FUKUSHIMA NUCLEAR ACCIDENT

Y. WANG, H. TANG, Q. MAO
China Nuclear Power Design Co., Ltd
Xia Meilin, Futian District,
Shenzhen, Guangdong Province, P.R.C.
E-mail: wangyuhong@cgnpc.com.cn

Abstract

The Fukushima Daiichi nuclear accident revealed the importance and demand for further reinforcement of defence-in-depth. CGN (China General Nuclear Power Group) has made a complete safety assessment on CPR1000 nuclear power plants under construction in China. Dozens of modifications have been implemented based on the assessment findings and lessons learned from Fukushima nuclear accident, taking into account of PSA (Probabilistic Safety Analysis) and comparison analysis of the latest regulations and standards. These modifications help to enhance nuclear safety significantly for nuclear power plants under construction in China, and provide helpful modification guidance for nuclear power plants in operation of the same type.

1. INTRODUCTION

On March 11, 2011, under the combined effect of earthquake and tsunami, a severe nuclear accident occurred in Fukushima Daiichi nuclear power plant and large radioactive substances were released into the environment. Soon after that, China National Nuclear Safety Administration (NNSA) organized a comprehensive safety inspection of all the nuclear power plants in operation and under construction in China and issued a *General Technical Requirements for Improvement Actions after Fukushima Accident (for trial use)* as a guidance for the modification of nuclear power plants. Meanwhile, according to China's current nuclear safety laws and regulations, as well as the international advanced nuclear safety standards and the lessons learned from Fukushima accident, NNSA issued *The 12th Five-Year Plan and 2020 Vision for Nuclear Safety and Radiation Prevention* and *Safety Requirements for Nuclear Power Plants to Be Built During the 12th Five Years (draft for comments)*.

These requirements highlight the defence-in-depth measures from several aspects, such as plant site safety, plant response to extreme external events, guarantee of safety function (emergency power/water supply), prevention and mitigation of severe accidents, radiation protection, and environment impact evaluation, etc. It is required that new power plants adopt adequate provisions to prevent and mitigate severe accidents. The core damage frequency (CDF) should be less than 1.0E-5/yr and large release frequency (LRF) should be less than 1.0E-6/yr.

Based upon CPR1000, dozens of modifications were studied and conducted resulting from systematic PSA and the latest regulations and standards, as well as the lessons from Fukushima accident. The scheme is called ACPR1000 technology.

ACPR1000 technology focuses on several aspects, such as protection against extreme external accident (earthquake and floods, etc.), severe accident prevention and mitigation, environment monitoring and emergency response, etc. After implementing these modifications, the CDF and LRF target are achieved. ACPR1000 has adequate provisions to prevent and mitigate severe accidents, and thus the safety and reliability are remarkably improved. In addition, this technology provides helpful improvement guidance for nuclear plants in operation and under construction.

2. MODIFICATION APPROACH

2.1. Lessons learned from the Fukushima accident

After the Fukushima accident, according to NNSA new requirements, a series of inspections, evaluations and reviews were carried out, such as external events impacts on the siting of CPR1000 nuclear power plant, prevention and mitigation of (combined) extreme natural events, response to site black out (SBO) and loss of ultimate heat sink, prevention and mitigation of severe accidents, environment monitoring and emergency response systems, etc. On the findings of these inspection, evaluation and reviews, combined with *General Technical Requirements for Improvement Actions after Fukushima Accident (for trial use)* issued by NNSA, the post-Fukushima-accident modifications were formed.

2.2. Probabilistic safety analysis

In order to improve the safety of CPR1000 nuclear power plant and lower the CDF and LRF, PSA method is employed to identify the dominant accident sequences that significantly contribute to the core damage and large release of radioactive substances and find out the weaknesses of CPR1000 nuclear power plants. Some important improvement measures were put forward.

2.3. Comparison and analysis of latest regulations and standards

Through the comparison and analysis of China's latest regulations and standards such as *the Safety Requirements for Nuclear Power Plants to Be Built During the 12th Five Years (draft for comments)*, IAEA latest safety requirements and guides, EUR/URD general safety requirements and requirements proposed by other international organizations, several modifications were proposed especially with regard to the prevention and mitigation of severe accidents. Through above actions and other references, a batch of modifications was put forward.

In terms of the levels of defence-in-depth, these modifications reinforced the fourth and fifth levels of defence, particularly the capability of prevention and mitigating functions of the severe accidents in the fourth level. This is consistent with the experience feedback from Fukushima and the latest regulations and standards.

3. OVERALL DESIGN SCHEME

On the basis of present CPR1000 NPP, together with lessons from Fukushima nuclear accident, PSA, and comparison analysis with the latest regulations and standards, ACPR1000 is improved in the aspects of defence against extreme external events (earthquake and floods), strengthening safety functions (cooling and power supply), prevention and mitigation of severe accidents, environment monitoring and emergency response, and emergency cooling of spent fuel pool, etc., according to the safety principle of defence-in-depth. Meanwhile, operation and management procedures have been revised to avoid any weaknesses in design and management through supplementary analyses, thus plant safety is further enhanced.

3.1. Enhancement of prevention against beyond-design-basis external events

Based on the experience feedback from Fukushima nuclear accident and defence-in-depth principles, ACPR1000 has strengthened its prevention capability against extreme

external events through improvements of protection against beyond-design-basis earthquake and floods.

3.1.1. Prevention against beyond-design-basis earthquake

Prevention capability against beyond-design-basis earthquake is strengthened through upgrading seismic margin of reactor coolant system. Weaknesses have been found and modified through seismic margin analysis (SMA). Detailed earthquake PSA is conducted.

3.1.2. Prevention against beyond-design-basis floods

As for the beyond-design-basis floods prevention, the combination of design basis flood (DBF) and the beyond design 1000-year rainfall has been taken into account so as to assure NI building, Pump Station and Diesel Generator building not be flooded under such condition.

3.2. Strengthening power supply capability under beyond-design-basis condition

ACPR1000 takes several measures to improve power supply based on defence-in-depth principles. In addition to normal and emergency power for design basis conditions, several types of backup power sources and batteries are taken into account and designed, thus assuring the necessary and reliable power for beyond-design-basis accident monitoring and mitigation.

3.3. Strengthening cooling capability under beyond-design-basis condition

Based on defence-in-depth principles, ACPR1000 takes several measures to strengthen cooling capability. In addition to normal and emergency water makeup under design basis conditions, temporary water makeup functions are also taken into account in case of failure of normal and emergency water makeup, thus assuring that there's adequate water to cool reactor core either from primary or secondary side. Meanwhile, a diverse heat sink system is designed to prevent the loss of ultimate heat sink.

3.4. Strengthening capability of preventing and mitigating severe accidents

In addition to the improved capability of power supply and cooling under beyond-design-basis conditions as mentioned above, ACPR1000 further strengthens capability of preventing and mitigating severe accidents, by means of modifications such as passive shaft seal of reactor coolant pumps, relief valves specific for severe accidents, diverse actuation system, safety injection pumps (LHSI) and containment spray pumps backup, reactor pit flooding, etc. These modifications improved the safety of the reactor core and the integrity of containment in severe accidents.

3.5. Improving environment monitoring and emergency capability under circumstances of accidents

Based on feedback from Fukushima nuclear accident, ACPR1000 implemented several modifications on emergency response and environment monitoring by reinforcing the capability of environment emergency monitoring and multi-unit emergency disposal. The

design basis is enhanced for emergency command center to assure its availability and habitability even in case of extreme external events.

3.6. Enhancing emergency cooling capability of spent fuel pool

According to experience feedback from Fukushima nuclear accident, the safety of spent fuel pool, as an important part of NPP safety, should be highlighted. ACPR1000 enhanced emergency cooling capacity of spent fuel pool on such aspects as : (i) improving the monitoring of temperature and water level of spent fuel pool; (ii) temporary refilling of spent fuel pool; and, (iii) adding mid- and long- term heat removal system after spent fuel pool accident, etc. These modifications enhanced the safety of spent fuel pool.

3.7. Supplementary analyses

In addition to the modifications mentioned above, ACPR1000 also carried out seismic margin analysis, full scope accidents analysis, full scope probabilistic safety analysis and availability and accessibility analysis of equipments in severe accidents, as well as the development of full scope severe accident management guidance. Modifications are conducted and accident management procedures are modified after weaknesses were found in design by these supplementary analyses.

4. CONCLUSIONS

The Fukushima Daiichi nuclear accident revealed the importance and demand for further reinforcement of defence-in-depth. CGN has made a comprehensive safety assessment on present CPR1000 nuclear power plants under construction in China. Dozens of modifications were studied and conducted.

These modifications, employing PSA risk-informed approach, reinforce the capacity of defence-in-depth on following aspects:

i. protection against extreme external events (flooding, earthquake or other hazards combination);
ii. guarantee of the effectiveness of safety function (especially for cold chain and power);
iii. the prevention and mitigation of severe accidents; and
iv. the improvement and complement of environment monitoring and emergency response system.

Meanwhile, the independence and diversity requirements for safety precautions are considered under different defence levels and conditions.

These modifications reinforce the fourth and fifth level of defence and enhance significantly the safety of nuclear power plants. The total CDF is less than 1.0E-5/yr and LRF less than 1.0E-6/yr. The provisions for prevention and mitigation of severe accidents are adequate. The modifications, based on CPR1000, which is under construction in China, act as a helpful guidance for the nuclear power plants of the same type under construction and in operation.

REFERENCES

[1] CHINA NATIONAL NUCLEAR SAFETY ADMINISTRATION (NNSA), General Technical Requirements for Improvement Actions after Fukushima Accident, NNSA (2012).

[2] CHINA NATIONAL NUCLEAR SAFETY ADMINISTRATION (NNSA), The 12th Five-Year Plan and 2020 Vision for Nuclear Safety and Radiation Prevention, NNSA, October (2012).

[3] CHINA NATIONAL NUCLEAR SAFETY ADMINISTRATION (NNSA), Safety Requirements for Nuclear Power Plants to Be Built During the 12th Five Years (draft for comments), NNSA, May (2013).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

[5] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), Safety of New NPP Designs, WENRA Reactor Harmonization Working Group, October (2012).

[6] CHINA NUCLEAR POWER DESIGN CO., LTD (SHENZHEN) AND NUCLEAR AND RADIATION SAFETY CENTER, Joint Research Report on ACPR1000 Standard Design, June (2013).

SUCCESSIVE EVOLUTIONS OF THE DEFENCE IN DEPTH CONCEPT

B. POULAT
International Atomic Energy Agency (IAEA), Department of Nuclear Safety and Security,
Wagramer Strasse 5, P.O. Box 100, 1400 Vienna, Austria
E-mail: B.Poulat@iaea.org

Abstract

Following Fukushima Daiichi accident, the Defence-in-depth concept, which is usually defined as a combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused, has been confirmed as an essential element to be applied in the design of a nuclear facility to protect people and the environment. However, and although the implementation of the defence in depth concept had been required for long, the Fukushima Daiichi accident and the "stress tests" conducted in different countries have revealed deficiencies in its implementation. Consequently within the review of the IAEA safety requirements requested by Member states, it was important to check whether this concept was appropriately defined in order to be properly understood and fully implemented by vendors and operating organizations. By screening the successive definitions of the defence in depth principle and concept, this paper emphasizes the few issues which have been gradually clarified and enhanced to ensure effectiveness of the defence in depth as expressed from its original statement.

1. INTRODUCTION

The Fukushima Daiichi accident was characterized by multiple failures in the safety systems resulting in a total loss of the decay heat removal systems at three units leading quickly to significant core damage, and then to large radiological releases both at the site and off the site due to failures in the confinement function. Even though the tsunami wave was exceptionally high, the likelihood of such a phenomenon was not totally unknown for this region and this accident inevitably raised the question whether some requirements for site hazard characterization and design of the plant were missed or incomplete. Consequently a review of the IAEA safety requirements was requested by Member states during the Ministerial Conference held in June 2011 and introduced in the draft Action Plan endorsed by the General Conference held in September 2011.

Following the Chernobyl accident the Defence in Depth concept was defined and recognized as fundamental to the safety of nuclear facilities and was considered as the overarching principle of nuclear safety. Although following Fukushima Daiichi accident it has been reaffirmed without ambiguity that this principle shall remain fundamental for the protection of people and the environment from harmful effects of ionizing radiation, it is of great importance to check whether this concept was appropriately defined in order to be properly understood and fully implemented by Vendors and Operating organizations. Indeed, if the basic principle, with all its implications for designing, manufacturing, constructing and operating nuclear plants as originally stated in Basic Safety Principles for Nuclear Power plants[1] [1] had been correctly understood and applied such large radiological releases should not have occurred at Fukushima Daiichi plant.

Later in 1996, INSAG-10 publication "Defence in Depth in Nuclear Safety" [2] and a few years after the IAEA Requirement Document NS-R-1 "Safety of Nuclear Power Plants: Design" [3] were published to clarify the objectives allocated to the consecutive levels and the expectations for a correct implementation of the concept. These two documents supplemented by IAEA Safety Standard SSR-2/1 [4] superseding NS-R-1, and proposals for amendments considered after Fukushima Daiichi accident constitute the basis for this analysis.

[1] INSAG -3: "All safety activities, whether organizational, behavioural, or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large…"

The concept of defence in depth cannot be understood as and limited to the request for the implementation of a number of consecutive barriers and levels, and any other requirement necessary to achieve the quality and reliability expected for the barriers and for systems ensuring their integrity shall be considered as part of the concept. Vulnerabilities for common cause failures, aptitude of system and equipment to accomplish its intended function under accident conditions, robustness and avoidance of cliff edge effect, and independence between the different levels need particular attention and are key issues to reinforce the overall efficiency of the defence in depth concept and consequently prevention of accidents having harmful consequences for the public and environment.

Design of Instrumentation and Control systems (I&C), namely its vital attributes such as single failure criterion, redundancy, independence, and diversity plays an important role in defence in depth strategy of nuclear power plant. Due to a large number of communications among the I&C safety divisions and I&C systems, particular attention should be paid to the identification and elimination of vulnerabilities for common cause failures. Consequently, an appropriate use of independence and diversity is now largely expected in design of I&C systems to justify that the defence in depth strategy would not be jeopardized by the propagation of a failure.

2. DEFENCE IN DEPTH: DEFINITIONS AND OBJECTIVES

A defence in depth strategy has been recognized as a fundamental principle to keep the likelihood of an accident having harmful consequences extremely low, which should be applied to all safety activities, whether organizational, behavioural or design related. Its application leads to implement layers of overlapping provisions so that if a failure should occur it would be compensated for or corrected. When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of defence in depth [5].

For nuclear power plants, even if the original concept on how to apply the defence in depth strategy has been successively extended and strengthened, the basic concept, asking to implement several confinement barriers in series between radioactive materials and workers/public or environment and a number of consecutive levels to ensure the appropriate effectiveness of these barriers under normal and accident conditions, remained unchanged [1-4, 6].

For nuclear power plants, the historical development of the concept of defence in depth quickly converged to a general structure of four physical barriers (fuel matrix, fuel rod cladding, Primary coolant boundary and confinement), and five consecutive levels where the first four levels were oriented towards the protection of barriers and mitigation of radiological releases by maintaining in accident conditions the three fundamental safety functions (reactivity control, decay heat removal and confinement of radioactive materials), and the fifth level was related to off-site emergency measures to protect the public in the event of a significant release [1, 6].

The successive evolutions of the concept described in [2], [3], [4] cannot constitute an excuse for an incorrect or incomplete application but must be considered either as a clarification of the formulation of existing requirements, or needs for a continuous improvement of nuclear safety by considering lessons learned from accidents, operation feedback and outcomes of probabilistic safety analyses. Indeed, continuous improvement of

safety is a design principle commonly agreed by Member States and widely applied in the design of new builds.

Already in 1988, both INSAG 3 and IAEA Safety Series 50-C-D documents emphasized importance of prevention and mitigation of accidents, particularly those which could cause severe core damage or significant radiological releases, stating that irrespective of design provisions implemented at the first three levels, accident conditions exceeding the design basis conditions could not be excluded and should be considered even though they were of low probability. So, such unlikely conditions were requested to be considered for the protection of the public and site personnel by specific complementary plant features to mitigate their consequences (accident management) and substantially to reduce the effects on the public and the environment of the release of radioactive materials (plans for emergency preparedness).

As effectiveness of defence in depth strategy relies on the integrity of the barriers, the concept included protection of the barriers by averting damage to the barriers themselves but also to the systems requested for the mitigation of accidents. The whole concept defined by these two documents was further clarified with the publication of INSAG 10 document (1996) and IAEA Requirements NS-R-1 in which the associated expectations or requirements were detailed.

Figure 1 provides an overview of the defence in depth concept [2] where:

- Level 1 aims to prevent deviations from normal operation and equipment/system failures. Level 1 provides the initial basis for protection against external and internal hazards.
- Level 2 aims to detect and intercept deviations from normal operation in order to prevent anticipated operational occurrences from escalating to accident conditions.
- Level 3 is the control of postulated design basis accidents within design basis conditions with the objective to prevent core damage.
- Level 4 is defined as the control of severe conditions in which conditions caused by design basis accidents may be exceeded with the objective to ensure that the likelihood of such accident and the magnitude of radioactive materials are both kept as low as reasonably achievable.
- Level 5 is defined as the mitigation of the radiological consequences of significant external releases of radioactive materials, and requires the provision of adequately equipped emergency facilities and plans for the on-site and off-site emergency response.

The INSAG 10 document already emphasized the necessity to pay attention to plant conditions caused by multiple failures such as the complete loss of all redundancies of a same safety system or by extremely unlikely external hazard such as a severe flood.

As level 4 was defined to mitigate to the extent possible the consequences of any severe accident, consideration was given to all the existing plant capabilities including the possible use of some systems beyond their originally intended functions and design basis, and the use of non-permanent systems or equipment.

Levels of defence in depth	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

FIG. 1. Overview of defence in depth concept as defined in INSAG 10 [2].

3. IAEA SSR-2/1 SPECIFIC REQUIREMENT: REINFORCEMENT OF DEFENCE IN DEPTH CONCEPT

With the publication of SSR-2/1 document addressing the specific safety requirements for the design of a nuclear power plant, the philosophy of the Defence in depth was not modified but the concept was reinforced to match the new objectives given by SSR-2/1 Requirements in terms of radioactive releases:

- Any sequence which could lead to high radiation doses or large radioactive releases shall be practically eliminated, and that there are no, or only minor potential radiological consequences for plant states with a significant likelihood of occurrence (SSR-2/1 Requirement 5, item 4.3).
- A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological impacts, on or off the site, and do not necessitate any off-site intervention measures (SSR-2/1 Requirement 19, item 5.25),
- For design extension conditions, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures (SSR-2/1 Requirement 20, item 5.31).

Level 4 has also been reinforced by enhancing the design requirements applicable to the means necessary to prevent severe accidents and to mitigate the consequences to make prevention and mitigation of such accidents more reliable taking into account that the consequences of their failures in case of demand would lead to large releases and

consequently to a long term off-site contamination. The relevant requirements are given in (SSR-2/1 Requirement 20 and associated items):

- First, initiating events or sequences of events which might exceed conditions caused by the design basis accidents shall be considered for the design of the plant unless their practical elimination by design be provided,
- SSCs implemented for prevention and migration of such conditions shall be independent, to the extent practicable, of those used in more frequent accidents,
- Conditions caused by these events or sequences of events shall be assessed and used to define the design basis of the SSCs necessary for mitigating their consequences. The assessment may be made using less conservative rules and less penalizing conditions than those required for the assessment of the conditions caused by the design basis accidents, but appropriate margins to avoid cliff edge effects are nevertheless requested. Demonstration that the mitigation of the consequences would be possible by crediting those SSCs only is requested.

The requirements established in SSR-2/1 primarily apply to new builds and might not be fully met at some existing nuclear power plants that were built to earlier standards. The extent to which the SSR-2/1 requirements are to be applied to existing plants is a decision for individual States. In particular, for existing plants the accident management of situations not explicitly considered in the original design might take use of non-permanent equipment, available at the site or not, provided the grace period before unacceptable consequences is sufficient for the installation of this non-permanent equipment. Nevertheless, accident management measures should not be used as an excuse not to install to the extent practicable permanent complementary equipment for both preventing progression of the accident and mitigating their consequences by limiting the radioactive release.

However, and although the Defence in depth concept with five consecutive levels was clearly defined in INSAG 10 document (1996) and its application required by the IAEA Requirements NS-R-1 (2000), the Fukushima Daii-chi accident and the "stress tests" conducted in different countries have revealed some deficiencies in its implementation. Consequently, the IAEA Secretariat was requested by the General Conference, held in September 2011, to review and to revise as necessary the IAEA Safety Standards in the light of the analysis of the Fukushima Daiichi accident.

For SSR 2/1 requirements, even if all the causes of the Fukushima Dai-ichi accident may not have not been identified yet, the following issues have already been identified as relevant and essential for the safety of nuclear plants and should be considered when designing new builds or re-assessing the design of existing plant:

- As external hazards can impair all the levels of defence, a correct site hazard characterization is of first importance for the design of a plant which should be such that any external hazard defined for design could not lead to the total loss of a system intended to accomplish one of the fundamental safety functions, (INSAG 10, 2.4 "levels of defence", item 36 : *Level 1 provides the initial basis for protection against external and internal hazards (earthquakes, aircraft crashes, blast waves, fire, flooding) even though some additional protection may be required at higher levels of defence*),
- Design of SSCs important to safety should provide adequate margins to cope with hazards and internal events causing loads exceeding those strictly considered for the design (derived from INSAG 10 "Basic prerequisites". *An effective implementation of defence in depth has some prerequisites which apply to all measures at all the levels. Appropriate conservatism* is one of these prerequisites).

Margins are needed to avoid a cliff edge effect in case of a small deviation in a plant parameters (SSR-2/1 Req. 17, item 4.11), and their magnitudes should generally be commensurate with the safety significance of the SSC. The magnitude of margins is determined by applying design rules and methodologies of different grades of conservatism (e.g. rules for design extension conditions may be less conservative than those used for the design basis accidents) and by considering number of uncertainties. Nevertheless, the Secretariat recognizes that there is a need for harmonizing the approach to defining and assessing margins. The Secretariat has undertaken activities to prepare a report on the technical basis for an expanded definition of margins.

- Any design should include provisions (complementary equipment, procedures, connections for non-permanent equipment) to facilitate the accident management of situations exceeding those originally considered.
  The relevant provisions should be identified and installed by assessing the timely response of the plant in the event of such situations.

Recently nature has shown us at various sites how much devastating natural phenomena could be, and taking into account the difficulty to predict the intensity of future natural hazards, some Contracting Parties have expressed during the 2nd extraordinary Convention on Nuclear Safety the idea to enhance in some areas the resistance of nuclear plants with regard to such extreme and unexpected natural hazards with the objective to avoid unacceptable consequences for the public, the environment and the society should such hazards occur. In this perspective, the set of structures and systems necessary to avoid unacceptable consequences which may be different from site to site and from one type of reactor to another should be identified first.

In conclusion in the frame of the review and revision of the SSR-2/1 requirement document, the IAEA Secretariat is proposing to the Member States to make more explicit some existing requirements and to add a few new requirements to strengthen the overall effectiveness of the defence in depth concept with the objective to make the likelihood of an accident having harmful consequences extremely low.

- A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological impacts, on or off the site, and do not necessitate any off-site intervention measures.
- For design extension conditions, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.
- Any sequence which could lead to high radiation doses or significant radioactive releases shall be practically eliminated. With the objective to practically eliminate high doses and releases, for reactors having a water pool system for spent fuel storage, the design shall include the necessary capabilities to prevent the uncovering of the fuel assemblies.
- Independence among the consecutive levels of defense shall be implemented as far as reasonably practicable with a particular attention for levels three and four because of the enhanced severity of overall consequences if failures of these two levels occur simultaneously.
- Design of systems and structures ultimately necessary to prevent early and large radioactive releases shall provide for significant margins to accommodate with external hazards of a severity or duration exceeding those considered in their definitions.

- To facilitate the accident management of situations not considered in the original design of the plant, appropriate and necessary features enabling the use of non-permanent equipment or power sources should be installed with the objective to avoid large releases and long term off-site contamination.

4. DEFENCE IN DEPTH CONCEPT: EFFECTIVE INDEPENDENCE OF THE CONSECUTIVE LEVELS

Although the independent effectiveness of the different levels of defence is a necessary element of defence in depth, independence of the redundancies of a safety system within the same level of defence is also necessary and has to be considered for the evaluation of the overall effectiveness of the defence in depth strategy. Indeed, the independence of the redundancies is a necessary element of the design of the safety systems for which a high reliability is requested, and the existence of a number of consecutive levels with an adequate independence among them cannot be an excuse to decrease the robustness of each level.

While independence between redundancies of a safety system was early understood and correctly applied in most of the reactors, independence between levels was less implemented certainly because of a lack of clarity in the expression of the requirement itself. By relying on a defence in depth strategy to prevent accidents with harmful consequences it is expected that should one level fail the subsequent level comes into play which makes sense, and therefore an adequate independence between the two levels is requested. Independence requirement was later explicitly expressed in SSR-2/1 stating “the levels of defence should be independent as far as is practicable” which left flexibility in the application.

Nevertheless taking into account that an ideal design where individual SSCs are allocated to a single defence in depth level is unrealistic in the view of designers, and could lead to excessive complexity of the design; how far independence must be implemented is not crystal clear for Member States. Nevertheless the following formulation already discussed with the NUSSC Members could be considered as an input to go further in the clarification of the independence requirements and associated expectations:

- The ability of SSCs should not be affected by the initiating event and its consequences for which they are designed to respond,
- The independent effectiveness of the different levels of defence is a necessary element of defence in depth, and is achieved by incorporating measures to avoid, as far as reasonably practicable, the failure of one level causing the failure of other levels involved in the mitigation of the event,
- Complementary safety features, designed to back up SSCs implementing safety functions, should be independent from SSCs postulated as failed in the sequence,
- Complementary safety features specifically designed to mitigate the consequences of a core melt accident should be independent from the SSCs designed for more frequent accidents.

5. COMMON CAUSE FAILURE (CCF), INDEPENDENCE AND DIVERSITY

Making the likelihood of an accident having harmful consequences extremely low cannot be achieved without any consideration of vulnerabilities for common cause failures among the consecutive levels with the goal of their elimination from the design to a reasonable extent.

A common cause failure is defined as the failure of two or more structures, systems or components due to a single event or cause.

CCF may be initiated by the propagation of the effects of an external or internal hazard to different SSCs, by the propagation of a failure originating in one system to other systems, or by unpredictable latent fault in design, manufacturing, or human errors which may cause the coincidental failure of several equipment, channels or systems when triggered by a specific event. Consequently physical separation, independence and diversity are generally implemented by designers to decrease the likelihood of failure by common cause. While physical separation and independence are effective to prevent the propagation of the effects of a hazard or the propagation of a failure, diversity is more appropriate to eliminate latent faults.

CCF to be considered for design can be identified by either probabilistic or deterministic approaches. The likelihood of the combination formed by the initiating event and the common cause failure might be nevertheless considered when the deterministic approach is preferred. Moreover, its elimination is usually not requested in so far as the consequences do not exceed those accepted for accidents caused by multiple failures. If exceeded, decision should be made to implement complementary safety features unlikely to be subjected to the same common cause failure.

Such principles are generally applied to define the needs of complementary safety features necessary to cope with multiple failures in the safety systems.

6. APPLICATION OF THE DEFENCE IN DEPTH STRATEGY IN THE DESIGN OF I&C SYSTEMS

6.1. I&C Architecture

I&C functions necessary to operate the plant during normal plant operation or to bring the reactor back to safe conditions in case of an accident are allocated to and implemented in different I&C systems. As I&C systems are necessary for monitoring and operating the plant in all conditions, I&C systems shall be designed according to design principles making sure that the defence in depth concept is correctly reflected at the overall I&C architecture level and not compromised in case of failures affecting a system. According to the general roles allocated to the defence in depth levels, the I&C architecture should comply with the following structure:

- At level 1, I&C functions should aim to prevent deviations from normal operation by keeping the plant parameters within the specified range for normal operation,
- at level 2, I&C functions should aim to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions,
- at level 3, I&C functions should aim to detect and control design basis accidents to prevent excessive core damage and evolution towards severe accidents,
- at level 4, I&C functions aim to manage the consequences of accidents that result from failure of the third level of defence so as to prevent progression of the accident or to mitigate the consequences of a severe accident by limiting the radioactive release, and
- at level 5, I&C functions aim to support and facilitate decisions with regard to the appropriate off-site emergency measures to be implemented to protect the public in the event of a significant release.

As multiple failures in one or several I&C systems could prevent protection actions from being initiated and accomplished, quality of each level and appropriate independence

and diversity between I&C systems are essential elements to achieve the necessary overall reliability requested by the defence in depth concept. However, as I&C systems do not have the same safety significance, the expectations in terms of reliability allocated to each of them are not the same. Commonly:

- at level 1, I&C systems should be reliable enough to limit the number of occurrences of Anticipated Operational Occurrences (AOOs) initiated by its malfunctioning. The target for the total AOO frequency commonly accepted by the Member States is less than 1/reactor/year,
- level 2 includes both protection I&C systems designed to prevent anticipated operational occurrences from escalating to accident conditions, and I&C limitation systems designed to the number of challenges of reactor trips. The probability of failure per demand of each of them should consider the magnitude of the consequences of their failures (e.g. if the consequences exceeded the criteria established for design basis accidents, the frequency of occurrence of the sequence should be in the range of that defined for the design extension category),
- at level 3, I&C systems should be reliable enough so that the conditional probability of a transient or accident without response of the I&C functions be low enough not to challenge level 4 I&C functions more than expected . An order of magnitude for the probability of failure per demand less than 10^{-4} is widely shared by Member States,
- I&C systems at level 4 aim to control the consequences of a core melt accident. The I&C system should have the appropriate reliability to implement with confidence its intended functions with account taken of the low probability of a core melt accident to occur.
  Level 4 should also include complementary I&C system to overcome situations caused by the non-response of the reactor protection system (level 3) when challenged. As generally the concomitance of failures of these 2 I&C systems is ruled out, vulnerabilities for CCF should be eliminated and the reliability of each of them should be such that this hypothesis is correct.

The individual reliability target of I&C system is typically achieved by making appropriate use of:

- Redundancy: redundancy is commonly used in I&C systems to achieve system reliability and availability goals (tolerance to a failure or prevention of spurious actuation), or conformity with the single failure criterion. To be fully effective, either/ or independence and physical separation may be necessary.
- Independence: independence is intended to prevent the propagation of failures between redundant channels or from system to system.
- Physical separation: physical separation is intended to prevent common cause failures due to internal hazards.
- Environmental qualification: environmental qualification is intended to protect from global effects of hazards (e.g., environmental conditions, earthquake, electromagnetic interferences).
- Fail safe design: the principle of fail-safe design should be considered and incorporated into the design of the reactor protection system.
- Diversity is intended to prevent common cause failures due to design, manufacturing, maintenance or other human intervention.
- Testability: I&C systems important to safety shall be designed to permit periodic testing to provide clear evidence of system availability and performance.

Adequate and proven codes or standards should be used for the design of I&C systems to give confidence that they will be designed, commissioned, maintained and tested according to their safety significance.

6.2. Common cause failure (CCF), independence and diversity

Principles described in paragraph 4 also apply to I&C systems. Taking into account the number of possible origins for a latent fault[2], and irrespective of all preventive measures, demonstration that an I&C system is proven to be error free is very difficult and may always be disputed. Therefore, postulating deterministic common cause failure is becoming the best practice. As a consequence, for new builds, I&C functions, necessary to cope with a non-response of the Reactor Protection System implemented at level 3, are expected to be implemented in an independent and diverse I&C system. This diverse I&C system should have a sufficient quality to accomplish its intended safety functions.

Methodologies and rules used for assessing the consequences of multiple failures, and methodologies and rules used to demonstrate the effectiveness of the diverse I&C system may be less conservative than those usually used for the design basis accidents analyses. Here again, the Secretariat recognizes that there is a need for harmonizing the approach to defining what that less conservative approach could be.

Finally how far independence and diversity should be implemented should be assessed by performing a defence in depth and diversity analysis of the overall I&C architecture to verify if independence and diversity have been adequately implemented in the consecutive levels of defence. Particular attention should be paid to verify the elimination of CCF vulnerabilities resulting in a core melt accident and the effective independence of I&C necessary to mitigate the consequences of a core melt accident.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG Series No. 12, IAEA, Vienna (1999).

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series, Requirements No. NS-R-1, IAEA, Vienna (2000).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY IAEA, Code on the Safety of Nuclear Power Plants: Design, Safety Series No. 50-C-D (Rev. 1), IAEA, Vienna (1988).

[2] Errors in the design/manufacturing process, inadequate specification, software errors and data transfer errors, etc.

THE ISAM TOOL "OBJECTIVE PROVISION TREE (OPT)", FOR THE IDENTIFICATION OF THE DESIGN BASIS AND THE CONSTRUCTION OF THE SAFETY ARCHITECTURE

G.L. FIORINI[*], L. AMMIRABILE[**], V. RANGUELOVA[***]
[*] Nuclear Safety Consultant
Email: gian-luigi.fiorini@orange.fr;
[**]European Commission - Joint Research Centre Institute for Energy and Transport
Email: luca.ammirabile@ec.europa.eu
[***]European Commission - Joint Research Centre Headquarters, Brussels
Email: vesselina.ranguelova@ec.europa.eu

Abstract

The design of the safety architecture of innovative as well as the assessment of existing nuclear systems needs to integrate the constraints related to the safety principles, requirements and objectives. Among these constraints, the compliance of the installation's architecture with the principles of Defence in Depth (DiD), and its different levels, is certainly one of the most structuring. Defence in depth is the key to achieve safety robustness, thereby helping to ensure that nuclear systems do not exhibit any particularly dominant risk vulnerability. To help designers of innovative systems to correctly implement the defence-in-depth, or to assess how well the latter has been applied for existing reactor systems, the Objection-Provision Tree (OPT) methodology, which is part of the Integrated Safety Assessment Methodology (ISAM) promoted by the Generation IV Risk and Safety Working Group (GIF/RSWG), is suggested as a useful tool to complement the required traditional deterministic and probabilistic safety assessments. The document recalls the content of the OPT method and gives some details for its implementation, including for the systematic identification of the initiating events to be considered in designing the system. This step is essential especially for new systems for which there is no sufficient operational to support their design. The interactions with other tools (e.g. Failure Mode and Effect Analyses (FMEA) or ISAM Tools) are also commented.

1. INTRODUCTION

The design of the safety architecture of innovative as well as the assessment of existing nuclear systems needs to integrate the constraints related to the safety principles, requirements and objectives. Among these constraints, the compliance of the installation's architecture with the principles of Defence in Depth (DiD), and its different levels, is certainly one of the most structuring.

The safety architecture is defined as the set of provisions and their articulation in place to:

- Ensure completion of the tasks allocated to the process, in satisfactory safety conditions, i.e. maintaining the parameters representative of the facility safety within the allowable ranges for the operational criteria (e.g. maximum fuel & coolant pressure & temperature).
- To prevent, as much as feasible, initiators of accident.
- Detect and control deviations from the normal operation.
- In case of abnormal conditions, prevent the degradation of the plant - i.e. prevent exceeding the permissible range for the operational and safety criteria[1] - while keeping and / or restoring the facility in a safe condition.
- In case of accidental conditions with plant degradation, mitigate the consequences.

In practice, the achievement and maintenance in safe condition requires to satisfy simultaneously a set of safety functions (SF - cf. §3.2).

[1] The criteria are usually related to categories of situations (i.e. design basis conditions, design extension conditions; cf. the notion of allowable risk space - Farmer curve) rather than to levels of DiD. That said, for the design of provisions implemented within the different levels of defence in depth it is essential to have criteria to be met. The latter, which are expressed both in physical terms and in terms of reliability, shall be connected directly to the allowable ranges of parameters for the different categories of situations.

To help designers of innovative systems to correctly implement the defence-in-depth, or to assess how well the latter has been applied for existing reactor systems, the Objection-Provision Tree (OPT) methodology which is part of the ISAM method, promoted by the GIF/RSWG, is suggested as a useful tool to complement the required traditional deterministic and probabilistic safety assessments.

2. OBJECTIVE PROVISION TREE: OBJECTIVES AND SCOPE

2.1. The logic of the OPT

The approach recommended via the OPT method [1] structures the construction of the safety architecture through the systematic identification, for a given level of defence in depth (DiD), and for each of the safety functions (SF) and the corresponding objectives, of the challenges to the SF under consideration. For each of these challenges, the designer must identify the mechanisms / initiating events which, considering the process and the architecture already in place, materialize the challenge.

For conceptual High Temperature Reactors or existing Light Water Reactors, examples of detailed OPTs have been developed within the context of the IAEA [2, 3]. However, since this is a relatively new tool, an educational effort is needed, in particular, to further understand its objectives, scope, strengths and limitations.

The OPT steps are resumed as follow (cf. Fig.1):

- ***Safety Function****: e.g. reactivity control ⇨ to be performed successfully*

  ↳***Challenge****: e.g. injection of reactivity ⇨ to cope with*

  ↳ ***Mechanism****: e.g. control rod withdrawal ⇨ to be prevented or controlled*

Once determined the acceptability criteria which, in relation to a given mechanism, guarantee the satisfaction of the safety objectives, the last step is to identify, for each initiating event, the provisions which, collectively, allow to manage the appearance of the event and/or to minimize its consequences.

↳ ***Provisions****: e.g. a limiting removal device & associated I&C*

For a given initiating event, these provisions are grouped in a so called “Line of protection” (LOP) whose overall performance, in terms of efficiency and reliability, ensures the achievement of the mission requested to meet the allowable operational criteria (limiting withdrawal device + the I&C for detection, the control and the actuation of the device). It may be noted that, for a given level of defence in depth, the concept of LOP is similar to that of "layers of provisions" as it is defined in Ref. [4].

The steps described above illustrate how the OPT structures the process of identification of initiating events to be considered in the design, as well as the necessary steps to identify the provisions and so the safety architecture which will allow to control these events and to limit their consequences.

That said a remark may be raised: the events are identified by examining the challenges of a given safety function and, consequently, the related provisions are those that act to control the safety function under consideration. The provisions to be implemented for the simultaneous control of the other safety functions do not appear explicitly and one could wonders if they will appear when reviewing these functions. The objective being to bring

back the plant in safe condition[2], the mission to be achieved is composite and, of course, the objective is the simultaneous realization of all the safety functions. Considering the remark above, two scenarios are considered:

- If a mechanism / initiating event does disturb / challenges only a safety function (e.g. fuel failure ⇨ function "Confinement"[3]), the realization of other SFs, to achieve a safe state, will be done normally, and therefore the "normal" provisions will be requested. Under these conditions it is not necessary to identify specific provisions.
- If, instead, a given mechanism disrupts / challenges simultaneously several safety functions (e.g. injection of positive reactivity ⇨ power increase), the same mechanism - through induced effects (i.e. fuel and cladding overheating) - necessarily appear among those which will be considered for the challenged functions (control reactivity, heat removal and confinement). Appropriate provisions will therefore be identified, provisions whose performance will necessarily be compatible with the conditions created by the initiating event (e.g. increase of the heat flux, possible localized deformation of the clad, possible clad failure, etc.)

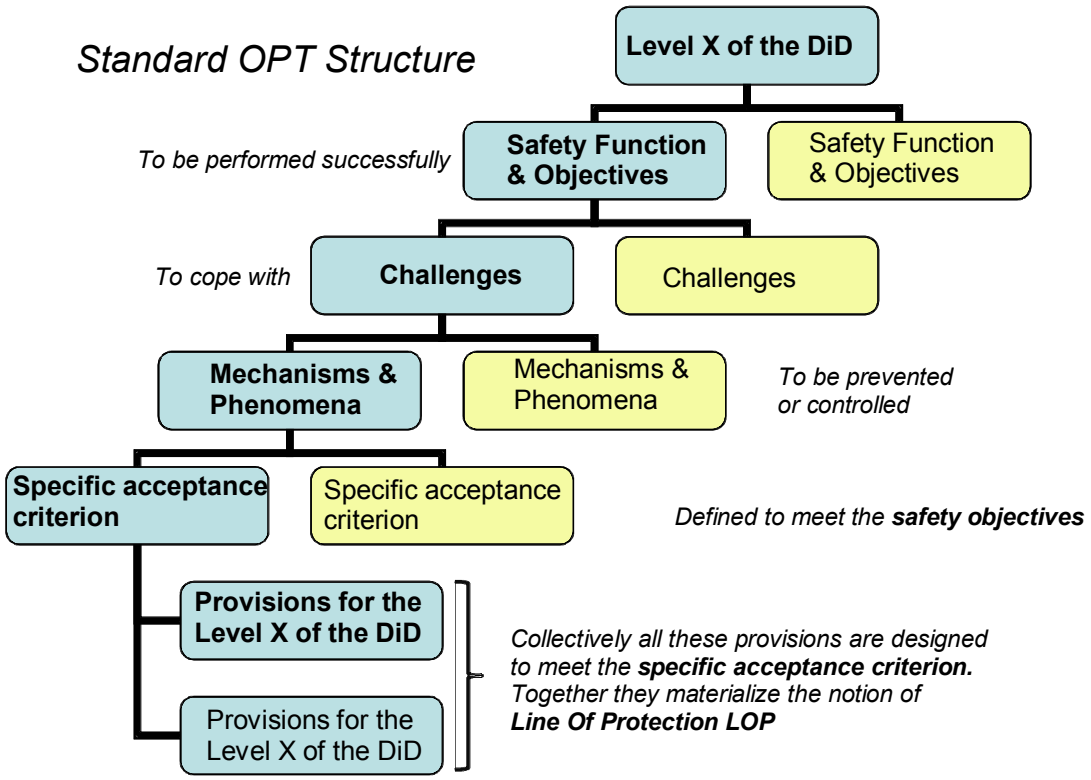

FIG. 1. Objective Provision Tree (OPT): Standard Structure.

[2] The safe state is characterized by the mastery of all the safety functions. This is what, within the IAEA documents (e.g. NSSR2-1, [4]) is defined as *"Safe state: Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time"*.

[3] Before, of course, a possible degradation of the hydraulic channel around the pin which will disturb the cooling of the fuel element and that will so affect the others safety functions.

2.2. The implementation of the OPT

Regarding the field for the implementation, the OPT method is applicable to concepts that would be at different stages of development:

- To design a concept which is at a preliminary stage (e.g. the Molten Salt Reactor - MSR), the OPT is used to identify initiators and to build - from scratch - the safety architecture.
- To finalize the design of a concept that is advanced or completed (e.g. the JSFR), the OPT can be used to check:
  - that all the initiators are adequately addressed;
  - that all levels of DiD are properly structured and organized (i.e. the necessary provisions are in place and are sufficient) to achieve the required missions;
  - that the mutual independence of the levels of DiD is guaranteed.

According to this last point, coherently with the principles of the DiD, the provisions associated with each level of the DiD must be independent and, if possible, diversified from those allocated to the other levels of the DiD. The objective is to ensure that the failure of a DiD level does not affect the efficiency and the performance of the next level. This must obviously be the case when studying a given event and the sequence(s) generated by the needs of its control (i.e. including the possible failures of the implemented provisions).

More generally one can raise the question of the acceptability of an architecture in which a given provision would be used for different initiating events and / or at different levels of the DiD, i.e. the provision is part of LOPs allocated to different levels of the DiD, depending on the requesting initiating event. This should be possible and allowed if the events which require the provision under consideration are completely independent. One must for example ensure that the solicitation of a provision by a given event, does not affect irreversibly its good behaviour if, once a safety state for system is restored, this provision can be sought for the management of another independent event[4].

This can be, for example, the case for shutdown provisions (incorporated within the shutdown system) that can be requested for initiating events which belong to the second level of the DiD (e.g. anticipated operational occurrences) or to the third level for others initiating events (design basis accidents).

Under these conditions one must not hastily conclude that the shutdown system should be doubled and diversified. The architecture must be such that a first failure[5], which would occur within the context of the control/management of an initiating event, and that would correspond to the effective deletion of a line of protection which is integral part of the shutdown system, i.e. the failure of a given level of the DiD (n), must be covered by the intervention of functionally redundant provisions; the latter shall guarantee, within the context of the next level of the DiD (n+1) [6], but still as an integral part of the shutdown system, the achievement of the "reactivity control" for the overall sequence: "initiating event + LOP(n) failure."

It remains to check that there are no conflicting implementations for the provisions under examination. From this perspective one can stress that, thanks to its comprehensive

[4] It would be, for example the case of a water tank used to remove residual heat under accident conditions and / or to inject water into the primary circuit under analogous or different accident conditions (this was the case for the architecture of an innovative "integrated" PWR in the '90ies).

[5] This situation does not address the case of the Single Failure Criterion (SFC) which is considered as a rule for the design of a specific LOP (e.g. the blockage of a control rod)

[6] i.e., with safety requirements and objectives which are specific of the new level of the DiD.

view of the safety architecture, the OPT facilitates the identification of possible conflicts and allows to verify the acceptability of the final architecture.

Finally, one can note that, the safety objectives being variable and dependent upon the category of the initiating event as, a fortiori, upon the DiD level within which the abnormal situation has to be managed, the same provision, implemented at different levels of the DiD for others specific events, will not necessarily be requested to meet the same functional specifications for those different levels[7].

3. ELEMENTS OF THE OPT

3.1. Levels of the Defence in depth (DiD)

According to [5] Defence in depth is generally structured in five levels. Should one level fail, the subsequent level comes into play.

The objective of the first level of protection is the prevention of abnormal operation and system failures. If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response."

3.2. Safety Functions

Safe design in general is characterized by the simultaneous control of the following safety functions (SF): *a) Containment of hazardous materials; b) Control of chain reactions; c) Control of removal of the energy produced; d) Control of radiation protection; e) Control of non-nuclear risks.* Other functions are implicit in that their compliance is ensured by the compliance with functions a) to d) above, e.g.: f) *Control of public health and environmental protection (see for example the Article 28 of the French TSN law - 2006).*

3.3. Safety objectives

As indicated above, the rationale for the safety architecture, after a given initiating event, is to maintain or bring back the plant to a safe state, i.e. to achieve a consistent set of safety functions while meeting the safety objectives.

The initiating events, once identified, are categorized following their estimated frequency of occurrence. For each category, quantitative safety objectives are usually suggested by the designer and endorsed by the regulators; this allows defining the space of acceptable risk: frequency of occurrence – allowable consequences (i.e. the so called "Farmer curve"[8]).

---

[7] i.e. Safety requirements and objectives will be specific of the level of the DiD.

[8] The latter is obviously perfectly coherent with the IAEA Technical Safety Objective: …. to ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and to ensure that the likelihood of accidents with serious radiological consequences is extremely low (Safety of Nuclear Power Plants: Design, IAEA Publication NS-R-1, Page 4.)

The proposal of WENRA/RHWG [6] shows that there is a direct relationship between the defence in depth and the "allowable risk domain". This is essential for the designer who can so superpose the levels of defence in depth within the area of allowable risk, and simultaneously, to give explicit targets (success criteria, both in terms of performances and reliability) for these levels. These targets are essential to size the provisions that are associated with each level of the DiD. Under these conditions, for a given SF, the objectives corresponding to a given level of DiD are translated into physical parameters or "decoupling criteria" that reflect the allowable consequences associated with this level of DiD[9]. So, for each of the safety functions, representative parameters (Figures of Merit - FoM, or decoupling criteria) can be identified with associated values that reflect compliance with safety objectives.

One can point out that, in the early phases, which correspond to the preliminary identification of *Challenges* ⇨ *Mechanisms* ⇨ *Provisions*, it is not necessary to have precise quantitative targets; orders of magnitude will be sufficient to select the provisions that designer feels able to comply with objectives. These quantitative values are nonetheless required later in the design process for the exact sizing of the implemented provisions[10].

3.4. Challenges

As indicated above a challenge represents a potential mode of aggression to a safety function, which could lead to exceeded allowable values for FoM and therefore non-compliance with safety objectives.

One may wonder to what extent it is possible to define "challenges" that are independent of technology and dependent only on the safety function under consideration. In practice this seems feasible:

- For the "*Containment of hazardous materials*", challenges result in possible aggressions on barriers; the parameters that characterize these aggressions are those that materialize the loads on barriers (harsh environment, e.g., pressure, temperature, radiation, missiles, etc.). An example of a challenge for this function is, for example, the "*abnormal thermal and or mechanical stresses on first barrier*"
- For the "*Control of chain reactions*" the challenges reflect the potential for alterations of the core/fuel k_{eff} (excessive variation of k_{eff} through local or global reactivity injection). Opportunities for positive or negative reactivity insertions must be considered. The representative parameters are those characterizing the reactivity in the core / fuel (reactivity introduced, counter reactions coefficients, etc.). In this case, an example of a challenge is "*insertion of positive reactivity*".
- For the "*Control of removal of the energy produced"* the challenges correspond to possible loss of integrity of the facility structures, e.g. fuel matrix, cladding, primary circuit structures, etc.. The representative parameters are loads on these structures (pressures, temperatures, etc.). An example of challenge to this function is the "*degradation of the residual heat removal path*"

[9] For example, for the "Control of removal of the energy produced", and the third level DiD applicable to a nuclear reactor - Prevention of the core deterioration and the potential aggression of containment - the decoupling criteria are represented by the fuel temperature and / or the temperature of the core structures which determine the beginning of the loss of geometry (e.g. in the case of conventional solid fuel: the fuel / cladding melting temperature).

[10] Example: for the Decay Heat Removal (DHR) the designer asks for an order of magnitude for the required coolant's flow. This order of magnitude is sufficient to choose the nature of the "provision" that will be implemented (e.g. for an SFR: mechanical pump or electromagnetic pump). During the detailed design phase the designer will size precisely the selected provision

- For the "*Control of Radiation protection*" challenges reflect alterations for protection measures against ionising radiation and in particular of the conditions under which operators are required to work. Potential for internal and / or external exposures should be considered. The first (internal exposures, e.g. after inhalation) would be caused by a prior loss of containment function. Concerning the external exposure, the parameters that characterize protection against sources are the distance, the activity, the time and the screens[11]. Under these conditions one can consider that alterations - or misconceptions - that would affect one or more of these parameters represent the potential challenges to the function. An example is the "*Abnormal exposure under maintenance conditions*".
- For the "*Control of Non-nuclear risks*" challenges reflect changes in environmental conditions that alter the loading conditions on the facility structures and / or, where applicable, the operating conditions. They may be due to chemical or thermodynamic reactions[12]. The representative parameters are loads on structures and possible abnormal conditions the operator intervention (pressure, temperature, humidity, visibility, etc.) [13]. An example of challenge for this function is the "*Explosion*".

Following the examples cited above it seems that the process of identifying the challenges could be neutral versus the technology, i.e., the identified challenges will be neutral vis-à-vis of the reviewed technology. Needless to say that, for the OPT methodology effectiveness, the effort to identify challenges needs to be explicit and as comprehensive as practicable.

3.5. Initiating events (mechanisms)

For the technology and the concept under examination (e.g. Sodium cooled Fast Reactor - SFR, pool concept), each challenge is materialized by a set of mechanisms / initiating events. These initiating events are obviously specific for the concept, and even specific for a given type of concept (e.g. SFR with or without intermediate circuit). The designer shall seek systematically mechanisms / initiating events among the plausible phenomena that are either related to the specific technology under consideration (e.g. sodium fires), or induced by the provisions already implemented (e.g. withdrawal of a control rod). Finally it should be noted that in case of application of deterministic rules (e.g., single failure criterion) the design of the needed provisions may postulate degradations without direct and explicit link to a specific challenge. However, despite this prescriptive approach the mechanism should be correlated, a posteriori, to a challenges among those identified; nothing changes in the process for the identification of provisions needed for its control and the mitigation of its consequences.

3.6. Provisions & LOP

Once the initiating events are identified, the designer must specify, for each event, the provisions that are integrated into the architecture to manage their advent and control /mitigate their consequences. All provisions which collectively perform the required duties are grouped in a line of protection (LOP) whose overall performance in terms of reliability and efficiency, allow the realization of the mission requirements and the meeting of the safety objectives. It is important to note that, in terms of overall LOP performance, for example with

[11] In French: Distance, Activité, Temps & Ecrans (DATE)

[12] e.g. sodium fires for the sodium cooled fast reactor (SFR)

[13] e.g. the presence of aerosols that would impede a given intervention. These conditions are considered reflecting the functional aspects.

the search for the LOP reliability that is needed to prepare a Probabilistic Safety Analysis (PSA), it is the characteristics of the lower reliability provision (i.e. the "weakest link") that will define the representative value for the reliability[14].

3.7. The OPT: an interesting tool to address the security concerns

It is interesting to point out that, as indicated for example by WENRA [7][15], the integration of safety and security concerns (i.e. physical protection and proliferation resistance) should be searched at the design level. This integration could be done, with logic similar to that of OPT, i.e. searching and organizing synergistically specific security provisions for the control of these concerns, through the consideration of "security functions" such as, for example:

- control of flows of hazardous materials;
- protection against malevolent hazards.

As for the function f) above (cf. § 3.2), one can consider that the "*protection against malevolent hazards*" is implicitly performed by the respect of safety functions listed above ("a" to "e") with, if necessary, the implementation of specific provisions[16].

Downstream the definition of the security function, the logic for the identification of the provisions, which will be specific to ensure the security of the plant, can be analogous to that for the safety functions. So, the comparable representation of the safety and the security architecture will be helpful to fulfil and prove the effective integration; possible security provisions which can have adverse impact on safety and vice-versa will be identified and alternative design solutions will be sought to avoid the potential for conflict.

4. ITERATIVE PROCESS FOR THE FINALIZATION OF THE SAFETY ARCHITECTURE

4.1. Recall the whole safety assessment

Before discussing the iterative process for the identification of the initiating events which will lead, through the safety analysis, to verify that the safety architecture meets the safety objectives, it is worth recalling that this analysis is only one component of the whole assessment for the safety architecture, assessment which also needs the compliance with principles requirements and guidelines (e.g. from [8][17], [9] and [10]). This compliance is checked through complementary ISAM tools as, for example, the Qualitative Safety Review [1].

4.2. Iterative process to identify the initiating events

The process of identification of the initiators to be considered when sizing the safety architecture, as performed using the OPT, is part of an iterative process (see Fig.2).

---

[14] It is essential that the designer, who is preparing a PSA and who is assessing the reliability of its system vis-à-vis a given initiator, be able to consider the whole LOP that performs the tasks required. To do this he must have properly identified the LOP with all its component. Similarly the treatment of common modes can also benefit from notions conveyed by OPT and the concept of LOP, especially as regards the independence of DiD levels.

[15] WENRA Objective O5. **Safety and security interfaces**: ensuring that safety measures and security measures are designed and implemented in an integrated manner. Synergies between safety and security enhancements should be sought.

[16] Thanks to the fact that the "malevolent hazards" will likely generate specific initiating events.

[17] Safety Assessment: the systematic process that is carried out throughout the design process to ensure that all the relevant safety requirements are met by the proposed (or actual) design. **Safety assessment includes, but is not limited to, the formal safety analysis.**

Once the OPT is completed and the components of the safety architecture are identified, it is essential to iterate over the identification of the initiators to verify that the implementation of other provisions, required by other levels of DiD and other safety functions, does not introduce additional risks whose consequences would not be covered by those already considered[18]. In other words, once the LOP is in place, an essential first audit should address the possible negative consequences associated with its presence and that of its provisions in case of normal and degraded operation conditions[19]. Further verification, equally important, concerns the analysis of the failure of the LOP and its provisions taken singularly; this failure (partial or total) obviously affects the achievement of the safety function under investigation[20] but may also represent an additional hazard for other safety functions[21].

Moreover, for the safety function under consideration, the failure of a LOP means the failure of the DiD level for which the LOP had been implemented. According to the definition of DiD [5], this failure, and the resulting situation, corresponds, automatically, to an "initiating event" for the next level which will be requested to manage and mitigate the corresponding consequences. It is this iterative process that must lead to the overall coherence of the safety architecture. This consistency is necessarily the result of compromises for which one strives to maximize the effectiveness of the architecture and to minimize the potential for the involved risks.

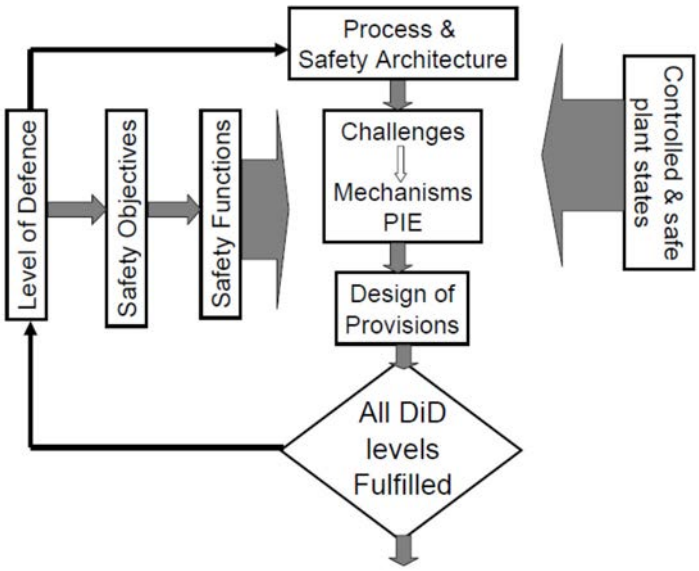

FIG. 2. Iterative process for the construction of the safety architecture.

[18] For example, in standard PWRs the presence of boron in the primary circuit is a provision to help the "Control of chain reactions". It must appear from the provisions listed in the OPT PWR, for example within the first level of DiD. But the implementation of this provision introduces the risk of boron dilution and an initiator raise: the "plug of clear water" directly generated by the provision. Additional provisions are expected to address this specific risk (at the second and third level DiD).

[19] E.g. the implementation of a mechanical pump could induce vibrations that would interfere with proper operation of other provisions already in place.

[20] *If a single provision is faulty the LOP could nevertheless correctly realizes its mission if it is designed, as a whole, considering the single failure criterion (SFC). This will not be necessarily the case if only the single provisions are designed with the SFC.*

[21] *It is possible that the failure of a provision, regardless of whether the proper functioning of the LOP is affected or not, affects the behavior of other provisions/LOPs if its failure generates a degraded environment (e.g. fire, smoke, aerosols, etc.).*

4.3. Possible role of the FMEA

In analysing the potential consequences of a LOP / provision failure, all plausible failure modes are considered. It is at this stage that an FMEA like analysis is possible and - at the discretion of the designer – will complete the OPT approach in order to: identify weaknesses in the system and make remedies; identify ways to prevent certain failures; study in detail the consequences of failures of the various provisions; classify failures with selected criteria; provide an optimization of the maintenance plan and provide insights to support the development of test plans; optimize tests to check the proper operation of the installation; motivate decisions for design's revisions; etc.

The FMEA can provide an important validation step in the identification of the initiators but it applies to an already globally defined architecture. From this point of view, it is complementary to the OPT. In particular the FMEA can check - through the analysis of "Criticality" (Criticality = Severity of failure x Frequency of occurrence x Detectability of the failure) – that the possible interactions between provisions are properly taken into account in terms of their real importance, and the possible consequences of failures are optimized in terms of risk / criticality.

While OPT helps to build an architecture according to the principles of defence in depth, FMEA can provide, in addition, an interesting indication for the optimization of the architecture in terms of "criticality". This optimization phase is a step that can be considered as part of the iterative process in the implementation of the OPT and, as such, FMEA, or any other method of risk analysis (e.g. HAZOP - Hazard and Operability analysis), can certainly help during the phase of detailed engineering for new installations.

5. THE OPT WITHIN THE FRAMEWORK OF THE ISAM

5.1. Introduction

As anticipated, the role and place of the OPT within the context of the ISAM needs to be discussed in order to point out the interactions with the other ISAM tools [1]:

- with the QSR to check the compliance with principles requirements and guidelines,
- with the PIRT for the identification of the initiators to be considered for the design of the installation, and
- with the DPA safety analysis which allow checking the meeting of safety objectives.

Finally the OPT has to be considered as a preliminary step for the preparation and the realization of the PSA.

5.2. OPT and Qualitative Safety Features Review (QSR)

As indicated within [2], the Qualitative Safety Features Review (QSR) is a new tool that provides a systematic means of ensuring and documenting that the evolving Gen IV system concept of design incorporates the desirable safety-related attributes and characteristics as identified by the available references. QSR is structured following the logic of the defence in depth, and merges a comprehensive set of qualitative foreseen characteristics and features which translate principles, requirements and guidelines applicable to future reactors. Such check list is helping the designer to qualitatively assess and select among different safety options and practical solutions (i.e. the provisions / LOP) those which, while allowing achieving the requested mission and meeting the safety objectives, will best guarantee the correspondence of the final result with the principles and the "good practices" suggested by the available references. The previous paragraphs illustrate how, through the OPT approach,

the designer is led to identify the missions and, once these missions defined, select the provisions / LOP which, once integrated into the safety architecture, will achieve them to satisfy the safety objectives. The systematic and parallel use of the QSR allows to check the compatibility of the selected provisions / LOP with the available principles, requirements and guidelines, and if several solutions are offered, select the one (s) that best meet these principles, requirements and guidelines. Moreover, as noted above, highlighting any weaknesses will allow the designer to give adequate priority to their resolution or, where appropriate, motivate the abandonment of the solution.

5.3. OPT and the Phenomena Identification and Ranking Table (PIRT)

Following [1], the method provides a "*discipline for identifying those issues that will undergo more rigorous analysis using the other tools that comprise the ISAM. As such, the PIRT forms an input to both the Objective Provision Tree (OPT) analyses, and the Probabilistic Safety Analysis (PSA). The PIRT is particularly helpful in defining the course of accident sequences, and defining safety system success criteria*". The PIRT is recognized essential in helping to identify phenomena areas in which additional research may be helpful to reduce uncertainties.

Discussing the OPT, the previous paragraphs illustrate how, once the challenges defined the designer is led to identify the mechanisms and phenomena which, for the plant under examination, materialize these challenges. In this logic the interactions between the OPT and PIRT are of double nature. On one side the PIRT, for a given challenge and considering the characteristics of the process, will help to identify the mechanisms / phenomena which shall be controlled by the safety architecture and, on the other side, it will allow ranking the corresponding phenomena in terms of importance and degree of knowledge. The latter contribution is essential for, within the context of the design / assessment of the provisions and the safety architecture, defined with the help of the OPT, the PIRT will allow: 1) to prioritize confirmatory research activities to address the safety-significant issues, 2) to inform decisions regarding the development of independent and confirmatory analytical tools for safety analysis, 3) to assist in defining test data needs for the validation and verification of analytical tools and codes, and 4) to provide insights for the review of safety analysis and supporting data bases. Themes 2, 3 and 4 generate essential interactions with another ISAM tool: the Deterministic and Phenomenological Analyses (DPA).

5.4. OPT and Deterministic and Phenomenological Analyses (DPA)

Deterministic and Phenomenological Analyses (DPA), which support the detailed safety analysis both for the design and sizing of the provisions / LOP, as well as for the safety assessment of the whole safety architecture, constitute a vital part of the overall Gen IV ISAM.

DPA is the natural complement of the work achieved with the OPT for, at the very end, DPA will allow sizing of the entire safety architecture and its provisions / LOP and proving that this architecture can meet, as requested, the safety objectives. Moreover, the DPA bring the quantitative assessment for the consequences of the design basis conditions and, as such, it will provide essential inputs into the PSA. Aside from the implementation of deterministic rules (e.g. single failure criterion) which define the framework for the analysis, DPA typically involve the use of familiar deterministic safety analysis codes whose degree of adequacy will be evaluated also with the inputs from the PIRT. Within [1], it is anticipated that DPA will be used "*from the late portion of the pre-conceptual design phase through ultimate licensing and regulation of the Generation IV system*". This is due to the fact that preliminary PIRT analysis

and OPT implementation will allow defining, and preliminarily sizing, the skeleton of the architecture on which the DPA can apply.

5.5. OPT and the Probabilistic Safety Assessment (PSA)

Probabilistic Safety Analysis (PSA), as indicated by [1], "*is the centerpiece of the ISAM*" for it can address in an exhaustive manner "*both internal and external events, and models potential accident phenomena from the hypothetical occurrence of an initiating event through the point at which accident progression is either arrested, or offsite consequences are realized*". Obviously PSA can only be meaningfully applied to a design that has reached a sufficient level of maturity and detail[22].

Nevertheless the exhaustiveness of the description is not an intrinsic characteristic of the tool and it must be provided through the input data. This is why the interaction between OPT and PSA are so essential: the former will provide the whole safety architecture that will be, with all its internal interactions, analytically described by the PSA.

While OPT will strongly contribute to check the consistency versus requirements such as, for example, the principles of the defence in depth (full coverage of all the levels, independence between the levels, etc.), only the PSA can allow the designer to verify the compliance with essential requirements such as the progressiveness of the safety response and the balance among the design conditions versus, for example, the risk for core degradation.

6. CONCLUSIONS

Critical analysis of the contents of the OPT and of the steps for its implementation allows to better identify what may be the role of the tool, especially for the identification of the initiators of incidents and accidents that the designer has to take into account for the design of the safety architecture.

The benefits from the implementation of OPT are even stronger when it is considered within the whole context of interaction with the other ISAM tools:

- with the QSR to allow checking the compliance of provisions, LOP and architecture with principles requirements and guidelines; this compliance is an essential step for the optimization of the selection among the possible technical solutions;
- with the PIRT for the identification of the initiators to be considered for the design and sizing of provisions, LOP and the architecture of the installation, and the ranking of these phenomena / mechanisms in terms of importance and degree of knowledge; this ranking is essential to prioritize the supporting R&D effort;
- with the DPA safety analysis which allow sizing the provisions and LOP, and demonstrating the quantitative compliance of the whole safety architecture with the safety objectives;
- with the PSA for which the OPT represents an essential input in terms of detailed presentation of the whole safety architecture which, once available, will be analytically described and assessed by the PSA.

In this context Objective Provision Tree (OPT) and the related concept of Line Protection (LOP) appear to be instruments well suited to articulate the work of design and

[22] So called "Living PSA" can be organized, and used as a key decision tool, in an early design stage but they can only apply to a system whose skeleton, in terms of safety architecture is already available and preliminarily defined and when data on reliability of different provisions can be generated with an adequate degree of uncertainties.

assessment of future Gen IV systems in which innovative options - active systems and passive, intrinsic characteristics, etc. - come in to organize safety architectures that one would expect to be simpler and more optimized. OPT/LOP can be implemented alone for punctual studies but the real interest, for the design and assessment of Gen IV systems, raises from the synergy with other ISAM tools and from the iterative way in which those tools are applied at different design development stages.

REFERENCES

[1] GENERATION IV INTERNATIONAL FORUM (GIF), An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems, GIF - Risk and Safety Working Group (RSWG), Version 1.1, June (2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors, IAEA-TECDOC-1366, IAEA, Vienna (2003).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Defence in Depth for Nuclear Power Plants, IAEA Safety Reports Series No. 46, IAEA, Vienna (2005).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

[5] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).

[6] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), WENRA Statement on Safety Objectives for New Nuclear Power Plants, November (2010).

[7] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), Safety of New NPP Designs, Study by Reactor Harmonization Working Group (RHWG/WENRA), March (2013).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards, General Safety Requirements Part 4, No. GSR Part 4, IAEA, Vienna (2009).

[9] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG Series No. 12, IAEA, Vienna (1999).

[10] GENERATION IV INTERNATIONAL FORUM (GIF), Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems, GIF/RSWG/2007/002 Revision 1, November (2008).

HOW TO REINFORCE THE "DEFENCE-IN-DEPTH" IN NPP BY TAKING INTO ACCOUNT NATURAL HAZARDS?

C. LAVARENNE, K. HERVIOU, C. PICOT, P. DUPUY
Institut de Radioprotection et de Sûreté Nucléaire (IRSN), Pôle Sûreté Nucléaire,
Fontenay aux Roses, France
E-mail: caroline.lavarenne@irsn.fr; karine.herviou@irsn.fr

Abstract

The "defence-in-depth" (DiD) principle is the fundamental safety principle for the design and operation of nuclear power plants. This principle aims to prevent as far as possible initiating events and managing their consequences if preventive provisions failed. It has to be applied to the protection against hazards so as to limit their likelihood and/or their consequences by the implementation of prevention, control and mitigation provisions in NPPs consistently with provisions for internal events. So far, the protection of nuclear power plants against external hazards follows a "load-cases" approach, which differs from the approach used for internal events. In 2011, the Fukushima accident showed that, for a beyond design hazard or a combination of hazards not considered at the design stage, all levels of defence may be swept away simultaneously and may lead to a disaster. Natural hazards can therefore be considered as a potential common cause of failure affecting at the same time all levels of the "defence-in-depth". In France, the definition and the implementation of a post-Fukushima "Hardened Safety Core" for operating NPPs should compensate for some weaknesses in the current approach and improve significantly the robustness of the installations against natural hazards. For future reactors, a new approach based on the definition of two domains, "design basis" and "design extension" for natural hazards, is examined in order to fulfil ambitious general plant safety objectives. It turns out that safety assessments related to natural hazards raise some challenges and difficulties, especially to characterize events with very low frequencies in a context of limited data, to define combinations of hazards (eventually with internal events) and to consider events that go beyond the design basis. For these issues, international guidance and discussions may be fruitful.

1. INTRODUCTION

The "defence-in-depth" principle is the fundamental safety principle for the design and operation of nuclear power plants. This principle aims to prevent as far as possible initiating events and managing their consequences if preventive provisions failed. But it is mainly applied to internal events.

In 2000, French and German advisory committees of experts agreed on a list of requirements to be met by the future generation of PWR to be built in France or in Germany [1], recognizing that vendors and operators may pay particular attention to external hazards: "*Design provisions must be taken with respect to external hazards, consistently with provisions for internal events and internal hazards; that is to say, external hazards must not constitute a large part of the risk associated to nuclear power plant of the next generation.*". An objective of global core damage frequency was fixed, including internal events, internal and external hazards and uncertainties.

In the meantime, taking into account the operation feedback, improvements regarding natural hazards have been progressively introduced in operating NPPs. The Fukushima accident of course has led to re-examining the adequacy of the measures taken or envisaged regarding natural hazards.

More broadly, it raises the question of the potential weaknesses of current approaches and the need to define a new approach for future reactors.

After going over the general approach used to take into account natural hazards in the design of French NPPs, the paper tackles how this approach has been completed for existing installations following the Fukushima accident and how it could be reviewed for the design of future reactors.

2. CURRENT APPROACH: LINK BETWEEN NATURAL HAZARDS AND DEFENCE-IN-DEPTH

At the design stage, the approach to take into account natural hazards, known as a "load cases" approach, was relatively decoupled from accident studies reported in the safety case; considering a list of natural hazards and associated characteristics (as maximum accelerations and spectrum for earthquakes, water levels and durations for flood, velocity for winds, intensity and duration for very high or very low temperatures…), the "load-cases" approach ensures the capability of NPPs to withstand natural hazards, with no consequences for plant safety. Systems, Structures and Components (SSC) needed to guarantee a safe shutdown and to fulfil the three fundamental safety functions (sub-criticality, decay heat removal, confinement) after shutdown are designed or protected against considered hazards.

However, this does not mean that equipment needed to manage an accident are not designed or protected against natural hazards, especially because natural hazards may cause damages to off-site devices that would affect the plant configuration (e.g. loss of off-site power, loss of heat sink…). For each external hazard, an appropriate approach is defined and used to determine the Systems, Structures and Components (SSC) which must resist or be protected, and to evaluate the dependencies with other external hazards and internal events.

Although the rules for cumulating external hazards and accident situations are complex and include specificities, it appears, in practice, that for generation II French PWR:

- Safety equipment needed for design basis accidents - DBA (level 3 DiD) - are generally protected against natural external hazards even if dependency between natural hazards and accidents is not systematically postulated for all hazards;
- Safety equipment used to cope with a Loss Of Off-site Power (LOOP) (e.g. diesels) are protected from natural hazards that may challenge the off-site power;
- Simultaneous occurrence of situations with multiple failures, such as total loss of heat sink or total loss of electrical power, and an external hazard is not postulated. However, according to "defence-in-depth" and especially when it is difficult to exclude a link between them (e.g. total loss of heat sink in case of ingress of vegetable matters or very cold weather, snow, extreme wind, projectiles…), equipment used to manage these situations are generally protected;
- For severe accidents (level 4 DiD), equipment are generally not designed to resist to natural hazards as it is considered that such hazards could not lead to core damage. However some equipment needed to manage an accident with multiple failures or core damage may also be required for DBA management, and, as such, can be designed or protected against hazards.

Figure 1 gives an overview of the level of protection against natural hazards of SSC participating to the different DiD levels. It can be noticed that rules applied for the design of SSCs or associated protective measures are such that the plant can withstand natural hazards that go beyond the "design basis hazards" but existing margins are not quantified.

By analogy with the provisions set up regarding accidents considered in the safety case, several lines of defence against hazards are generally planned to:

- Prevent hazard impact on the safety functions (e.g. design and qualification of safety equipment);

- Anticipate hazards when predictable or detect their occurrence in order to implement protective measures or verify plant behaviour (e.g. procedures to verify the water tightness of the rooms housing safety equipment in case of flooding);
- Manage an accident situation such as LOOP or LUHS.

For SSCs that are designed or protected against natural hazard, it should be pointed out that the hazard "intensity" considered is generally the same for all SSC, whatever the level of DiD they refer to. In other words, when going beyond this "design basis hazards", all provisions taken for the different levels of the "defence-in-depth" can be affected simultaneously. This may be considered as a weakness of the approach against hazards, especially when the probability to go beyond the "design basis hazard" is not very low.

3. LESSONS LEARNED FROM OPERATING EXPERIENCE AND IMPROVEMENTS SET IN PLACE

The operating experience in terms of climatic events having disrupted French nuclear power plants is important. From design, events emphasized the weakness of the approach for the protection against natural hazards (partial flooding of the Blayais NPP in 1999, heat waves in 2003 and 2006, frazil in Chooz in 2009 ...) and motivated the development of new standards and additional protection measures. It also confirmed the risk of LOOP or LUHS situations in case of some natural hazards. Some of these events are discussed below.

3.1. Le Blayais incident in 1999 (level 2 on the INES scale)

During this incident, safety functions were still ensured, despite the unavailability due to the flooding of several systems important to safety (safety injection and emergency spray systems, several rows of essential cooling water system). Fortunately, cooling systems were not totally lost and there was no initiator requiring unavailable safety systems. This incident showed among others the threat of flooding for external power supplies (main and auxiliary power lost successively but not simultaneously) and ultimate heat sink ("turbidity" of water), with a risk of LOOP and LUHS. Moreover, the Le Blayais site was temporarily inaccessible.

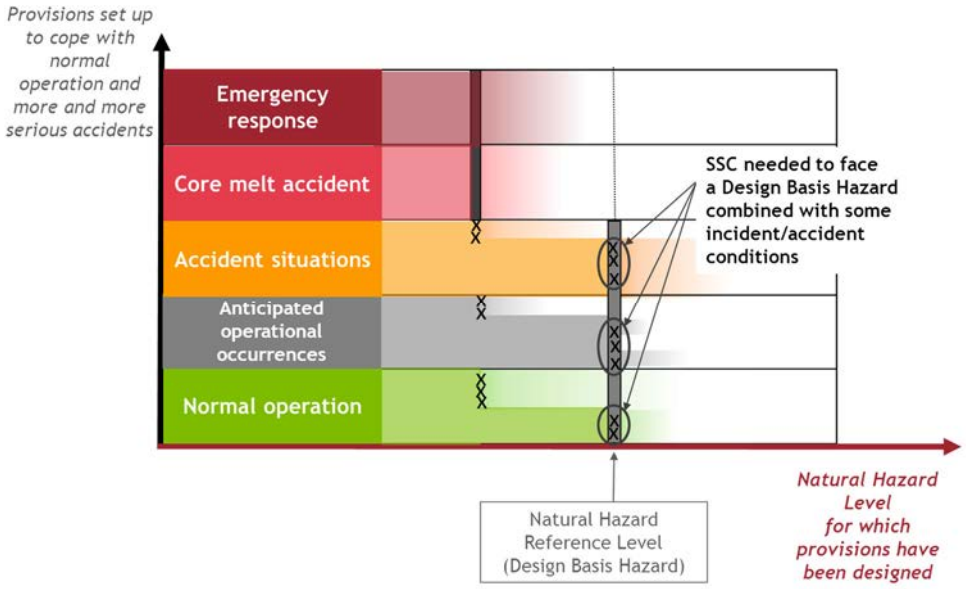

FIG. 1. Design/protection of SSC for different levels of "Defence-in-Depth".

3.2. Cruas massive arrival of sticky algae in 2009 (level 2 on the INES scale)

A LUHS occurred at unit 1. The consequences were mastered and the duration of the loss of heat sink was relatively limited (10 hours). A single unit was concerned, however a threat was identified for two of the three other site units.

3.3. Winters 1985, 1986 and 1987 with temperatures below -15°C (corresponding to the minimum outdoor temperature taken into account at the time for the design of French NPPs)

Temperatures below -15°C were observed and affected several safety systems on several NPPs. Consequences varied from one site to the other: loss of ultimate heat sink (formation of ice, pile of ice blocks in front of the water intakes of the plants along the Loire river), weakening of the electrical grid (some units were stopped due to the risk of loss of off-site power), freezing of some equipment (sensors, extra water lines to the steam generator emergency auxiliary feedwater...), unavailability of some diesel generators due to low temperature of lubricating oil.

Therefore, significant improvements have been implemented since initial design of French NPPs to take into account the operating feedback, particularly through periodic safety reviews:

- Verification of "design basis hazards" and if necessary increase of their "intensity", extension of the list of hazards (e.g. including tornadoes). Some difficulties arose to reach low annual exceeding frequency (10^{-4}/y target if one refers to the frequency of category 4 accidents) due to insufficient databases or validated methods;
- Extension of the provisions against natural hazards in order to:
  - handle situations corresponding to DiD level 3;
  - handle situations with combination of natural hazard and LOOP or LUHS affecting all units of a given site;
- Modification of emergency operating procedures and on-site emergency response plans to cope with disorders or accidents affecting simultaneously several units of a given site, taking into account possible site inaccessibility, following a natural hazard.

In addition, Le Blayais incident analyses pointed out the need to examine the risk of cliff-edge effects for hazards that go slightly beyond the "design basis floods".

4. THE FUKUSHIMA ACCIDENT: PROVISIONS SET UP IN EXISTING NPPs

The Fukushima accident showed again the need to go further in the management of risks related to natural hazards. It led to "strengthen the requirements" in terms of verification of SSCs protection against natural hazards and induced consequences, on site and off site. The accident raised questions on:

- Behaviour of a NPP in case of "beyond design hazard" or combinations of hazards not considered at the design stage or during periodic reviews.
- Management of long-term LOOP or LUHS due to a natural hazard, including potential induced events in the plant (pipes breaks, explosions…).
- Management of a severe accident due to a natural hazard.
- Emergency response for beyond design hazards affecting several units on the same site.

In France, it was decided to increase the protection of NPPs against natural hazards by reinforcing some parts of the installation and implementing complementary equipment aiming to limit the releases in case of "beyond design hazards". This set of equipment is called the post-Fukushima "hardened safety core" (HSC).

For operating reactors, even if some severe accident management provisions have been implemented in the past (hydrogen passive auto-catalytic recombiners PARs, containment filtering and venting system…), the releases that may occur in case of core melt may be still important in case of total loss of electrical supply or heat sink: on-site, it may disrupt on-going actions to restore installations safety, while off-site, the protection of the population in the surrounding area may be particularly difficult, if not impossible in case of a natural disaster. Therefore, as the most efficient way to limit releases is to prevent core melt, a first set of provisions that aims to prevent core melt, i.e., stop the nuclear reaction, cool the core and ensure confinement, has been defined.

Induced effects in the plant could make the situation more complex than the one anticipated to define the former set of equipment of the HSC: failure of existing equipment that have not been initially designed to cope with "beyond design hazards" (like small pipes breaks or load drops) could not be excluded, other induced effects like fire or explosion may aggravate the plant configuration.

Therefore, French safety organizations have estimated that the HCS should include as well a set of provisions to cope with severe accidents, in order to limit the releases. Finally the HSC also includes SSCs needed for emergency management (I&C, telecommunication means, meteorological and radiation monitoring devices…). Figure 2 gives a schematic overview of the HSC (only main SSCs are presented).

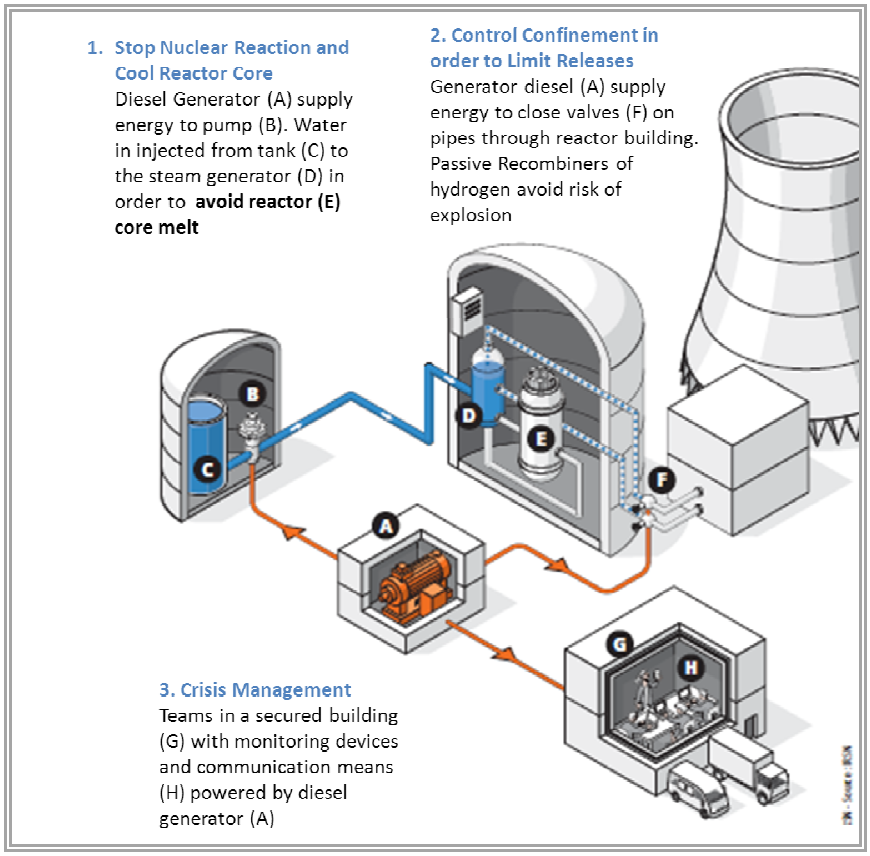

FIG.2. Schematic representation of the hardened safety core (reactor-side) that will be implemented in French NPP.

Addition of new fixed equipment is preferred to have a high level of confidence in the capability of the HSC to fulfil its missions in due time. Of course, some existing SSCs will still be necessary (at least the reactor coolant system, pipes to feed steam generators…) and particular attention will be paid to connections and concerned SSCs. HSC supporting systems (such as electrical switchgears, ventilation…) should be designed accordingly and should be as far as possible independent from existing provisions. In France, specific electrical distribution is requested to support HSC equipment.

Provisions are defined in order to face several accidents on the different units of a given site. Site autonomy with HSC should be sufficient to maintain safety functions at least until off-site provisions are set in place, i.e. 48 to 72 hours. Off-site resources will then be deployed to back up on-site equipment and to manage accidental situations in the long-term (e.g. human resources, mobile electrical supplies, pumps…). In France, Electricité de France already set up a Nuclear Rapid response Force (FARN) in this objective. Figure 3 shows how the HSC contributes to reinforce the DiD.

Discussions are still on-going in France to define the "beyond design basis hazards", including associated characteristics, and the methodologies to design or verify HSC provisions. Indeed, the two aspects are strongly linked: there is no interest to consider a severe hazard "intensity" if the rules used for equipment design give poor confidence in the capability of the HSC to perform its functions. A global well-balanced approach should be applied.

5. A CONSOLIDATED APPROACH FOR FUTURE REACTORS

Given the feedback on operating experience related to natural hazards, in particular the Fukushima accident, it is essential to re-examine, for future reactors, the way such events are taken into account at the design stage.

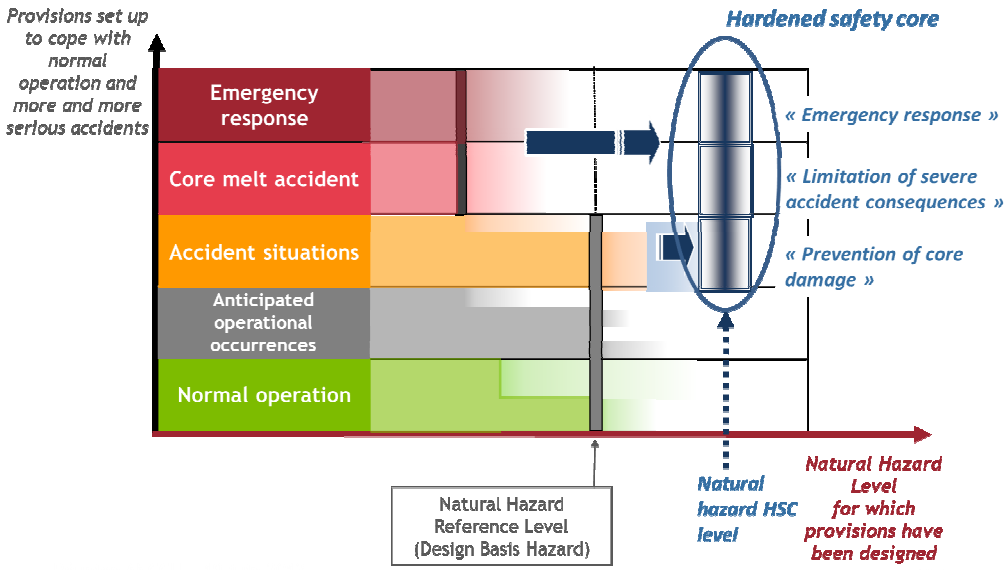

FIG. 3. Implementation of a "Hardened Safety Core" to reinforce the Defence-in-Depth regarding natural hazards on existing reactors.

In this perspective, the comparison between probabilities of internal events and probabilities of "design basis hazards" taken into account in the safety case for existing NPPs shows that the risk associated with external hazards may be higher, if not much higher, than the risk associated with internal events: the probability to have hazards that go beyond the "design basis hazards" (up to ~ 10^{-2} to 10^{-4}/y depending on the hazard) and the internal events probabilities considered in the safety case are not consistent (see Figure 4). In any case, there is no formal demonstration that respective risks are in the same order of magnitude, even for generation III reactors despite the fact that requirements were expressed in this way ("*external hazards must not constitute a large part of the risk associated to nuclear power plant of the next generation*" [1], [2])).

As seen in Section 2, it has always been considered that a natural hazard could not induce core damage. After the Fukushima accident, it is of course necessary to reconsider this position and evaluate the probability of core damage due to beyond design natural hazards. Taking into account the exceeding probability associated with "design basis hazards" on one hand, rules used to design and qualify SSCs or protective measures and resulting safety margins on the other hand, it is not obvious to conclude on the probability of resulting plant configurations and then to take position on the sufficiency of provisions against natural hazards, especially if one refers to the objective fixed in terms of global core damage frequency.

Generally, escalation will be sought for the protection of facilities against natural hazards (see Figure 5):

- Natural hazards considered in the design of the facility must not lead to accident sequences, in particular core damage [2] ("Natural hazards reference design" domain);
- Beyond design natural hazards should not lead to a cliff-edge effect in terms of releases in the environment ("Natural hazards design extension" domain). It means that if core damage could not be avoided, consequences to the environment should be compatible on-site interventions and do not necessitate the implementation of off-site countermeasures in large areas.

At the end, the sufficiency of the provisions set up to protect the plant against hazards should be assessed regarding the general plant safety objectives fixed in terms of global core damage frequency for the design and of limitation of consequences for a severe accident situation.

The list of SSCs that need to be protected against natural hazards should include, in addition to SSC that fulfil the three fundamental safety functions, SSC needed to monitor the situation in order to: (i) operate the plant in accidental conditions, (ii) diagnose the plant configuration, in particular the state of the containment barriers, and (iii) assess current and potential releases outside the site and consequences for the population.

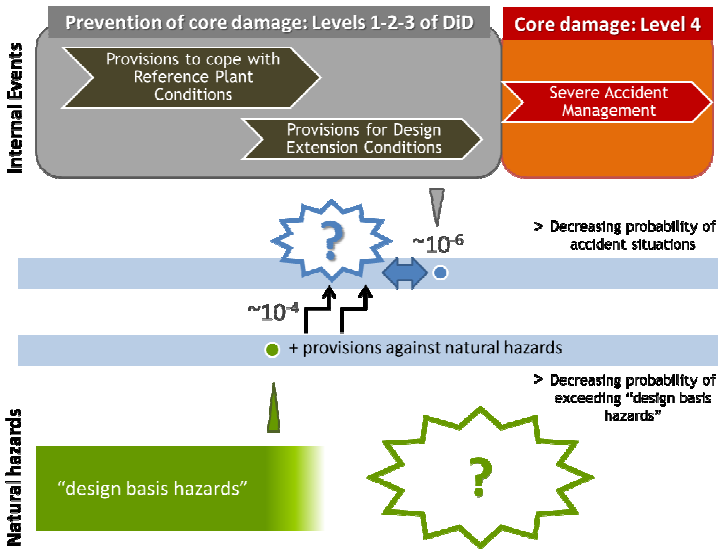

FIG.4. Situations considered to design/protect provisions.

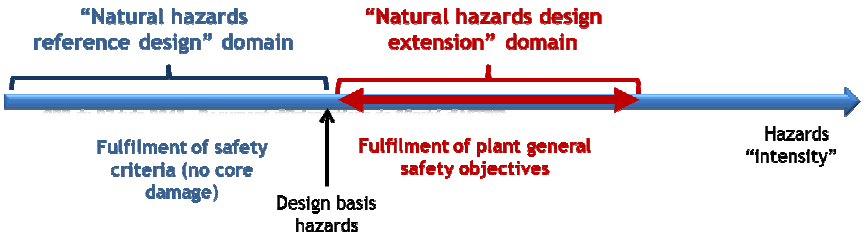

FIG. 5. Approach proposed to reinforce the Defence-in-Depth for new reactors regarding natural hazards.

5.1. Natural hazards reference design: prevention of accidents, in particular core damage

Preliminary discussions in France for future reactors led to propose an approach including the following steps:

- Prevention of natural events: the only way is to choose a site with low risks of natural hazards;
- Definition of the list of hazards to take into account in the design and detailed characterization (maximum accelerations for earthquakes, water levels and durations for flood…);
- Limitation of the impact of natural hazards in the installation: important for safety SSCs should be designed or protected against hazards, considering that hazards may affect at the same time several units of a given site; accident long-term management; due combination of hazards, eventually with internal events, should be examined (in particular for hazards with a lower "intensity" than "design basis hazards", but which have a higher frequency);

- Definition of provisions to take into account the failure of design protective measures: conventional rules on the way to consider the failure of protection measures defined in the preceding step should be determined.

All NPP operating states should be considered. As far as possible, passive protections against natural hazards, i.e. not requiring human actions or energy supply should be implemented.

The definition of "design basis hazards" is challenging in a context of limited data and safety assessment exploratory methods. It may be difficult to determine hazards with a very low exceeding probability with a high level of confidence (high percentile). Nevertheless, it is essential to have a safety level well-balanced between internal and external events. Then, objective defined in terms of global core damage frequency for the plant, including uncertainties, should be taken into account as an input for the definition of the "design basis hazards".

5.2. Natural hazards design extension: limitation of consequences

The list of hazards and hazard combinations to be considered in the "natural hazards design extension" must be established on the basis of the analysis of potential cliff-edge effects in terms of releases into the environment, when going beyond load cases considered for the design of reference. Hazards considered should correspond to exceeding probabilities significantly lower than probabilities used for reference design, with a high level of confidence.

For this domain, a specific demonstration of the capability of the plant to face hazards without important releases should be required.

In order to limit the risk of common cause failure and to reduce the risk of induced effects on "hazards design extension", provisions should be as far as possible independent from the other plant equipment.

Moreover, to take into account long-term situations after such natural hazard, additional provisions should be defined for repairing equipment, connecting off-site mobile means to extend site autonomy (with predefined on-site hook-up points). In this frame, off-site provisions should be defined to complete on-site ones, considering possible difficulties to access the site.

6. CONCLUSIONS

The review of current approaches to deal with natural hazards in the safety case pointed out many issues that need to be better addressed, despite all improvements set in place since the initial design of operating plants, concerning hazards identification and characterization and protective measures.

Further improvements are necessary in order to get more consistency with the "Defence-in-Depth" approach used for internal events and to demonstrate that provisions taken regarding natural hazards are sufficient to fulfil plant general safety objectives.

In France, the definition and the implementation of a post-Fukushima "Hardened Safety Core" for operating NPPs should compensate for some weaknesses in the current approach and improve significantly the robustness of the installations against natural hazards. For future reactors, a new approach based on the definition of two domains for natural hazards, "design basis" and "design extension", is examined.

The question of developing an equivalent approach for other external hazards, e.g. those induced by human activities and malevolent acts should be examined as well.

It turns out that safety assessments related to natural hazards raise some challenges and difficulties, especially to characterize events with very low frequencies in a context of limited data, to define combinations of hazards (eventually with internal events) and to consider events that go beyond the design basis. For these issues, international guidance and discussions may be fruitful.

REFERENCES

[1] Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with PWRs, GPR/German experts plenary meetings, 19-26 October (2000).

[2] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), Reactor Harmonization Working Group Report on Safety of New NPP Designs (2013).

APPLICATION OF THE DEFENSE-IN-DEPTH CONCEPT IN THE PROJECTS OF NEW-GENERATION NPPS EQUIPPED WITH VVER REACTORS

YU. V. SHVYRYAEV, V. B. MOROZOV, A. YU. KUCHUMOV
JSC Atomenergoproekt,
Moscow, Russian Federation
E-mail: morozov@aep.ru

Abstract

The projects of new-generation NPPs equipped with VVER reactors are developed as projects the safety level of which is superior to that of NPPs that are currently in operation. The main design solutions adopted for implementing the defence-in-depth (DiD) concept in the projects of new-generation NPPs equipped with VVER reactors are briefly characterized in the paper.

1. THE OBJECTIVE AND MAIN PROVISIONS OF SAFETY ASSURANCE

In accordance with the requirements of the Russian regulatory documents [1, 2] and the IAEA documents [3, 4], the fundamental objective of safety assurance in the projects of new-generation NPPs equipped with VVER reactors is to protect the personnel, population, and environment from radiation hazard [1, 2] or from excessive risk of inflicting radiation-induced harm [3, 4] during NPP operation.

2. APPLICATION OF THE DEFENSE-IN-DEPTH CONCEPT

The above-mentioned targets are achieved in the projects of new-generation NPPs by applying the main principles and requirements of the defence-in-depth (DiD) concept [2, 4].

2.1. Radiation sources and safety barriers

The main sources of radioactivity (RS) that contain the largest amounts of radioactive substances and present a potential hazard of inflicting radiation harm are the nuclear fuel in the reactor core (NF in the RC) and spent nuclear fuel (SNF) in the fuel pool (FP).
The design and neutron-physical characteristics of nuclear fuel and the designs of the reactor core and fuel pool exclude the occurrence of spontaneous uncontrolled chain nuclear reactions in all possible states of the NPP, including severe accidents involving complete destruction and melting of nuclear fuel.

Physical barriers preventing release of radioactive substances and radioactive radiation from radiation sources into the environment serve as safety barriers. These barriers include the following:

- the fuel matrix and claddings of fuel rods forming the nuclear fuel;
- the reactor vessel, pipelines, and other equipment containing the coolant cooling the NF in the RC;
- the FP building structures, pipelines, and other equipment containing the coolant cooling the SNF in the FP;
- the double-shell reinforced-concrete containment with a leak-tight steel liner and the inner containment prestressing system, the system for passively removing hydrogen from the inner containment volume, and with the system for passively filtering the space between the inner and outer containments; and
- the biological shielding.

2.2. Classification of elements according to their effect on safety

In accordance with [2], the term "elements" means buildings, structures, equipment casings, pipelines, thermal equipment, electrical equipment, instrumentation and control devices, etc.

The main objectives of carrying out classification consist of estimating the extent to which failures of elements affect safety with separating elements important to safety (EIS) and ranking them into safety classes.

In accordance with [2], EIS are subdivided into the following safety classes 1, 2, and 3, the proper (acceptable) levels of quality and reliability of which are achieved in the design, manufacture, and construction and maintained during operation by adopting the following design solutions:

- applying standards containing the most stringent requirements imposed on the quality and reliability of elements related to safety classes 1 and 2;
- using elements related to class 3 the acceptable reliability of which has been proven by field experience gained at operating NPPs;
- assurance of proper reliability levels (i.e., acceptably low levels of conditional probabilities of dependent failures) of EIS by providing sufficient safety margins with respect to loads caused by on-site and external effects;
- design, manufacture, and construction of EIS by organizations having licenses from the regulatory authority for carrying out the relevant kinds of activities, in accordance with the technical requirements specified by the NPP General Designer and the General Designer of the reactor plant; and
- keeping the acceptable reliability level during operation by monitoring the state and carrying out maintenance and repairs of EIS.

2.3. Postulated initiating events

For working out design solutions on safety assurance, full lists of PIEs are determined, the occurrence of which leads to upsetting normal operation (NO) and generates the need to actuate the protective systems of NO or safety systems (SSs) to prevent the preset damage limits of radiation sources and the limits of radiation effect (safety limits) from being exceeded.

Depending on the occurrence rates and systems the operation of which prevents the safety limits established in the design from being exceeded, all PIEs are subdivided into the following categories:

- Category 2 encompasses PIEs anticipated during NPP operation, that may occur one or more times during the power unit service life (i.e., with an occurrence rate of higher than 10^{-2} 1/year) as a consequence of failures of systems and elements the operation of which is necessary for implementing technological processes and conditions. Violation of the preset operational limits and occurrence of design-basis accidents in the case of such events are prevented through the operation of the protective NO systems incorporated in the project. Such systems perform the functions of bringing the reactor into subcritical state (the reactor preventive protection system), creating the shutdown concentration of boric acid (the normal volume and boric acid control system), and removing decay heat from the reactor core (the normal heat removal

systems through the secondary and primary coolant circuits). Design operation of NO protective systems prevents the occurrence of PIEs of design-basis accidents and creates conditions for eliminating deviations from normal operation by restoring serviceability of failed elements with subsequently returning the power unit in the NO states at Level 1 of DiD:

- Categories 3 and 4 cover PIEs of design-basis accidents (DBAs) the occurrence rates of which lie in the range 1.0E-04 – 1.0E-02 1/year for category 3 and in the range 1.0E-06 – 1.0E-04 1/year for category 4. PIEs of DBAs encompass both single internal events (which occur as a consequence of single failures of elements or human errors), on-site events (which occur due to the effect of fires, floods, etc. in NPP premises or in the NPP site) and external events (of natural or man-made origin). The project incorporates full lists of PIEs of DBAs, including the categories of internal, on-site, and external events for all operational states of the power unit:
    - operation at full or decreased power;
    - startup and shutdown modes; and
    - outages for refueling and planned maintenance and repair operations.

  To reduce the amount of deterministic and probabilistic safety assessments, the PIEs of DBAs are united in a few groups with the same sets of required safety functions, their success criteria, and safety system configurations for individual PIEs of DBAs included in each group, the main ones being as follows:
    - leaks from the primary coolant circuit inside the containment;
    - primary-to-secondary leaks;
    - leaks from the primary coolant circuit to outside of the containment;
    - transients without leaks from the primary coolant circuit involving failures of normal heat removal systems from the reactor core;
    - degradation of normal heat removal from the SNF in the FP; and
    - failures of support safety systems causing loss of heat removal by active SSs to the ultimate water heat sink (water in the spray ponds).

Violation of the safety limits established for design-basis accidents and occurrence of beyond-design-basis and severe accidents in the case of such events are prevented through the operation of safety systems incorporated in the design basis with reaching control state and then safe state. Justification of reaching safe state is based on conservative acceptance criteria and design rules (Single Failure Criterion, etc.)

2.4. Beyond-Design-Basis Accident conditions

The BDBA conditions can be interpreted as IEs, which are not addressed in design basis as well as complex sequences, initiated by PIEs, but characterized by at least one event in sequence in addition to the independent failure which is postulated in accordance with Single Failure Criterion (SFC). BDBA IEs may occur with frequency less than 1.0E-06 1/year. The BDBAs reflect the two sets of accident scenarios: first can be mitigated by operation of safety systems and extra engineering features and second that includes severe accidents.

For the first one the safety goal typically corresponds to limits established for design-basis accidents, however, assuming more flexibility in analysis methods and acceptance criteria. Among all set of these scenarios the comprehensive list, which covers scenarios with

largest frequency to be identified and considered in the design as Design Extension Conditions. The engineering features and means include the following:

- any engineering features available at the NPP irrespective of their initial purpose;
- supplementary engineering features and measures to control BDBAs.

3. APPLICATION OF THE DID CONCEPT IN DESIGNING SAFETY SYSTEMS

3.1. Safety functions

Safety systems are intended to perform the following basic safety functions (SFs):

- SF1. Bringing the reactor into subcritical state and maintaining it in this state in the entire range of the reactor coolant system parameters, including the parameters corresponding to the power unit cold shutdown state;
- SF2. Decay heat removal from reactor and spent fuel pool;
- SF3. Confinement of radioactive substances;

Each basic function in specific conditions of accident can be subdivided, in turn, into a number of more specific functions, like:

- SF2.1. Maintaining the inventory of coolant in the reactor core;
- SF2.2. Isolating a faulty steam generator from the surrounding medium in the case of primary-to-secondary leaks;
- SF2.3. Heat removal and cool-down of the reactor plant through the secondary coolant circuit.

3.2. Main deterministic principles and requirements of the DiD concept

Acceptable reliability of performing safety functions is achieved through applying the main deterministic principles and criteria of the DiD concept in designing SSs listed below.

3.2.1. The redundancy principle

An additional (excessive) quantity of systems, trains, or elements is included in the SS configuration above that minimally required for successfully fulfilling the safety functions. The following kinds of redundancy are used in the design:

- functional-system redundancy, in accordance with which the configuration of safety systems consists of several (two or more) systems differing from each other in operating principles (active or passive) and able to perform, independently of the other ones, the relevant safety function;
- structural redundancy, according to which the SS configuration consists of a few trains that operate based on the same principle and consist of elements having the same or different designs;
- redundancy in time, according to which time windows are used in the design for the restoring the serviceability of the failed SS, or using supplementary engineering features and measures.

3.2.2. The diversity principle

In accordance with functional-system redundancy, or use of components based on different principles of operation, different in design or manufactured in different companies are used in the NPP design.

3.2.3. The principle of independence

Redundant systems and trains as much as possible do not have common parts (elements) single failures of which could lead to a failure to perform the safety function as a whole and shall be protected from onsite and external effects.

3.2.4. The single failure criterion

The SS configuration shall retain its ability to perform the preset safety functions taking into account the failure of anyone of its active elements or passive elements having moving mechanical parts independent of the initiating event at which the mission of this system is required.

3.2.5. The requirement of providing protection from common-cause failures (CCF)

The SSs shall retain their ability to perform the intended safety function under the effect of factors or events that may be caused by errors in design, manufacture, construction, and operation, as well as under the effect of onsite and external influencing factors. The adequate immunity of SSs with respect to CCFs is achieved by applying the principles of diversity, independence, and protection from human errors.

3.2.6. Improved reliability

The requirement of ensuring more reliable performance of safety functions (i.e., lower conditional probabilities of failure to perform the safety function) with respect to PIEs of DBA with higher occurrence rates.

4. BRIEF CHARACTERIZATION OF THE SS CONFIGURATIONS ADOPTED IN THE PROJECTS

4.1. General Solutions Adopted for the NVNPP-2 Project

The objective of developing the NVNPP-2 project was to construct the pilot NPP unit based on the AES-2006 (third-generation of NPPs with light-water reactors), which shall possess, as compared with the reference power units at NPPs equipped with VVER-1000 reactors, an increased power capacity, better technical-economic and performance indicators, and enhanced safety level. The basic AES-92 project having a EUR certificate was taken as the basis for working out the NVNPP-2 project.

Two power units are supposed to be constructed at the NVNPP-2 site.

At present, the NPP construction process is close to completion, and the progress of works is in accordance with the adopted schedule.

In accordance with the defence-in depth (DiD) concept, the NPP project incorporates protective normal operation systems (DiD 2 level) intended to overcome anticipated operational occurrences (with an occurrence rate from 1.0E-02 1/year or higher) and safety systems intended (taking into account the single failure criterion) to bring the power unit into safe state in case of all initiating events postulated in the project that lead to upsetting the DiD 2 level.

The list of postulated initiating events of design-basis accidents includes events with an occurrence rate in the range from 1.0E-06 1/year to 1.0E-02 1/year. The safety systems and

their elements, as well as the buildings in which they are placed are designed taking into account the requirement of their being able to perform their functions in case of external effects typical for the NPP site with an occurrence rate of up to 1.0E-04 1/year (natural effects) and up to 1.0E-06 1/year (man-made effects).

The following safety principles were laid as a basis for safety substantiation in working out the basic AES-2006 project for the conditions of the NVNPP site in accordance with the process-related safety concept:

- each safety system (be it a protective, support, or control system) includes two active trains, and each of them is able to fully perform the safety function imposed on the system. The configuration of the front-line safety system trains (with redundant elements inside the train) has been defined proceeding from compliance with the single failure principle for active elements, as well as for passive elements having moving parts; in addition, functional redundancy is used in the reactor core flooding systems that have dependent failures in case of LOCAs;
- to this end, a combined ejecting pump is used in the high-pressure ECCS, which is characterized by efficient performance at medium and low pressure in the RP, due to which reliable core flooding is ensured in case of failure of low-pressure pumps under the conditions of large-break leaks from the reactor coolant system;
- emergency removal of heat from the SGs and reactor plant cool-down operations are performed by the closed-loop emergency cool-down system (ECS), each train of which comprises two pumps connected with one pair of SGs. Operation of the ECS in the cool-down mode jointly with the HA-1 makes it possible to reduce pressure in the RP in case of failure of the ECCS pumps to the working range of the EPCS system pump, due to which flooding of the reactor core is ensured in the case of small- and medium-break leaks;
- the scope of front-line systems performing the functions of removing residual heat release from the reactor core also includes passive systems: the system for passive removal of heat from the SGs fitted with air-cooled heat-transfer modules (PHRS) and the supplementary system of hydro accumulators serving to flood the reactor core in case of LOCA accidents that take place at low pressure in the RP.

To achieve better reliability, the design of safety systems implements the "combination principle", according to which the safety functions are combined with normal operation functions. With such an approach, protection from common-cause failures is ensured.

In accordance with the PSA recommendations, the project incorporates redundancy of active elements in the trains of support systems except with the diesel-generators (DGs).

The project incorporates means intended to protect safety systems from onsite effects (fires, floods, steaming, steam-water jets, missiles, and whipping of pipelines in the NPP premises). Protection from such effects is ensured by implementing the principle of physical separation, i.e., by placing the equipment of individual safety trains in separate rooms segregated from each other by distance or protective barriers, and also by reliably fastening the equipment. Table 1 presents the configuration of safety systems.

TABLE 1. STRUCTURE OF SAFETY SYSTEMS ADOPTED IN THE NEW VVER PROJECTS

Name of safety system	System structure
High-pressure ECCS	An active two-train system equipped with fully-variable combined pumps (2x100% trains)
Emergency and planned coodown system (EPCS)	An active two-train system (2x100% trains)
Emergency boron injection system JND	An active two-train system (2x100% trains)
SG emergency cooldown system (ECS)	A closed-loop active two-train system (2x100% trains)
ECCS passive part (HA1-)	A four-train passive system (4x33% trains)
Supplementary passive core flooding system (HA-2)	A four-train passive system (4x33% trains)
Passive heat removal system (PHRS)	A four-train passive system (4x33% trains) fitted with air-cooled heat exchangers
Passive annulus filtration system (PAFS)	A four-train passive system (4x33% trains)

4.2. Layout Solutions applied for the reactor building

The reactor building (UJA) consists of a double-shell cylindrical reinforced-concrete containment, which encloses an accident confinement area and of a set of adjoining structures resting on a common main building's foundation raft (Figure 1).

The reactor building has a fully symmetrical layout, due to which it becomes possible to separate the equipment of different safety trains both physically and spatially. The containment is a component of the isolation system and consists of two shells an inner one and an outer one; the latter is intended to protect the building from external impacts. The space between the shells (called the annulus) is used for collecting radioactive leaks penetrating through the inner containment during accidents.

The accident confinement area inside the sealed containment is occupied by the reactor plant and systems connected to it, the spent fuel pool, and the ventilation systems and equipment required for carrying fuel handling operations and repairs.

Located on different sides of the reactor cavity are the fuel pool and the shaft for inspecting reactor internals, reactor coolant circuit boxes containing steam generators, RCPs and reactor coolant pipelines, the pressurizer, the pressure relief tank, and reservoirs of the quick boron injection system.

The 1^{st}- and 2^{nd}-stage ECCS hydro accumulators are located at the maintenance elevation +26.300 m. The passive heat removal system (PHRS) is arranged on the external side of the outer containment dome and cylindrical part. The PHRS heat exchangers are arranged over the containment perimeter.

4.3. The Basic VVER-TOI Project as a Further Development of the AES-2006 Project

The VVER-TOI project was developed with a view to work out a standard (basic) project of a large-capacity NPP able to compete in the market with the products offered by rapidly developing and recognized leaders in the field of nuclear power engineering.

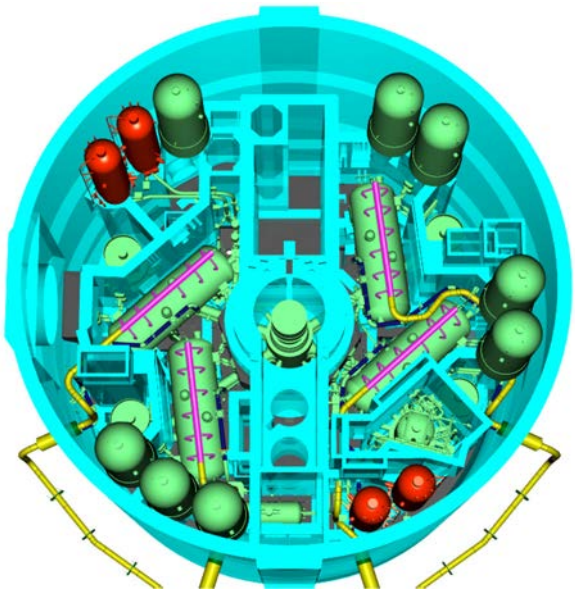

FIG.1. Reactor building layout.

Specialists who worked out the project pursued the goal of creating and introducing modern information technologies for design, engineering, and management of information on the plant in all stages of its lifecycle.

A comprehensive information model of an NPP has been developed as a result of the performed works. Suitability for serial production and a shorter construction period have been achieved as compared with the AES-2006 project.

The main characteristics of the two projects are given below in Table 2. The general layout of a two-unit NPP of the VVER-TOI project is shown in Figure 2.

TABLE 2. THE AES-2006 AND VVER-TOI PROJECTS

Key indicators	AES-2006	VVER-TOI
Power unit electrical capacity	1 198 MWe	1 255 MWe
Power unit (RP) service life	50 years	60 years
Power unit gross efficiency for annual average conditions	37.4%	37.9%
Availability factor (with a 18-month fuel cycle)	91%	93%
Plant independent survival time in case of BDBA	24 h	72 h
DNE/SSE	6/7 points	7/8 points
Design option for SSE (on the Customer's request)	-	9 points
Aircraft crash (a design-basis initiating event)	5.7 t	20 t
Heavy aircraft crash (a beyond design-basis event)	-	400 t
Time of construction	54 months	48/40 months
Power consumption for plant auxiliaries	7%	6.47%
Amount of SRWs	50 m3/year	44.5 m3/year
Specific area of occupied land for main production	272 m2/MW	200 m2/MW
Specific civil construction volume of the reactor and reactor auxiliary buildings	380.89 m3/MW	340.8 m3/MW
Turbine unit	High-speed	Low-speed

FIG.2. Genral plant layout (two-unit VVER-TOI).

4.4. Main Technical Solutions on the Safety Systems Adopted in the VVER-TOI Project

The safety assurance concept adopted in the VVER-TOI project is based, as in the AES-2006 project on applying active and passive safety systems having different principles of their operation. Active SSs have a two-train structure, and each train has a 100% capacity. In order to achieve a longer time of independent survival under the conditions of BDBAs involving failure of active systems, the project incorporates supplementary (3^{rd}-stage) hydro accumulators, which in case of BDBA guarantee, jointly with operation of the PHRS, maintaining controlled state of the shutdown reactor for no less than 72 h without any intervention of the personnel at any postulated IE. Storage batteries for long-term operation are also included in the project.

The main technical solutions on safety systems in the VVER-TOI project are also reflected in Figure 3.

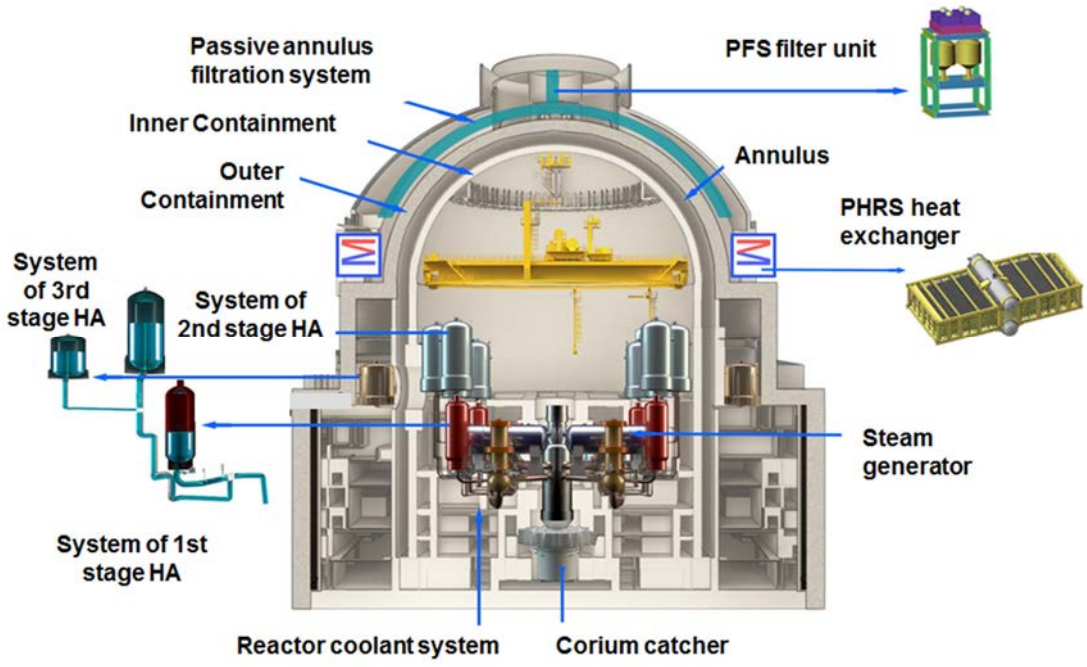

FIG. 3. VVER-TOI main design solutions for safety systems.

4.5. Supplementary Measures Aimed at Control of BDBAs

In case of accidents evolving under the conditions of multiple failures of elements in active SSs (e.g., common-cause failures of inner nature) the time interval equal to 72 h from the accident onset moment is sufficient for taking corrective measures on restoring equipment, as a result of which the NPP is transferred from controlled state into safe state.

However, in the light of the accident that occurred at the Fukushima NPP, during which extreme (off-design) natural events led to multiple failures that are not removed for a long period of time and eventually to a severe event, the VVER-TOI project incorporates supplementary systems ensuring safety in the following extreme situations:

- SBO (total loss of all AC sources including emergency ones);
- loss of all ultimate water heat sinks; and
- a combination of the above-mentioned events.

In the above-mentioned cases, after exhausting water inventories in the hydro accumulators, if attempts to restore normal or emergency power supply were not met with success, makeup of the reactor and fuel pool is organized using pump sets powered from a mobile air-cooled diesel generator (water may be inaccessible as DG cooling medium), as well as heat removal by means of a dry mobile cooling tower. The operating principle of these systems is presented below in Figure 4.

Similar supplementary systems were introduced in the NVNPP-2 project based on the results of performed tests.

It should be noted that described above measures are effective at shutdown state, in which Passive Heat Removal System via steam generators is not available.

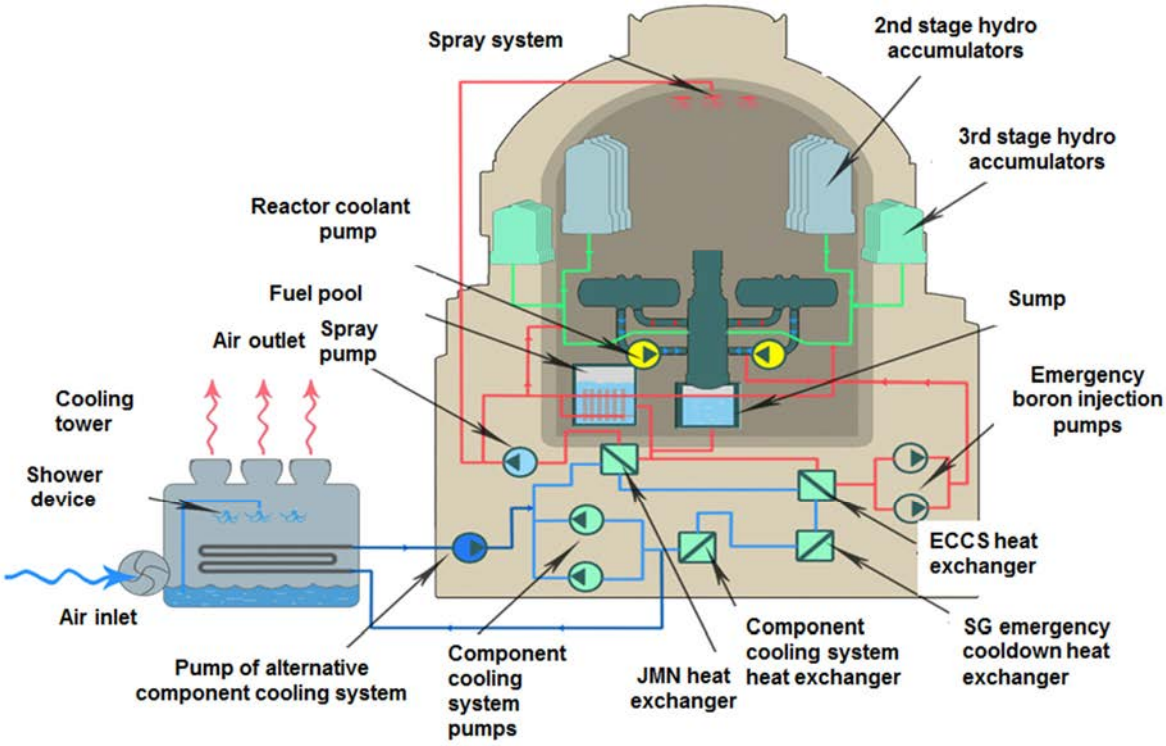

FIG. 4. Supplementary safety systems.

4.5.1. Protection from Airplane Crash

The VVER-TOI project, incorporates more enhanced - as compared with the NVNPP-2 project - protection from accidents caused by aircraft crashes. At present, such accidents, along with extreme natural phenomena, are regarded as one of the main risk factors in the subsequent decades. The VVER-TOI project takes into account recommendations formulated in the new revision of the EUR document and in the WENRA documents. The characteristics of the considered events with regard of the design aircraft and a large commercial aircraft are given below in Fig 5.

5. CONCLUSIONS

The following conclusions can be drawn from analysis of new VVER NPPs design:

1. The up-to-date principles, criteria, and requirements pertinent to the DiD concept have been applied for new-generation NPPs equipped with VVER reactors. Traditional for VVER NPPs active SS structure for these projects include two separate independent trains with internal redundancy, which at unit power operation state fully met all deterministic criteria, in particular SFC.
2. Use of passive SS (PHRS, HA) makes it possible to guarantee performing safety functions in conditions of CCFs in active SS, including total loss of active SS for 24h (VVER-2006) and 72h (VVER-TOI).
3. Both designs are adequately protected against external (natural and man-made) hazards. Along with this, PHRS uses atmospheric air as ultimate heat sink, which serves for many kinds of external events that result in loss of main heat sink (water) for a long time period together with LOOP.
4. In order to provide protection against CCFs in support systems, as well as total loss of these systems due to external hazards at shutdown state, the extra engineering features is used.
5. All this decisions make possible an achievement of acceptably low risk indicators considering all categories of internal, onsite, and external PIEs and for all unit operational states. This is confirmed by PSA results, presented in different paper.

Mass, t	Velocity, m/s	Impact spot, m²	
LearJet 23 (considered in the NVNPP-2 project)			
5.7	100	12	
Phantom RF-4E – a design-basis initiating event			
20	215	7	
Boeing 747-400 – a beyond design-basis initiating event			
400	150	50+50	

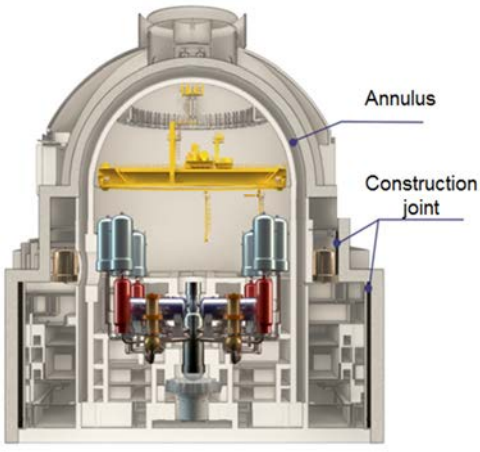

FIG. 5. Airplane crash protection.

REFERENCES

[1] Federal Law of the Russian Federation No. 170-FZ "About the Use of Atomic Energy."

[2] General Provisions for Ensuring Safety of Nuclear Power Plants, OPB-88/97, Moscow (2001).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

ADVANCES AND CHALLENGES IN THE IMPLEMENTATION OF DEFENCE IN DEPTH IN COMMISSIONING AND OPERATION (TOPICAL SESSION 2)

INVITED PRESENTATION

A DISCUSSION ON RISK IN COMPLEX OPERATIONAL SETTINGS

K. ELLIS
WANO, London, United Kingdom
Email: ken.ellis@wano.org

Many apparatus today are complicated in that they consist of many components. The risk associated with these complicated apparatus is a product of their unreliable system components and sub-components. The components are a collection of inter-related individual components/ sub-components that can be correlated in a direct cause and effect manner and thus failures can be historically retraced or predicted.

Once the confines of the complicated apparatus is extended to include such inputs as humans operating the equipment, man-machine interfaces, multiple processes surrounding the operation of the apparatus, etc., the whole system becomes complex. Complex systems are based on interdependencies versus dependencies, and risk becomes a product of improperly aligned or poorly integrated activities. Cause and effect becomes more loosely coupled and both path and circumstance dependent.

To better understand and improve our defence in depth strategies we need to better understand and discuss complex systems and hence allow better erection of protective barriers.

INVITED PRESENTATION

LESSONS LEARNED FROM PROCESS SAFETY MANAGEMENT: A PRACTICAL GUIDE TO DEFENCE IN DEPTH

N. LANGERMAN
Advanced Chemical Safety, Inc., SAN DIEGO,
USA
Email: neal@chemical-safety.com

Beginning with the experiences of Alfred Nobel, the chemical enterprise has learned from failures and implemented layers of protection to prevent unwanted incidents. Nobel developed dynamite as a more stable alternative to nitroglycerin, a process we would today call "inherently safer technology". In recent years, the USA has issued regulations requiring formal "risk management plans" to identify and mitigate production risks. The USA set up the "Chemical Safety and Hazard Investigation Board" as an independent investigator of serious chemical enterprise incidents with a mission to issue recommendations aimed at preventing repeated incidents based on lessons learned. Following a particularly violent explosion in Texas in 1989, the US Occupational Safety and Health Administration issued the "Process Safety Management" (PSM) rule.

PSM is a singular guide to defence in depth for preventing large-scale production incidents. The formalism is equally applicable to the chemical enterprise and the nuclear installation enterprise. This presentation will discuss the key elements of PSM and offer suggestions on using PSM as a guide to developing multiple layers of protection. The methods of PSM are applicable to Nuclear Generating Stations, research reactors, fuel reprocessing plants and fissile material storage and handling. Examples from both the chemical and nuclear enterprises will be used to illustrate key points.

INVITED PRESENTATION

LESSONS LEARNED AFTER NUCLEAR POWER PLANTS AND HYDRO-POWER PLANTS ACCIDENTS

A. MOSKALENKO
GCE Group, Saint Petersburg, Russian Federation
Email: gce@gce.ru

The World is becoming more open and free for communication. However, the experience (positive or negative) is still badly cross over sectorial borders. I would like to illustrate the point with the examples, even with several unexpected ones. I would like to start with a few words regarding the Sayano – Shushenskaya Hydro Power Plant accident and the factors that caused it.

Sayano – Shushenskaya Hydro Power Plant is a unique Hydro Power Plant with efficiency factor of 96 %. Nevertheless, the efficiency factor, in particular, caused a series of restrictions: hydro-electric units vibration amplitude must not exceed 4 micron!!!

(Slide 1: Vibration amplitude dependence on output capacity)

As it is clearly seen, there is a so called “prohibited area”, which the hydro-electric unit must pass over. Operations in the area are prohibited in accordance with the regulatory documents. However, due to the changes that occurred in Russian power supply industry, the hydro-electric unit passed through the prohibited area more than 12 times, if we take into account only the day of the accident.

The bolts keeping the turbine cover, keeping water apart from the machinery hall, were too much released. The mentioned above reasons led to the hydro-electric unit disruption and the machinery hall flooding. Water inflow was possible to stop by putting down the regulating valves. However, the regulating valves control console was in the flooded machinery hall. There was standby emergency control console, but it was in the machinery hall, as well. The machinery hall was flooded, consequently, main and standby systems were destroyed. Moreover, the machinery hall, where all the units were disposed, was a huge hall without dividing walls, etc. (Photo)

Take a look at the next slide. (Photo – Chernobyl Nuclear Power Plant machinery hall).

Take note of Fukushima–1 Nuclear Power Plant: standby power supply source was situated in the same place and destroyed by water.

All the mentioned facts mean that we miss one of the most important issues - a fail safety factor of all these facilities and the system as a whole, while working up questions regarding nuclear safety, efficiency, and individual units’ advancement.

The most advanced organization in this matter is the Navy, where this particular question is one of the major ones. They have been working for several years in order to find the solution. Particular provisions are doubtless and have saved lots of lives and properties.

1. All the vessels are compartmental (all the rest compartments are safe in case of flooding or fire in the other ones)
2. Standby emergency control consoles, control centres, etc. are disposed in different compartments, far from each other.

LIFE MANAGEMENT AND SAFETY OF NUCLEAR FACILITIES

S. FABBRI, A. DILUCH, G.VEGA
Comisión Nacional de Energía Atómica,
Buenos Aires, Argentina
Email: fabbri@cnea.gov.ar

Abstract

The nuclear programme in Argentina includes: nuclear power and related supplies, medical and industrial applications, waste management, research and development and human training. Nuclear facilities require life management programs that allow a safe operation. Safety is the first priority for designers and operators. This can be attained with defence in depth: regular inspections and maintenance procedures to minimize failure risks. CNEA objectives in this area are to possess the necessary capability to give safe and fast technical support. Within this scheme, one of the main activities undertaken by CNEA is to provide technological assistance to the nuclear plants and research reactors. As a consequence of an increasing concern about safety and ageing a Life Management Department for safe operation was created to take care of these subjects. The goal is to elaborate a Safety Evaluation Process for the critical components of nuclear plants and other facilities. The overall objectives of a safety process are to ensure a continuous safe, reliable and effective operation of nuclear facilities and it means the implementation of the defence in deep concept to enhance safety for the protection of the public, the workers and the environment.

1. INTRODUCTION

The nuclear programme in Argentina includes: nuclear power and related supplies, medical and industrial applications, waste management, research and development and human training. National Commission of Atomic Energy (CNEA) related companies are the following:

- CONUAR S.A.: Nuclear fuel elements.
- FAE S.A.: Special alloys and Zry tubes.
- DIOXITEX S.A.: Uranium supply.
- ENSI S.A.: Heavy water production.
- INVAP S.E.: Aerospace, Hot Cells, Nuclear medicine, and Nuclear Reactors for Research & Isotopes production, etc.

Since September 1994 the organisation of the Argentine nuclear activities consists of three separated companies. CNEA in charge of the research and development of nuclear activities, fuel cycle & supplies, nuclear waste management, operation of the research reactors and other nuclear facilities, and technical support to the Nuclear Power Plants (NPPs), Nucleoeléctrica Argentina Sociedad Anónima (NASA) which operates the two NPPs and the National Regulatory Authority (ARN). The two NPPs in Argentina in operation are, Atucha 1 (CNA 1) placed in Buenos Aires province and Embalse (CNE) in Cordoba province. Atucha 2 (CNA 2) is under the end of the construction (see Table 1). All of them are based on natural uranium as fuel with heavy water moderation and cooling. Atucha 1 and 2 are PHWRs of German (Siemens) design and Embalse is a Canadian (AECL) CANDU reactor. Within this scheme, one of the main activities undertaken by CNEA is to provide technological assistance to the nuclear plants and research reactors. Works on life management are included in these activities. In the past, NPPs life management in Argentina were mainly based on the corrective maintenance concept, based on the replacement of damaged parts detected during the periodical outages. In recent times, as a consequence of an increasing concern about safety and ageing a Life Management Department (LMD) for safe operation was created to take care of these subjects.

The goal is to elaborate a Safety Evaluation Process (SEP) [1] for the critical components of nuclear power plants and other facilities. This means to increase technical assistance with technological developments and methodologies for life management of Systems, Structures and Components (SSCs) in order to prevent accidents due to service failures. Obsolescence of electronic components in nuclear facilities is a common safety issue concern. Nuclear plants that face these situations must determine how to inspect and repair/replace electronic components. Therefore a detailed electronic components safety evaluation process to review the obsolescence consequences is important to safety. The overall objectives of the SEP are to ensure a continuous safe, reliable and effective operation of nuclear facilities.

Argentina has six Research Reactors. Five of them operational and one is temporally shut down. The Table 2 shows the characteristics and location of all Argentinean research reactors and critical assemblies.

2. SAFETY EVALUATION PROCESS DESCRIPTION

A detailed safety evaluation process is the best way to prevent failures and accidents due to ageing consequences on SSCs important to safety. The major objective of the process is to justify that all the components concerned by an ageing mechanism remain within the design and safety criteria. Managing safety aspects of RRs ageing requires implementation of a program for the monitoring, prediction, detection and mitigation of degradation of SSCs important to safety during the research reactor service life. SEP is in practice accomplished by coordinating existing programs including maintenance, periodic testing and inspection, as well as good operational practices, research and development and incorporating lessons learned from operating experience [2]. The SEP review is carried out by periodical analysis to establish the actual status of SSCs regarding degradation from ageing. Degradation mechanisms, which could impact on facilities safety, are promptly investigated so that mitigating programs can be designed. The Safety Evaluation Process is shown in Figure 1.

The safety evaluation process begins during design and construction of a nuclear facility taking in account design features and materials selection. The process continues in operation with surveillance, monitoring, maintenance and repair or replacement. It is very important the review of the potential ageing mechanisms, taking in account the worldwide experience and nuclear facilities information. Evaluation and estimation on time, whether residual lifetime of SSCs will end before foreseen end of life or not, brings safety and availability of the facility.

CNEA also contribute to the efforts in the area of lifetime evaluation and extension, especially in relation to control and instrumentation equipment testing, upgrading or replacements by updated or technologically more advanced designs. Similarly, specific studies are carried out in certain areas looking for improvements, for instance, of degraded radiological conditions relevant for maintenance tasks, degraded risk level in safety systems, operational optimisation in particular with regard to fuel management.

Technological assistance is provided to the power stations through research and development laboratories in the areas of chemistry, materials, nuclear fuels and nuclear reactors. Also the area of non-destructive testing techniques is of utmost importance for the detection, analysis and evaluation of discontinuities and material characterization. They are oriented to the diagnosis of SSCs in order to guarantee safe and reliable operation, without impairing their integrity or properties.

An appropriate testing and inspection plan throughout the different stages of the service life of a component from design, fabrication, assembling and commissioning will supply the necessary information for follow-up of its integrity.

TABLE I. NPPs in Argentina

Unit	Type	Grid connection	Status
Atucha 1	PHWR 360 Mwe	1974	Operation
Atucha 2	PHWR 700 Mwe	----------	Under construction
Embalse	Candu 600 Mwe	1984	Operation

TABLE 2. Research Reactors and Critical Assemblies in Argentina

Facility	Type	Operator	Location
RA-0	Critical assembly	Córdoba University	Córdoba Province
RA-1	Research reactor	CNEA	CAC
RA-3	Production reactor	CNEA	CAE
RA-4	Research reactor	Rosario University	Santa Fe Province
RA-6	Research reactor	CNEA	CAB
RA-8	Critical assembly (Shut down)	CNEA	Rio Negro Province

CAB: Bariloche Atomic Center, Río Negro Province
CAC: Constituyentes Atomic Center, Buenos Aires Province
CAE: Ezeiza Atomic Center, Buenos Aires Province

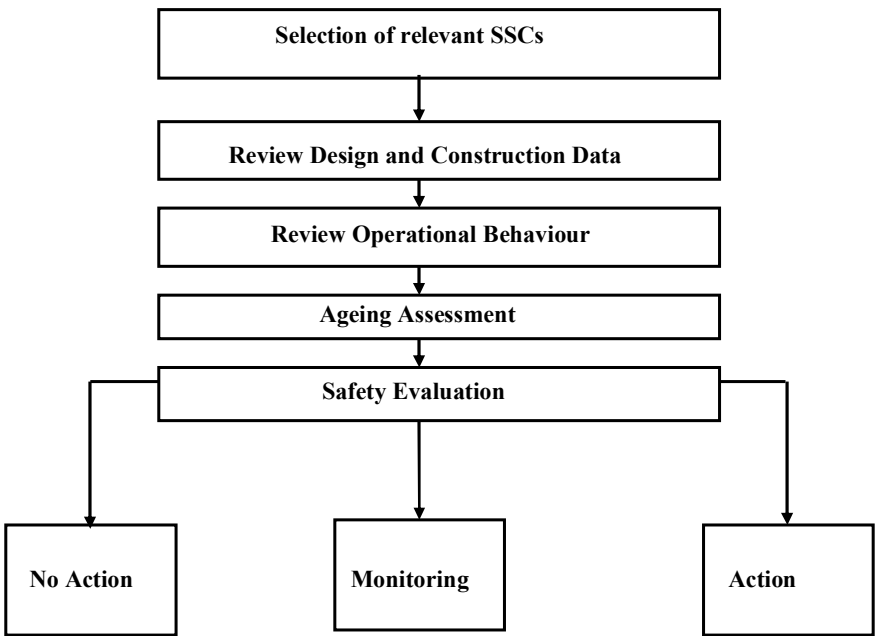

FIG. 1. Safety Evaluation Process.

3. COMPONENTS RELEVANT TO SAFETY

3.1 Mechanical components

Critical components of nuclear plants suffer several types of degradation during operation. Examples include: reactor internal coolant tubes suffer oxidation and hydrogen absorption, irradiation embrittlement, and irradiation creep and growth. The degradation has led to embrittlement and loss of integrity of the component wall. The irradiation growth of the components has also shown a breakaway behaviour. As a consequence of an ageing assessment and a safety evaluation, the decision to replace critical components was taken.

3.2 Heavy components replacement

The objective is to anticipate potential safety risk and to be ready on time to repair or replace components important to the operation of the nuclear plants [3]. Different material degradation mechanisms have been identified on components resulting from the ageing phenomenon. The effects of ageing lead to changes, with time, in the SSC materials, which are caused and driven by the effects of erosion, corrosion, varying loads, flow conditions, temperature and neutron irradiation. Component replacement is often the most feasible solution to solve the effects of ageing. A Heavy Components Replacement Program (HCRP) should be consistent with regulatory requirements. The main points of the program are the following:

- Zero injuries
- Low radiation exposure
- Reasonable cost and time
- Get the right people involved early enough as part of the replacement staff project
- Replacement must be in compliance with safety rules
- Replacement policy should be based in safety criteria and the best economic criteria
- Successful heavy components replacement will enhance safety and economic benefits for the nuclear industry

3.3. Electronic components

Obsolescence of electronic components in nuclear facilities is a common issue concern. A component becomes obsolete when the manufacturer decides to stop production. Nuclear facilities are facing the issue of ageing and obsolete instruments and electronic systems. Circuit boards used in the electronic instrument and control (I&C) systems of nuclear facilities may suffer from ageing failures that can cause unavailability of plant systems [4]. Since nowadays is expected a safe long term operation of nuclear facilities a series of issues can be found:

- analog technologies without technical support,
- unavailable spare parts,
- suppliers that no longer exist,
- equipment without the required functionalities, and
- high maintenance and operation cost.

Nuclear plants that face these situations must determine how to inspect and repair/replace electronic components. Therefore a detailed electronic components safety evaluation process to review the obsolescence consequences is important to safety.

3.4. Concrete degradation

The physical characteristics of a concrete structure can be established, or monitored, by a number of different non-destructive techniques. These techniques could be used to determine the corrosion rate of the reinforcing bars in order to predict the state of the materials. The growth of the corrosion products induces spalling and fractures on the structures. This could be used to graduate the rate at which the damage is introduced and to determine the moment at which the layers are ripe to be removed.

On the other hand, some of the non-destructive techniques are able to detect the placement and characteristics of the steel rebar grid. This knowledge might enable the application of the descaling method to existing structures to be deactivated. The available techniques are the following:

- gamma rays tomography ,
- ultra sonic,
- acoustic emission,
- geo radar, and
- electrical, chemical, and mechanical methods.

4. DEFENCE IN DEPTH DURING DESIGN

DID concept must be implemented during all stages of the plant life cycle. The design of nuclear facilities should comply with all regulatory requirements establish by the Nuclear Regulatory Authority (ARN) including international safety standards. The following concepts are used to enhance safety during the design stage with the objective to protect the public, the workers and the environment:

- **"**Defence in Depth" concept will be applied in all the facility supplying multiple levels and protection barriers against accidental release of irradiated materials. SSCs will be designed with adequate margins to guarantee safe behaviour under operational incidents foreseen and design base events.
- Safety systems will be designed with the redundancy, diversity and independence principles to ensure reliable performance and reduce potential failures mode. Each safety system (or group of systems) will be able to fulfil its safety function even in the event of a failure within the system simple random.
- Whenever possible inherent and passive safety features will be incorporated in the design of systems important to safety, in particular systems that ensure the three basic safety functions: reactor shutdown, heat removal, and containment of radioactive material.
- Passive safety features in the design means those that allow devices to fulfil their safety function without human intervention or active power sources (electricity, compressed air, etc.).
- When an equipment or component has several functions one of which is safety, it should be classified as part of the safety system. The safety role should not be affected by other functions that the equipment or component has been assigned.
- The design must foresee that all the components of safety systems can be adequately inspected and verified before the commissioning and at regular intervals during operation in order to ensure its availability.

5. CONCLUSIONS

As a consequence of an increasing concern about safety and ageing a Life Management Department for safe operation of nuclear facilities was created to take care of these subjects. The goal is to elaborate a safety evaluation process for relevant components of nuclear plants and other facilities. This means to increase technical assistance with technological developments and methodologies for life management of systems, structures and components in order to prevent accidents due to service failures. The overall objectives of a safety process are to ensure a continuous safe, reliable and effective operation of nuclear facilities and it means the implementation of the defence in depth concept to enhance safety for the protection of the public, the workers and the environment.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementation and Review of a Nuclear Power Plant Ageing Management Programme, Safety Reports Series No. 15 IAEA, Vienna (1999).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management for Research Reactors, IAEA Safety Standards Series No. SSG-10, Specific Safety Guide, IAEA, Vienna (2010).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Heavy Components Replacement in Nuclear Power Plants: Experiences and Guidelines, Nuclear Energy Series No. NP-T-3.2 IAEA, Vienna (2008).

[4] U.S. DEPARTMENT OF ENERGY, Evaluating the Effects of Aging on Electronic Instrument and Control Circuits Boards and Components in Nuclear Power Plants, 1011709, Final Report, May (2005).

GUIDANCE ON THE IMPLEMENTATION OF MODIFICATIONS TO MITIGATE BEYOND DESIGN BASIS ACCIDENTS

F. DERMARKAR, J. MARCZAK, M. O'NEILL
Ontario Power Generation,
Pickering,
Ontario, Canada
E-mail: fred.dermarkar@opg.com

Abstract

Following the events at Fukushima, Canadian Nuclear Power Plants (NPP) procured equipment and initiated modifications to improve response capability for Beyond Design Basis Accidents (BDBA). These changes were not typical of other design modifications to the nuclear power plants and reinforced the need for additional guidance for modifications to address BDBA. This paper describes the guidance that was developed to guide the design, procurement, installation, operation, and maintenance of equipment and modifications to mitigate BDBAs. The guidance developed prescribes a graded approach based on a categorization of the nature of the modification. Four categories of modifications are introduced, with the distinction being the degree of interface with existing design basis systems, structures and components (SSCs). This has resulted in a cost-effective means of implementing additional capability to mitigate BDBA conditions, and yet ensure the design basis capability of SSCs is maintained.

1. INTRODUCTION

The Canadian nuclear utilities' decision to pursue station modifications to address the lessons learned from the events at Fukushima, have reinforced the need for guidelines related to plant modifications to address BDBA. The standard processes related to NPP modifications have been developed to stipulate a high degree of rigour to ensure consistency with the design basis of the station. When developing modifications related to BDBA conditions, alternate strategies may be appropriate in some cases. Recognizing the need for guidance to assist the organization in the implementation of modifications to address BDBA, Ontario Power Generation (OPG) established a task team to develop guidance in this area – covering the design, procurement, installation, operation, and maintenance of equipment associated with these modifications. A corporate guide document was generated that outlined the processes to be used for BDBA modifications. As part of the development protocols, the process guide was reviewed by stakeholders – within the company and industry and benchmarked against similar Canadian and international guidance. The process was presented to senior engineering leaders to be challenged and was then accepted. The guidance was rolled out to staff and has been incorporated into OPG modification change control governance. While this paper deals primarily with the OPG BDBA modification process, it is representative of the overall Canadian approach in this area. The guidance, as implemented, is recognized as providing interim direction – that will continue to evolve reflecting changes in national and international requirements.

2. OVERALL OBJECTIVE

The overriding objective of the modification process for BDBA response is to:

- Deliver the required functionality with high confidence under anticipated BDBA conditions. In general, this functionality will prevent or mitigate significant adverse consequences (such as fuel and/or core damage and/or significant radiological releases).
- Ensure that NPP functionality is not compromised under design basis conditions.

The guidance, therefore, must represent a balanced approach to manage the consequences of low frequency, high impact event sequences which are not considered in,

and lie outside of, the design basis of the station. This approach is discussed in the following sections.

3. APPROACH TO MANAGING BDBA CONDITIONS

The approach used to establish the normal design basis reflects the large body of codes, standards, established practices, and operating experience which provides the underlying framework of NPP design and operation. The standard processes related to plant modifications have been developed to stipulate a high degree of rigour to ensure consistency with the design basis of the station. Consequently there is limited latitude for relaxation when addressing BDBA conditions.

For low frequency, high consequence event sequences, where significant uncertainty around the plant conditions which could challenge safe operation exists, strict adherence to "normal" practices may prove to be problematic. For example, in NPP operation, the "symptom based approach" is adopted to ensure that operational strategies provide adequate flexibility. Performance requirements must be met. Yet cost and schedule flexibility are also a consideration.

Figure 1 presents an overview of the OPG approach, and shows the relationship between the design, operations, and regulatory considerations. The referenced procedures in Figure 1 (eg, N-PROC-MP-0090 – Modification Procedure, and N-GUID-01130-10000 – Modifications for BDBA) and regulatory documents (CNSC RD-310 – Safety Analysis for NPP, Siting Guide (SG), and CNSC Consultative Document (C6)) are specific OPG and Canadian regulatory references which delineate process and analysis requirements and safety limits for Canadian NPP.

In developing the Canadian approach to BDBA modifications, regulatory guidance (Canadian Nuclear Safety Commission (CNSC) RD-337 [1] and RD-310[2] were considered – as they provide general guidance regarding the treatment of BDBA from the perspective of plant design requirements and the associated Nuclear Safety Analysis (NSA). CNSC Guidelines (e.g., G-306 [3]) also provide supporting guidance. US NEI 12-06 [4] provides guidance on the "FLEX" approach to BDBA. In addition, IAEA guidelines (e.g., SS-R-2/1 [5] and SS-R-2/2 [6]) also provide guidance on BDBA considerations.

Consistent with the current approach in IAEA guidelines, the strategy developed aligns with BDBA Design Extension Conditions (DEC) and Safety Features for DEC.

3.1 Graded Approach

A graded approach to modifications for BDBA conditions has been adopted within OPG. The graded approach is implemented because it is anticipated that some relaxation of conservatisms is warranted, or even necessary, to address the BDBA conditions in a reasonable and cost-effective manner. These changes from the normal full change control processes are always reviewed and approved, and in all cases, the processes and the resultant modifications are consistent with the Power Reactor Operating Licences of the stations, appropriate engineering codes and standards, and the overall practice of engineering.

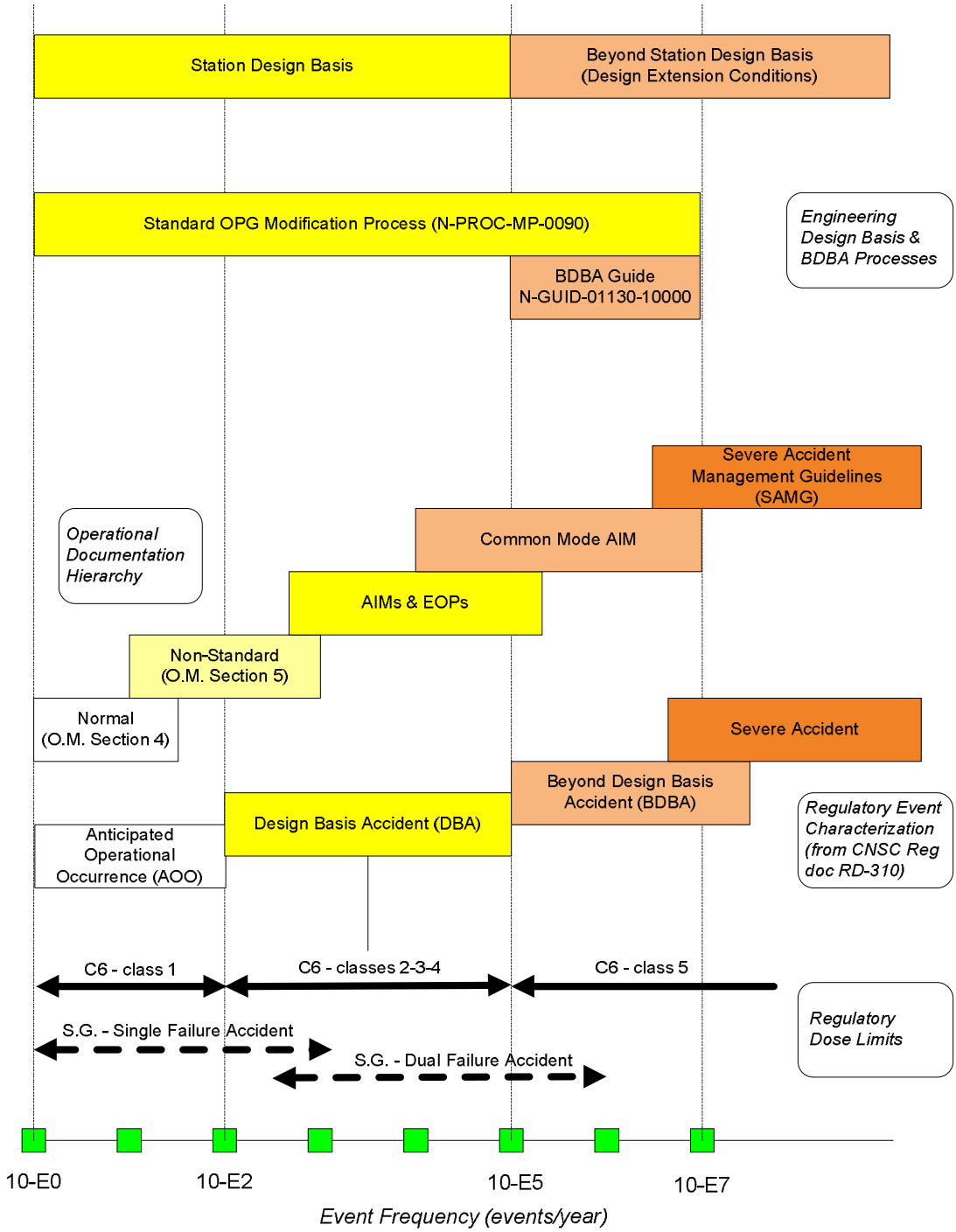

FIG.1. Beyond design basis overview.

The guide that has been developed prescribes four categories of modification:

1. Existing engineering SSCs which can be called upon to manage BDBAs. This category includes all permanently installed station SSCs, where operation outside and/or beyond the design basis of the SSC may be required under BDBA conditions. This category covers documentation changes, and updated analyses to address BDBA conditions, but does not require a physical change to the SSC.

2. Equipment upgrades installed on existing engineered SSCs to manage BDBAs. This category includes any modification (either in terms of additional equipment or upgraded equipment) in any permanently installed station SSC, which is required to maintain essential functionality under BDBA conditions.
3. New engineered SSCs added for the sole purpose of managing BDBAs. This category includes all new SSCs which are permanently installed specifically to manage and/or mitigate BDBA conditions.
4. Portable SSCs which can be attached to an existing SSC to manage BDBAs. This category includes all portable (or any temporarily connected) equipment required to manage and/or mitigate BDBA events.

The objective of the categorization is to ensure that the highest degree of rigour (least flexibility) is applied to the lower number categories, and increasing flexibility is applied to the higher numbered categories.

3.2. Examples of Modifications within Categories

To clarify the categorization of modifications for BDBA, the following examples are provided as representative of the categories:

Category 1: The assessment of the survivability under greater mechanical or thermal stresses which the SSC might be subjected to under a set of specific BDBA conditions.

Category 2: Seismic reinforcement of the deaerator to ensure that the deaerator inventory is available to the Steam Generators following an Extended Loss of all AC Power (ELAP) event.

Category 3: The addition of a new permanently installed Containment Filtered Venting System to enhance containment venting capability under BDBA conditions.

Category 4: The addition of Emergency Mitigating Equipment (EME) (including portable pumps and generators) to provide fuel cooling and essential monitoring following an ELAP.

3.3 Accountabilities and Approvals

The application of the guidance for modifications for BDBA conditions requires that the modifications packages are prepared by appropriately qualified staff and reviewed by the accountable manager. Deviations and variances from the full engineering change control procedures are approved by the accountable Design or Program Authority and are documented via signature. Design Authority approval for all BDBA modifications is required.

4.0 APPLICATION OF GUIDANCE

For Categories 1, 2, and 3, the standard rigorous engineering change control processes apply, with only limited deviations to simplify and streamline the process. For Category 4 – the portable equipment that is tied in to support BDBA response, there exists the largest degree of flexibility. This can be seen in its application to particular aspects of plant modification change control, commissioning, and operation.

4.1. Design

In the design process for BDBA – Category 1, 2, and 3 modifications follow the detailed design engineering change control process, with all of the associated screens and

considerations and rigors based on the design basis of the system. Category 4 has the largest degree of design flexibility. Distinctions are as follows:

- Category 1, 2, 3, 4: Analysis supporting BDBA capability is conducted based on more realistic initiating conditions rather than considering limit of envelope conservative assumptions typically included in design basis analysis. This is consistent with the treatment of safety analysis for BDBA.
- Category 1, 2, 3, 4: Interfacing components must be designed to system requirements of the parent system (for design basis considerations).
- Category 1, 2, 3, 4: Review Level Conditions (RLC) – seismic (10^{-4} probability), wind (F4 tornado), flood (probable maximum precipitation with wave overtopping considerations) must be applied to credited systems. RLCs are established to be appropriate estimates of worst case conditions and are typically events at lower probability than design basis conditions. Systems must be designed to their nominal design basis requirements. Robustness to withstand these RLC must be demonstrated. In some cases this qualification/robustness is further extended – for example – in a situation with a containment filtered venting design, seismic qualification to an even higher level than nominal may be prescribed to provide a larger safety margin.
- Category 4: Design process must be established by the accountable manager and approved by the Design or Program Authority, in accordance with the BDBA Modifications Guide. It should be documented, and auditable, and include consideration of the elements of full design change control. (e.g., the Modification Outline Form does not have to be used prescriptively, but the document should be consulted to ensure appropriate areas of consideration are captured). Pressure boundary code requirements do not apply specifically. Codes and standards appropriate for portable equipment should be used and documented.
- Category 4: Equipment should be designed for two tie-in points, at least one of which is an engineered tie-in point. The second tie-in point may require some additional system modification at the time of installation (e.g., removing a spool piece), provided sufficient instruction and fittings are included as part of the modification process.

4.2. Procurement

Procurement processes are also variable depending on the categorization.

- Category 1, 2: Full procurement rigor – application of catalogue identification, procurement engineering, technical specifications, etc. apply.
- Category 3: As above, but typical commercial / industrial process can apply beyond system isolation tie-in points. Deviations approved by the appropriate Design Authority.
- Category 4: Commercial/industrial processes apply and manufacturer's standards apply. Equipment will typically be tested by the manufacturer and inspected by OPG upon receipt. May be treated as transportation and work equipment if appropriate records are maintained and the process is auditable.

In the cases above, the use of commercial/industrial equipment allows the use of equipment that is readily available and with a proven commercial performance record. This can reduce costs and speed deployment. Functional performance capability is demonstrated through manufacturer's specifications and testing.

Spare parts considerations must be included in the procurement process. For portable equipment – under Category 4 – there are requirements for some spare parts to be maintained on site – for running spares and for N+1 capability (where N is the required number of

components to support all units at a site) is a requirement. This is consistent with US requirements for FLEX equipment [4].

4.3. Installation, Testing, Commissioning and Availability for Service

Installation, testing, commissioning, and availability for service of the modifications for BDBA mitigation is according to the following guidance.

- Category 1, 2: Normal installation, testing and commissioning process per station procedures.
- Category 3, 4: Commercial/industrial processes apply for installation, testing and commissioning – with sufficient rigour to demonstrate functional performance requirements are met.
- Category 1, 2, 3: Available for service / Operations Acceptance processes consistent with all permanent station modifications.
- Category 4: Availability for service should follow station Operations Acceptance process. Where deviations are required – demonstration of equivalent level of review and acceptance is required.
- Category 4: Equipment should be stored in an area that will not be impacted by the accidents that the equipment is being procured to provide mitigation for.

In all cases, associated training, parts lists, operating documentation, maintenance documentation, spare parts, etc. are confirmed as part of the availability for service process.

4.4. Operations and Maintenance

Operations, Maintenance, Testing, Routines and Call-ups are required to support the modifications installed – to provide confidence in their ability to continue to perform to meet their functional requirements.

- Category 1, 2, 3: Operating instructions are typically incorporated into Abnormal Incidents Manuals, Emergency Operating Procedures, and Severe Accident Guidelines.
- Category 4: Operating Instructions are included in Emergency Mitigating Equipment Guidelines and Severe Accident Guidelines.
- Category 1, 2, 3, 4: Maintenance and testing is performed based on manufacturer's requirements, maintenance standards, and regulatory requirements. For Category 4, testing is conducted to demonstrate functional performance for BDBA is achieved.

To ensure that Category 4 equipment is maintained available, where equipment redundancy exists, equipment can be taken out of service for maintenance for up to 90 days. Where no equipment redundancy exists, equipment can be taken out of service for up to 14 days for maintenance. A longer restoration period requires approval of the Operations and Maintenance Director.

5. SUSTAINABILITY

It is important to ensure that processes are in place to ensure that station modifications to support BDBA response is maintained available after it is installed. Processes must be established based on similar practices for design basis equipment, and additional considerations must be put in place.

- The technical basis for modifications for BDBA response capability should be formally documented and periodically reviewed to ensure that it remains current.

- Regular maintenance and testing is controlled through a predefined process consistent with regular station equipment – or using alternate tracking schemes for portable equipment. In all cases this must be documented and audited.
- BDBA response capability maintenance is audited by Nuclear Safety Division – program owners of the Nuclear Safety Program.
- BDBA response capability must be revisited when new safety analysis is done – to ensure that the assumptions and analysis that went into the development of BDBA capability remains valid with the new assumptions.
- Station modification / change control processes must ensure that beyond design basis capabilities are not inadvertently altered.
- Documentation of BDBA response requirements for SSC (e.g., for ELAP event credits) should be documented in a Beyond Design Basis Functional Safety Requirements document (based on similar Operational Safety Requirements documents for design basis credits). This will allow subsequent design changes to easily confirm that changes will not impact BDBA response capability.
- Station transient material (laydown areas, etc.) processes must include controls to ensure that access to tie-in points and staging locations for Emergency Mitigating Equipment are not blocked.
- Maintenance and Outage Management processes must account for capability to implement BDBA response. Such schemes may include recall times, controlling outages of redundant tie-in points, pre-staging equipment where required, etc.

6. APPLICATION EXAMPLES

The guidance summarized in this paper has been recently applied during BDBA modifications at OPG. Flood barrier protection at OPG's Pickering, Emergency Mitigating Equipment modifications at Pickering and Darlington, and Containment Filtered Venting System modification at Darlington. The application of the process has identified that it is sound and provides required flexibility. Communication between project staff, nuclear safety staff and design organizations is key to ensure the correct balance and rigour is applied.

7. SUMMARY

It is generally accepted that a graded level of rigour may be applied to modifications for BDBAs, provided the functionality is provided through the modification and the design basis integrity is not compromised. The guidance that has been developed, as presented in this paper, provides a structured, systematic, and risk-based approach for ensuring that an appropriate level of rigour is applied and that capability to respond to BDBA is maintained.

REFERENCES

[1] CANADIAN NUCLEAR SAFETY COMMISSION (CNSC), Design of New Nuclear Power Plants, CNSC Regulatory Document RD-337, November (2008).

[2] CANADIAN NUCLEAR SAFETY COMMISSION (CNSC), Safety Analysis for Nuclear Power Plants, CNSC Regulatory Document RD-310, February (2010).

[3] CANADIAN NUCLEAR SAFETY COMMISSION (CNSC), Severe Accident Management Programs for Nuclear Reactors, CNSC Regulatory Guide G-306, 2006.

[4] NUCLEAR ENERGY INSTITUTE, Diverse and Flexible Coping Strategies (FLEX) Implementation Guide, NEI-12-06, 2012.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).
[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/2, IAEA, Vienna (2011).

ENHANCING NPP SAFETY THROUGH AN EFFECTIVE DEPENDABILITY MANAGEMENT

G. VIERU
AREN, Bucharest, Romania
Email: g_vieru@yahoo.com

Abstract

Taking into account the importance of the continuous improvement of the performance and reliability of a NPP and practical measures to strengthen nuclear safety and security, it is to be noted that a good management for a nuclear power reactor involves a "*good dependability management*" of the activities, such as: *Reliability, Availability, Maintainability (RAM)* and maintenance support. In order to evaluate certain safety assessment criteria intended to be applied at the level of the nuclear reactor unit management, equipment dependability indicators and their impact over the availability and reactor safety have to be evaluated. Reactor equipment dependability indicators provide a quantitative indication of equipment RAM performances (Reliability, Availability and Maintenance). One of the important benefits of maintenance and failure data gathering is that it can be used as a *support of probabilistic safety assessment (PSA).* Also, a good dependability management implementation may be used to complement reactor level unit performance indicators in the field of *safe operation, maintenance and improving operating parameters,* as well as *for Strengthening Safety and Improving Reliability of a NPP.* This paper underlines the importance of nuclear safety and security as prerequisites for nuclear power. In addition, it demonstrates how different technical aspects, through implementation of a good dependability management, contribute to a strengthened safety and an improvement of availability of the NPP through dependability indicators determination and evaluation.

1. INTRODUCTION

Dependability involves the management of ***Reliability, Availability and Maintainability (RAM)*** and maintenance support [1, 2], to ensure that plan meets the RAM targets, which must be attained. ***(Dependability- the collective term [1] used non-qualitatively to describe the availability performance and its influencing factors: reliability performance [3], maintainability performance and maintenance support performance)***.

Each of those five indicators can be applied separately, both for preventive and corrective maintenance (PM &CM), giving rise to as many as ten indicator values for each item of equipment.

Used in this way, the indicators provide a comprehensive picture of the maintenance strategy employed the for key pieces of analysed equipment and its effectiveness as well as a valuable tool for maintenance activities improving at the reactor level and certain safety criteria to be taken into consideration for the safe management of the nuclear reactor. The paper provide guidance on the division of nuclear plant into their component parts and in each case the types of equipment having the most dominant effect on dependability are identified. These are the items which merit the greatest attention with regard to the equipment dependability indicators.

It is recommended that the equipment dependability parameters should be used within reactor [4] to improve *equipment dependability and, hence, to reduce operating costs, particularly through the implementation of improved maintenance strategies and spare part policies.*

2. DEPENDABILITY INDICATORS EVALUATION

As mentioned the above, five indicators are to be calculated both for the Preventive Maintenance and for the Corrective Maintenance (***PM & CM***) and have the following interpretations: ***(I_1)*** is related to maintenance frequency; ***(I_2)*** represents maintenance effort; ***(I_3)*** concerns equipment unavailability; ***(I_4)*** and ***(I_5)*** are associated with the effects of

equipment maintenance activities, at system function level and reactor level. $\boldsymbol{I_1}$ is linked to the reliability performances and $\boldsymbol{I_2}$ to the maintenance and support performance.

2.1. Method of Calculations:

I_1= (No. of Maintenance actions per item of equipment)/(Reference time period)

I_2 = (ΣMMh per item of equipment)/(Reference time period)

I_3= [(Equipment maintenance downtime, in hrs.)/(No of equipment items x no. of years x 8760h)]x100

I_4 = [(System function downtime per item of equipment, in hrs.)/(Reference time period)]x100

I_5 = [(Unit capability loss per item equipment-in MW)/(Reference power generation, in MW)]x100

where:

Reference time period = 8760 hours (one year)

ΣMMh reflects the total effort needed for maintaining a given equipment

Equipment Maintenance downtime = cumulative duration of maintenance actions (including all delay times) during the reference time period

System function downtime = cumulative durations over which the system function is lost due to maintenance activities (CM or PM)

Reactor capability loss per item equipment = corresponds to the equipment unavailability because of maintenance activities [1], [2], [5]

All the determined calculations are referred to the primary circuit of NPP only **[5]**, as shown in Fig. 1.

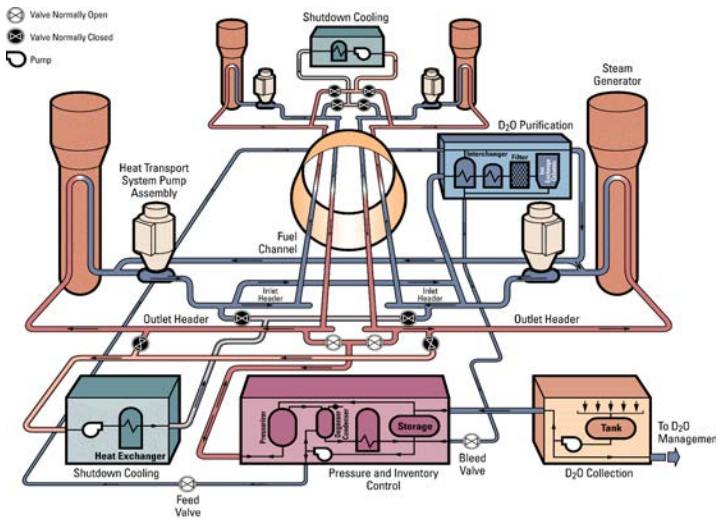

FIG.1. The primary circuit of a CANDU Nuclear Power Reactor.

The primary Circuit includes the following main equipment:

- 4 circulation pumps, 2 heat exchangers, 4 valves NO (Normally Open), 6 valves NC (Normally closed).
- 4 Heat Transport System Pump Assemblies.
- 4 Steam Generators.
- 2 system Shutdown Cooling systems.
- 1 D_2O Purification System (from primary circuit itself and from the moderator system).
- 1 system for Pressure and Inventory control.
- 1 emergency pump; instrumentation and control.

It is to be noted that the equipment dependability indicators are linked to the maintenance activities and associated work (repair after a failure, preventive maintenance, inspection, tests, etc.) [2], [4]. However, modifications, much part of the process of improving reactor dependability are not taken into consideration. This means that only preventive maintenance (**PM**) and corrective maintenance **(CM)** are to be involved.

Important note: *Corrective maintenance (**CM**) is carried out after recognition of a fault due to a failure, which can be partial or complete (i.e. either some or all of the required functions cannot be performed) according to the IEC 50 (191). Maintenance, which is not corrective, is termed preventive maintenance (**PM**). Component **PM** will only be taken into account in calculating dependability indicators if the availability of the equipment is affected by the **PM** activity. **PM** can be carried out on an opportunity basis during **CM** and vice-versa. **CM** carried out during PM on the same equipment is considered as a single **PM** action; **PM** carried out during **CM** on the same equipment is considered as a single **CM** action.*

To facilitate the interpretation of dependability indicators, all equipment were classified according to its mode of operation [2], [5]. ***The dependability indicators*** [2], [3] will apply to all these different possibilities and the operational mode will be determined by the time equipment was in operating during the period of time under consideration (reactor operating time per year). It is to be noted that the equipment dependability indicators are linked to the maintenance activities and associated work (repair after a failure, preventive maintenance, inspection, tests, etc.) [2], [6].

For the equipment operation a factor, C_o [4], [5] is used to identify the equipment operational mode. This factor [1] is defined as the ratio of the time that the equipment was in operation to the overall duration of the period of time under consideration:

$$Co = \frac{t_o}{t_p}$$

where:

t_o = total time the equipment was in operation during the overall period of time under consideration; t_p = overall period of time under consideration (reactor operating time per year, in hrs.).

To facilitate a comparison between different equipment with similar operational modes, the values of the equipment operation factor are grouped into four different categories [1], [2], [5], such as:

a) Base load category (C_{o1}): $C_o \geq 0.5$;

b) Two shifting category (***C_{o2}): $0.1 \leq C_o < 0.5$;***

c) Peaking category: ***(C_{o3}): $0.01 \leq C_o < 0.1$***;

d) Standby category ***(C_{o4}): $C_o < 0.01$***.

2.2. Equipment dependability indicators:

The NPP CANDU, in Romania, started operation in April, 1996, [2], [5], [6]. In this paper, the period 2003-2007 has been taken into consideration and the following table summarizes data (*generic*) for the calculation of the dependability indicators, as follows, in Table 1. The calculating numerical values for the equipment dependability indicators (***$I_1 \div I_5$***) are shown in Table 2.

Note that there is no possibility of derating ***$I_3 = I_4 = I_5$,*** whenever the repair on the equipment causes total unavailability of the reactor (unit). These indicators can differ in a significant manner depending upon the maintenance practice and the degree of urgency associated with repair. Since there is clearly a trend with time, values averaged over a number of years must be treated with caution.

TABLE1. DATA FOR CALCULATION DEPENDABILITY INDICATORS

Year	Reactor operation time (hrs.)	Unavailable time (hrs.)	Reference time period (hrs.)	Number of Failures	Maint. Man-hrs. For repair-MMh
2003	7968	792	8760	12	350
2004	7920	840	8760	11	230
2005	7894	866	8760	22	456
2006	7796	964	8760	25	412
2007	7872	888	8760	23	275

TABLE 2. NUMERICAL VALUES FOR EQUIPMENT DEPENDABILITY INDICATORS

Year	I_1 (y^{-1})	I_2 ($MMhy^{-1}$)	I_3 (%)	I_4 (%)	I_5 (%)	Factor C_o
2003	3.9	350	3.9	3.9	3.9	0.909
2004	2.6	230	2.6	2.6	2.6	0,904
2005	3.62	312	5.2	5.2	5.2	0. 901
2006	3.45	297	4.7	4.7	4.7	0.889
2007	3.16	275	2.85	2.85	2.85	0.898

2.3. Equipment maintenance indicators

A comparison concerning equipment maintenance indicators for circulation pumps belonging to a CANDU NPP nuclear reactor's primary circuit are presented in Tables 3 and 4.

Generally, the System that merits a RAM analysis can quickly be pinpointed from the ones with:

- High concern with respect to the safety and environment;
- Large number of CM actions in recent years or predicted for future;
- Frequent PM tasks/High PM costs;
- Large contributions to full or partial outages.

As an example, from NPP, 30 to 40 systems may be chosen from over one hundred possibilities for the RAM analysis. These can be grouped into only 9 to 10 functional system groups, in accordance with the IAEA provisions on *Operating experience with Nuclear Power Stations in Member States* and the ***NPRDS*** (Nuclear Plant Reliability Data System) Reporting Guidance Manual, The Institute of Nuclear Power Operations.

In addition to their value to improve maintenance activities with a reactor unit, an important application of the equipment dependability indicators is to facilitate comparison between different utilities. Where there appear to be significant differences in the values of the equipment dependability indicators between different utilities, detailed investigation is needed to determine the explanation for them. One reason for discrepancies relates to the use of different cut-off levels when recording maintenance activities. Other may relate to the use of different system boundaries or to differences in size, design, or redundancy levels.

Considerable flexibility is allowed in defining precise boundary points to allow equipment to be grouped in the most efficient manner for analysis purposes. To maintain consistency between different data sources, some general agreement on equipment boundaries for apportioning the maintenance actions is appropriate and must be clearly stated and documented as a part of the analysis process, bearing in mind the benefits of keeping things as simple as possible.

TABLE 3. CORRECTIVE MAINTENANCE INDICATORS

Heat Transport System Pump Assembly	$\mathbf{I_1}$ (Maint. freq-Events/pump x year)	$\mathbf{I_2}$ (Maint. effort-Man-hours/pump x year)	$\mathbf{I_3}$ (Equip. downtime-Downtime/Ref. time period %)	$\mathbf{I_4}$ (System Function downtime–Ref. time period - %)	$\mathbf{I_5}$ (Reactor capability loss factor (Unavailable power/Ref. power-%)
P_1	1	50	0.25	0.03	$3.5x10^{-2}$
P_2	0.75	62	0.31	0.2	$2.3x10^{-2}$
P_3	1.5	69	0.72	0.13	$1.5x10^{-2}$
P_4	1.8	78	0.89	0.07	$2.1x10^{-2}$

TABLE 4. PREVENTIVE MAINTENANCE INDICATORS

Pump	$\mathbf{I_1}$ (Maint. freq-Events/pump x year)	$\mathbf{I_2}$ (Maint. effort - Man-hours/pump x year)	$\mathbf{I_3}$ (Equip. downtime-Downtime/Reference time period %)	$\mathbf{I_4}$ (System Function downtime Ref. time period - %)	$\mathbf{I_5}$ (Reactor capability loss factor (Unavailable power/Ref. power-%)
P_1	0.5	45	1.12	0	0
P_2	0.7	47	1.21	0.25	0
P_3	0.90	63	1.05	0.5	0
P_4	1	65	1.7	0.8	0

3. DEPENDABILITY INDICATORS EVALUATION FOR THE INR TRIGA RESEARCH REACTOR

For the INR's TRIGA research reactor analysed, all the determined calculations are referred only at the primarily circuit [7], (see Figure 2). The primary circuit includes the following main equipment:

- 4 circulation pumps - ($P_1 \div P_4$)
- 3 heat exchangers - ($S_1 \div S_3$)
- 1 delay tank
- pipes 820x10 mm
- 20 relief and safety valves (in operation or standby)
- 1 emergency pump
- instrumentation and control

The INR TRIGA research reactor has started operation in 1979. In this paper, the period 1994-1999 has been taken into consideration [8]. Table 5 summarizes the data for the calculation of the dependability indicators. The calculated numerical values for the equipment dependability indicators ($I_1 \div I_5$) are shown in Table 6.

Similarly, as in the case of the NPP CANDU analysed primary circuit, there is no possibility of derating, $I_3=I_4=I_5$, whenever the repair on the equipment causes total unavailability of the TRIGA research reactor. These indicators can differ, also, in a significant manner depending upon the maintenance practice and the degree of urgency associated with repair. There is clearly a trend with time, and *the averaged values over a number of years must be treated with caution.* The equipment operation factor C_0, as described in the beginning of this work, has clearly a value between $\boldsymbol{0.1 \leq C_o < 0.5}$, which means that the research reactor is included in the second category-two shifting category ($\mathbf{C_{o2}}$). [1]

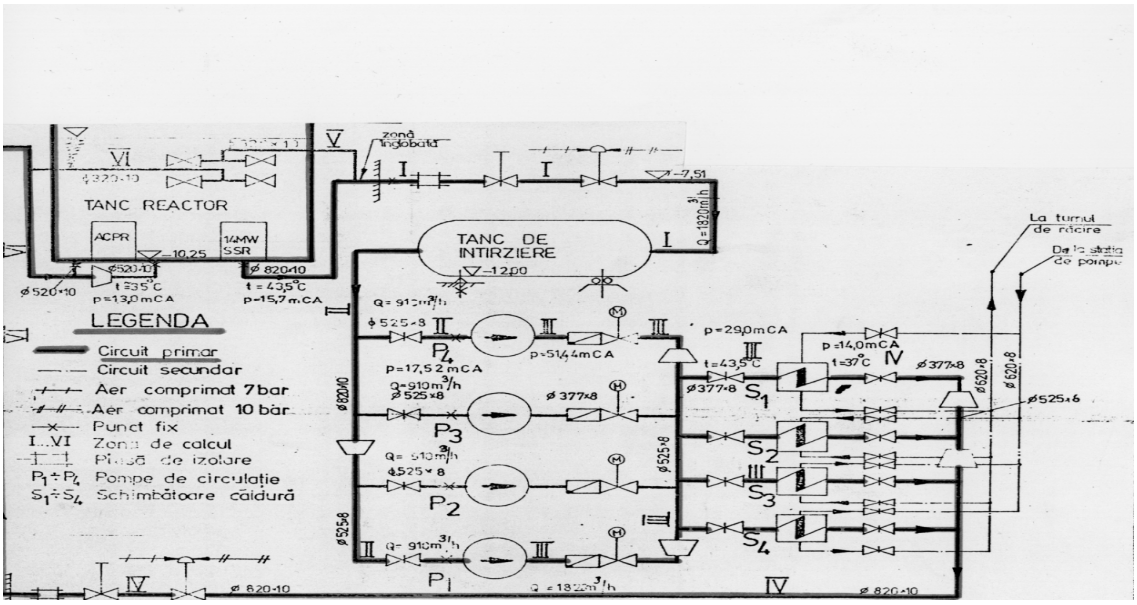

FIG. 2. The primary circuit of inr's triga research reactor.

TABLE 5. DATA SUMMARIZED FOR THE CALCULATION OF THE DEPENDABILITY INDICATORS

Year	Reactor operation time (hours)	Unavailable time (hours)	Reference time period (hours)	Number of Failures	Maintenance Man-hours for repair (MMh)
1994	1689	22.75	8760	16	350
1995	1724	118.75	8760	12	230
1996	1762	162.6	8760	27	456
1997	1834	175.0	8760	26	412
1998	1925	213.0	8760	19	275
1999	2134	169.5	8760	25	436

TABLE 6. THE CALCULATED NUMERICAL VALUES FOR THE EQUIPMENT DEPENDABILITY INDICATORS

Year	I_1 (y^{-1})	I_2 ($MMhy^{-1}$)	I_3 (%)	I_4 (%)	I_5 (%)	Factor C_o
1994	2.5	350	3.45	3.45	3.45	0.19
1995	2	230	2.17	2.17	2.17	0.21
1996	5	456	4.53	4.53	4.53	0. 22
1997	4	412	3.22	3.22	3.22	0.23
1998	3	275	1.74	1.74	1.74	0.25
1999	3	436	4.88	4.88	4.88	0.26

4. COMMENTS AND CONCLUSION

4.1. Comments

From Table 2, is easily to observe that the equipment operation factor $\mathbf{C_0}$ for NPP CANDU corresponding to the first category (a) *baseload-*($\boldsymbol{C_{o1}}$)*:* $\boldsymbol{C_o \geq 0.5}$, which shows a normality in operation, while for the INR TRIGA Research Reactor analysed equipment, Table no. 6, corresponding to the second category (b)-*two shifting category* ($\mathbf{C_{o2}}$) *:* $\boldsymbol{0.1 \leq C_o < 0.5}$.

The high values of the indicators I_1 and I_2 shows that the equipment used have high reliability parameters with significant influences to the reactor PSA analysis. Also, the determination of dependability parameters may lead to the establishment of programming aimed at protecting valuable nuclear power reactor or research reactor, from High Impact, Low Probability (HILP) failures.

The five indicators of equipment dependability are as follows [1], [2], [5], [6]:

- Equipment Maintenance Frequency ($\mathbf{I_1}$);
- Equipment Maintenance Effort ($\mathbf{I_2}$);
- Equipment Maintenance Downtime Factor ($\mathbf{I_3}$);
- Equipment Maintenance Contribution to the System Function Downtime Factor ($\mathbf{I_4}$);
- Equipment Maintenance Contribution to the Unit Capability Loss Factor ($\mathbf{I_5}$).

The first indicator, $\mathbf{I_1}$ reflects reliability performance, while $\mathbf{I_2}$ is an indicator of equipment maintainability and of the performance of the maintenance support function. The remaining indicators, $\mathbf{I_3}$, $\mathbf{I_4}$, and $\mathbf{I_5}$ are all linked with various aspects of availability at the equipment, system function and unit levels, respectively. These indicators complement, at the equipment level, the ten plant-level performance indicators that were developed by UNIPEDE (*International Union of Producers and Distributors of Electrical Energy*), in 1991.

On the other hand, these indicators offer potential for wider application since:

- Provide valuable dependability characteristics to those responsible for the specification and procurement of equipment;
- May be used to complement reactor level performance indicators in the field of operation, safety, maintenance and improving of operating parameters at the unit level unit;
- Using the maintenance related indicators it is possible to follow trends with time and to compare different operating experience and maintenance strategies.

The form of the indicators permits the exchange of data between different NPP CANDU users, as well as between TRIGA owners, with design decisions, availability predictions and operational assessment. Data exchange will facilitate the analysis of RAM as a function of time (trend analysis). Data exchange can also be used to verify RAM objectives or predictions.

4.2. Conclusions

Reactor equipment dependability indicators provide a quantitative indication of an equipment RAM performance. These indicators can be applied separately to those corrective and preventive maintenance activities related to equipment unavailability. It is recommended that these indicators should be used within reactor unit to improve management of dependability. In particular, this can be of value in optimizing maintenance strategies and improving spare

part policies. Provided that attention is paid to specifying equipment boundaries precisely and to record the size, type, level of redundancy and mode of operation of the particular equipment under consideration.

The Reactor Equipment International Group's experience on dependability indicators determination has shown that this can be of great value as *a means of benchmarking dependability performance for key items of equipment and of identifying where there is scope for improvement through the implementation of international best practice.* Other benefits may include **e. g**, the followings:

- Optimization of the design of a new nuclear power plant;
- Reduction of life cycle costs for each individual unit;
- Quantification of the value of redundant equipment;
- Assessment of the value of R&D projects to improve Dependability;
- Data exchange and resulting modification of existing plants;

In the light of the Accident at the Fukushima Daiichi Nuclear Power Plant (2011), the implementation of the Dependability Management could be an important element of the strengthening and broadened safety and an additional layer of protection to prevent severe accidents, coupled with an increased priority on mitigation and a focus on the preservation of containment to enhance defence in depth (DID).

REFERENCES

[1] IEC 300-1 Dependability Management, Part 1-Dependability Programme Management, 1995.

[2] VIERU, G., "The Evaluation of the Dependability Performance Parameters for NPP CANDU, Cernavoda", Internal Report (Internal Scientific Research Report) no. RI 8701/2009, INR Pitesti (2009).

[3] VIERU, G., "Consideration on the Experimental Reliability Determination, Reliability Improvement for Nuclear Reactor Instrumentation", Paper printed in the Proceedings of ICONE-3 International Conference, Kyoto, Japan (1995).

[4] VIERU, G., INR Pitesti-RI 6060, "Safety Criteria for the TRIGA Reactor management and the evaluation of its applicability at NPP Cernavoda", Internal Scientific Research Document (2001).

[5] VIERU, G., "The Evaluation of the Dependability Performance Parameters for NPP CANDU, Cernavoda", Internal Report (Scientific Research Report) no. RI 8701/2009, INR Pitesti (2009).

[6] VIERU, G., "Requirements concerning testing of the equipment intended to be used in nuclear installations including NPP CANDU Cernavoda", SCN Pitesti, Internal Scientific Research Report no. RI 6613 (2003).

[7] TRIGA Research Reactor-Technical Specification, INR Pitesti, Romania (1979).

[8] VIERU, G., et al, "Safety criteria for the management of a research reactor", International TRIGA Research Reactor's Conference, INR Pitesti, Romania (2000).

SAFETY ANALYSIS IN DESIGN AND ASSESSMENT OF THE PHYSICAL PROTECTION OF THE OKG NPP

P. LINDAHL
OKG Aktiebolag, Oskarshamn, Sweden
Email: par.lindahl@okg.eon.se

Abstract

OKG AB operates a three unit nuclear power plant in the southern parts of Sweden. As a result of recent development of the legislation regarding physical protection of nuclear facilities, OKG has upgraded the protection against antagonistic actions. The new legislation includes requirements both on specific protective measures and on the performance of the physical protection as a whole. In short, the performance related requirements state that sufficient measures shall be implemented to protect against antagonistic actions, as defined by the regulator in the "*D*esign *B*asis *T*hreat" (DBT). Historically, physical protection and nuclear safety has been managed much as separate issues with different, sometimes contradicting, objectives. Now, insights from the work with the security upgrade have emphasized that physical protection needs to be regarded as an important part of the *D*efence-*I*n-*D*epth (DID) against nuclear accidents. Specifically, OKG has developed new DBT-based analysis methods, which may be characterized as probabilistically informed deterministic analysis, conformed to a format similar to the one used for conventional internal events analysis. The result is a powerful tool for design and assessment of the performance of the protection against antagonistic actions, using a nuclear safety perspective.

1. BACKGROUND

OKG AB operates a three unit nuclear power plant close to Oskarshamn, a town in the southern parts of Sweden. In 2004 and 2005 new legislation was issued in Sweden regarding physical protection of nuclear facilities. These included requirements both on specific protective measures and on the performance of the physical protection as a whole. On a high level, the performance related requirements imply that sufficient measures shall be implemented to protect against antagonistic actions, as defined by the regulator in the "*D*esign *B*asis *T*hreat" (DBT). On a more detailed level, the DBT shall also be used specifically as a basis for designing the protection of the main control room, of rooms for storage of theft-prone nuclear material and of the surveillance centre for the plant. The OKG response to the new requirements was to launch a project for upgrading the physical protection to modern standards.

In the early phases of this project the general guidance issued by the regulator was sufficient for defining the scope, but to comply with all requirements it was also necessary to build capacity for evaluating the importance/benefits of different security measures. As the project progressed it became apparent that existing methods for analysis of physical protection were insufficient with respect to this purpose, and that new methods for DBT-based analysis were needed to avoid different problems encountered in the past.

Historically, physical protection and nuclear safety has been managed much as separate issues with different, sometimes contradicting, objectives. From a security perspective it may e.g. be justified to prevent unauthorized access to certain areas by introducing protective barriers (physical measures for obstructing and delaying an antagonist) and checkpoints, but from a nuclear safety perspective this kind of protection may also pose a risk of delaying important safety measures in emergency situations. The insights gained from this and other examples thus motivated OKG to develop a common analytical platform for design and assessment of physical protection from a nuclear safety point of view.

As a basis for this development it was first recognized that physical protection is an important part of the "*D*efence-*I*n-*D*epth" (DID) against nuclear accidents. The natural next step was then to seek for analogies within the well-established framework for managing nuclear safety. As a result, the methodology for managing risks associated with internal

events (such as fire and flood) was identified as a possible "template" for management of risks due to antagonistic actions included in the DBT.

2. DBT-BASED ANALYSIS METHODS

2.1. Requirements on nuclear safety analysis

The Swedish legislation specifies requirements and objectives both for deterministic and for probabilistic safety analysis.

Deterministic safety analysis (DSA) shall be applied as a tool for designing and verifying that the DID has sufficient capacity to protect against nuclear accidents, and to mitigate the consequences should an accident occur. More details regarding DSA are presented in section 2.2.

Probabilistic safety analysis (PSA) shall be applied to verify that nuclear risks (in terms of frequencies for "core damage", "large radioactive release" etc.) are not dominated by any specific weaknesses in design or operation. More details regarding PSA are presented in section 2.3.

2.2. Deterministic safety analysis

The expectations on the method for deterministic analysis of physical protection were that it should be (*i*) DBT-based and (*ii*) consistent with the requirements on DSA.

To meet expectation (*i*) the DBT was interpreted and transformed into a set of scenarios, potentially challenging nuclear safety. The scenarios specify the different antagonists, their motifs/objectives and their abilities. However, depending on the number of degrees of freedom in the DBT, the number of scenarios needed to cover all relevant aspects may be large. To keep the number of scenarios at a manageable level, the number of degrees of freedom was reduced by introducing "pessimistic postulates". If the physical protection have sufficient capacity to protect against the most challenging variant of a class of scenarios, then the capacity will be sufficient also for the more benign variants.

To meet expectation (*ii*), the DBT-based method was developed by mapping the generally applied steps in conventional DSA.

2.2.1. Selecting initiating events/scenarios

- Conventional DSA:

Identify initiating events and, for each of these, determine the appropriate event class based on the expected event frequency.

- DBT-based DSA:

Identify a relevant set of DBT-based scenarios. Antagonistic actions in these scenarios are considered to be precursors, which may result in initiating events (e.g. if an action triggers the need to shut down the reactor). However, an initiating event due to an antagonistic action is not assigned a specific event class, since the DBT consists of postulated threats not actual ones.

2.2.2. Setting up the analysis

- Conventional DSA:

Based on event class, identify deterministic requirements, relevant boundary conditions and simplifying assumptions.

- DBT-based DSA:

Conventional deterministic requirements, e.g. regarding single failure tolerance and CCF tolerance, are applied if considered appropriate (this is not explicitly required in the Swedish legislation). Antagonistic actions may include degradation of barriers (physical confinement of radioactive substances) or safety functions (barrier protection systems). This resembles the boundary conditions used for "internal events" analysis, which is why this is a relevant template for analyzing the DBT-based scenarios (analysis of "theft of nuclear material" and similar scenarios may need to have a different form). The selected "pessimistic postulates" are necessary, but not unique simplifying assumptions (it is possible to define sufficient sets of postulates in several ways).

In addition, since the purpose of the required protective measures is to relax the impact from actions described in the DBT, this is mirrored in the analysis set-up. E.g. the set of "tools" available for a specific antagonistic action may be reduced if the physical protection is designed to protect against one or more of these tools. The remaining "abilities" should be considered in the analysis of the different scenarios.

2.2.3. Acceptance criteria

- Conventional DSA:

Each event class is associated with a set of acceptance criteria.

- DBT-based DSA:

Acceptance criteria are harmonized with the ones used in conventional DSA. It is reasonable to require that less serious threats (e.g. non-violent demonstrations) may only lead to small consequences (e.g. similar to the ones accepted for the event class "anticipated events"). More serious threats (e.g. terrorist attacks) could lead to larger but still acceptable consequences (e.g. similar to the ones accepted for "improbable events" or "highly improbable events").

2.3. Probabilistic safety analysis

Full implementation of the DBT-based scenarios into the conventional PSA is problematic, since the scenarios are based on postulates, not on actual threats. This is manifested in different ways, e.g. in the absence of relevant initiating event frequencies.

Still, PSA may be used as an important source of information for the DBT-based DSA, taking advantage of the physical, functional and spatial dependences represented in the PSA model.

The following information is relevant in setting up analysis cases in the PSA-model:

- Mode of operation (power operation, outage period, …) defines the general state of the nuclear facility.

- Scenario specific information (the antagonist´s objective, knowledge and abilities combined with relevant "pessimistic postulates" and measures in the physical protection) defines the maximum degradation of the DID.

The number of analysis cases may be large, and a systematic screening process is necessary in order to identify weaknesses. If any of the analysis cases lead to unacceptable consequences (e.g. "core damage" or "large radioactive release" in association with a terrorist action) additional measures in physical protection and/or in nuclear safety functions may be warranted.

2.4. Demonstration of the methods

To demonstrate the methods in the previous sections, without revealing details of the OKG specific analysis, the following example is based on a *fictive* DBT[1].

Two antagonists are defined in this fictive DBT, A1 and A2.

A1: *A non-violent group of activists*

Motif/Objective: The activists seek public attention to convey an anti-nuclear message through an illegal, but non-violent demonstration at the site. Their objectives may include attempts to penetrate protective barriers, if this is beneficial to the activists in attracting public attention and/or in strengthening their message.

Abilities: The activists have access only to information that is publically available. At site, they may try to break through protective barriers using "burglary type" tools, e.g. ladders, crowbars etc.

Pessimistic postulates: The description has one relevant degree of freedom. Actions including attempts to penetrate protective barriers are judged to be more challenging compared with more benign scenarios. Such penetration attempts are therefore postulated to take place.

A2: *A terrorist cell*

Motif/Objective: The terrorists seek to create public fear, by causing a nuclear accident.

Abilities: Apart from publically available information, the terrorists have access to insider information regarding routines associated with normal operation. To achieve their goal they will if necessary use explosives to force protective barriers, with the intent of

[1] This fictive DBT is based only on some simplistic assumptions using publically available information. It is developed for illustrational purposes only, and does *not* imply any similarity with the actual DBT issued by the Swedish regulator.

detonating a bomb somewhere in the power plant. Offsite power may be taken out in association with the attack, if this is beneficial to the terrorists with respect to the planned bombing.

Pessimistic postulates: The description has one relevant degree of freedom. Actions including loss of offsite power are judged to be more challenging compared with more benign scenarios. Offsite power is therefore postulated to be non-available.

After applying pessimistic postulates, two scenarios remain to be analyzed.

Scenario 1: *A non-violent demonstration, including attempts to force protective barriers*

Acceptance criteria: Consequences must not exceed the limits defined for the event class "normal operation". (It must be possible to continue operation within the limits of the technical specifications.)

Vulnerability analysis: The acceptance criteria will be violated if the activists are able to provoke the operator to shut down the reactor. Given that reactor shut down is the normal operator response to conditions outside the technical specifications; all safety relevant equipment credited must be protected against conditions that may arise during the demonstration. In addition it is also necessary for the operator to be able to detect if the activists go beyond the conditions set for this scenario, since if this happens reactor shut down may very well be the appropriate action.

Protective measures: Safety relevant equipment is required to be placed inside the restricted area, which must have sufficiently robust walls, doors and other openings. It is also required that arrangements are made to detect unauthorized access to the restricted area, resulting in a verified security alarm.

Conclusion: By designing a protection of the safety relevant equipment that will withstand "burglary type" tools, *normal operation may continue* as long as there is no verified security alarm indicating a breach into the restricted area. Thus, given that the protective measures are implemented, the acceptance criteria for scenario 1 are met.

Scenario 2: *A terrorist attack, including loss of offsite power and a bomb detonating somewhere in the power plant*

Acceptance criteria: Consequences must not exceed the limits defined for the event class "unanticipated events. (Safe shut down must be achieved.

Some outage time is accepted for repairs and replacements of damaged equipment.)

Vulnerability analysis: The acceptance criteria will be violated if the terrorists are able to detonate a bomb at a "weak spot" in the power plant, i.e. in an area where a bomb detonation is likely to cause core damage or damage to spent fuel. The PSA models for the power plant may be used as one source of information to identify weak spots. If any weak spots are found, they may need additional protection, if the terrorists are likely to be able to identify them as targets. E.g. some potential target areas (the main control room being one) are identified in the Swedish legislation through the requirement to show that the physical protection is sufficient with respect to the DBT. These areas must not fall into the category of "weak spots", or if they do they need a protection to match. Weak spots due to dependencies that are very difficult to find without the aid of PSA, may not warrant the same priority in design of the physical protection.

Protective measures: Restrictions must be placed on the type of information that is put into documents describing routines for normal operation; sensitive information regarding dependencies must not be given away. Adequate information security will thus prevent terrorists from selecting a relevant target for the bomb. If an attack involving a breach into the restricted area still occurs, this must be associated with a verified security alarm, triggering the operator to take relevant action. E.g. if a security alarm signals that the main control room is threatened, the operator is required to abandon it. In association with this, measures must be taken to bring the reactor to a safe shutdown mode and to prohibit unauthorized manoeuvres from the control room. In addition to these immediate actions, other measures may also be warranted. If external intervention is credited as a mean to prevent a bomb from detonating near an identifiable weak spot, obstructing and delaying measures must be implemented to allow assisting forces to arrive in time.

Conclusion: By implementing administrative routines to protect sensitive information, and by making arrangements for security alarms and action plans for the operator to follow in case of an attack, the physical protection as a whole (including obstructing and delaying measures) will be sufficient to *enable safe shut down and prevent core damage*. Thus, given that the protective measures are implemented, the acceptance criteria for scenario 2 are met.

This demonstration shows how DBT-based analysis may be used to identify different protective measures, and to make an evaluation of the physical protection as a whole. Some

indication is also given on how the analysis may support prioritization between different measures. Another example of a decision support application is presented in section 3.2.

3. APPLICATIONS

3.1. Design and assessment of the physical protection

According to the Swedish legislation, the physical protection is required to have protective barriers at the boundary to the surveilled area at the site, to the restricted area containing equipment relevant to nuclear safety and to a number of specified rooms within the restricted area (relevant to nuclear safety and physical protection). The general guidance issued by the regulator suggests a set of protective measures to achieve a minimal level of protection for each of these barriers. Considering this minimal set of protective measures, the principle design was developed in an iterative fashion using scenario analysis as the decisive assessment tool.

If the physical protection together with remaining nuclear safety functions (after scenario specific degradation) was found to be sufficient to fulfil the appropriate acceptance criteria, then the set of protective measures were declared to be sufficient. If the acceptance criteria could not be met, additional protective measures were suggested and evaluated against the conditions specified in the DBT.

Given that acceptance criteria are met for all scenarios, all nuclear facilities and all modes of operation, verifying analysis is reduced to verification of the adequacy of the separate functions and protective barriers in the physical protection.

3.2. Management support - safety evaluation

At OKG a structured method for safety evaluation is used to provide input to safety related decision making. After the integration of security into the set of safety analyzes covered by the *S*afety *A*nalysis *R*eport (SAR), this decision support tool may now be applied for a broader class of safety related issues.

The OKG method for safety evaluation – the principles are described in [1] (an IAEA Safety Report) – aims at categorizing safety issues based on their real or potential negative influence on the DID. This influence could include changes to the set of analyzed initiating events or their expected event rates, to barriers or the safety function capability of the facility or to the potential consequences of analyzed event sequences. Four safety significance levels are defined; each associated with generic recommendations on appropriate actions.

Negligible: No actions are necessary.

Low: Risk reducing interim measures are not necessary. Permanent corrective measures may be considered if shown to be reasonably practicable.

Medium: Risk reducing interim measures are usually necessary. Plant operation may continue for some limited time. Permanent corrective measures should be implemented.

High: Immediate risk reducing interim or corrective measures are necessary, or plant shutdown should be considered.

Before security related issues are evaluated, the DBT-based analyzes for affected scenarios need to be reviewed, to determine if or under what conditions they may lead to initiating events challenging nuclear safety. If nuclear safety is challenged, the method for safety evaluation may be applied with some modifications, e.g. regarding treatment of event rates[2] (event rates not being defined for postulated threats). With these modifications the safety evaluation method may be applied without making any other distinction between DBT-based and conventional DSA.

A specific example of the benefits with this approach is that safety/security conflicts may be managed just as conventional safety conflicts-of-interest has been managed before; guided by the safety significance determined for affected event sequences. Thus, it does not matter if these event sequences are associated with DBT-based scenarios or with conventional initial events.

3.3. Operational support - requirements in technical specifications

The final design of the OKG physical protection was documented in the SAR. This documentation included a comprehensive description of the design and a summary of the results of the DBT-based analysis.

Based on this documentation, the technical specifications will be updated with sufficient requirements. These requirements are readily acquired from the DBT analysis results. For each scenario a *F*ailure *M*odes and *E*ffects *A*nalysis (FMEA) is performed to identify dependencies between different parts of the physical protection – technical systems as well as administrative routines. The cumulative requirements for obtaining sufficient capacity for all scenarios define the requirements for safe operation.

In addition, as a sensitivity analysis, the impact of different foreseeable problems in the physical protection is assessed using the method for safety evaluation described in section 3.2. Temporary exceptions from the requirements in the technical specifications during corrective measures are judged to be acceptable, given that the safety significance of these exceptions have “Negligible” or “Low” safety significance.

4. CONCLUDING REMARKS

The updated SAR for the OKG nuclear power plant, including the results of the DBT-based analysis, was submitted to the Swedish authorities in 2011. Since then, these analyzes have been used as a basis for design and safety related decisions regarding the physical protection. The OKG experience is that physical protection is now managed in a more systematic manner, and that decided actions enjoy a higher degree of acceptance than before. This acceptance is credited to the ability to speak “physical protection” in the language of “nuclear safety”.

[2] For safety evaluation purposes the following approach is used. Under normal conditions, each scenario is treated as if it belonged to the event class that defines the acceptance criteria for this scenario. Under conditions where there is an *actual threat* against the power plant, the corresponding (most relevant) scenario is treated as if belonged to the event class “anticipated events”.

According to plan, the upgraded technical specifications will be taken into practice during 2013. Until now, a conservative approach has been used in specifying the operational requirements on the physical protection. The expectations are that the upgraded version will significantly reduce the administrative load, and help directing resources to issues that matter the most for an effective protection against antagonistic actions.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards – A Common Basis for Judgment, Safety Reports Series No. 12, IAEA, Vienna (1998).

ADVANCES AND CHALLENGES IN THE IMPLEMENTATION OF DEFENCE IN DEPTH IN ACCIDENT MANAGEMENT AND EMERGENCY PREPAREDNESS AND RESPONSE (TOPICAL SESSION 3)

INVITED PRESENTATION

EMERGENCY PREPAREDNESS AND RESPONSE: A SAFETY NET

H. AALTONEN
Radiation and Nuclear Safety Authority (STUK),
Helsinki, Finland
Email: hannele.aaltonen@stuk.fi

The objective of nuclear regulatory work is to prevent accidents. Nevertheless, possibility of a severe accident cannot be totally excluded, which makes a safety net, efficient emergency preparedness and response, necessary. Should the possibility of accidents be rejected, the result would be in the worst case inadequate protection of population, functions of society, and environment from harmful effects of radiation. Adequate resources for maintenance and development of emergency arrangement are crucial. However, they need to be balanced taking into account risks assessments, justified expectations of society, and international requirements.

To successfully respond to an emergency, effective emergency preparedness, such as up-to-date plans and procedures, robust arrangements and knowledgeable and regularly trained staff are required. These, however, are not enough without willingness and proactive attitude to

- communicate in a timely manner;
- co-operate and coordinate actions;
- provide and receive assistance; and
- evaluate and improve emergency arrangements.

In the establishment and development of emergency arrangements, redundant and diverse means or tools used are needed in, for example, communication and assessment of hazard.

Any severe nuclear emergency would affect all countries either directly or indirectly. Thus, national emergency arrangements have to be compatible to the extent practicable with international emergency arrangements. It is important to all countries that the safety nets of emergency arrangements are reliable - and operate efficiently in a coordinated manner when needed - on national, regional and international level.

INVITED PRESENTATION

THE ROLE OF THE INTERNATIONAL ATOMIC ENERGY AGENCY IN A RESPONSE TO NUCLEAR AND RADIOLOGICAL INCIDENTS AND EMERGENCIES

E. BUGLOVA, F. BACIU
International Atomic Energy Agency (IAEA), Department of Nuclear Safety and Security, Wagramer Strasse 5, P.O. Box 100, 1400 Vienna, Austria
Email: E.Buglova@iaea.org

The role of the International Atomic Energy Agency (IAEA) in a response to nuclear and radiological incidents and emergencies has been defined and further expanded through the IAEA Statute, the Convention on Early Notification of a Nuclear Accident, the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, the Convention on Physical Protection of Nuclear Material, IAEA safety standards, relevant decisions by Policy Making Organs of the IAEA, inter-agency agreements and other documents such as the IAEA Action Plan on Nuclear Safety. The IAEA Secretariat fulfils its roles through the Agency's Incident and Emergency System (IES) and the Incident and Emergency Centre (IEC). The IEC is the global focal point for international preparedness and response to nuclear and radiological safety or security related incidents, emergencies, threats or events of media interest and for coordination of International assistance.

During a response the IEC performs and facilitates for Member States many specific functions which include: prompt notification; official information exchange; assessment of potential consequences; prognosis of emergency progression; provision, facilitation and coordination of International assistance; provision of timely, accurate and easily understandable public information; coordination of inter-agency response at the International level. Through officially designated contact points of Member States the IEC is able to communicate at any time with national authorities to ensure the prompt and successful sharing of information and resources.

The IEC routinely performs internal exercising of all aspects of the IAEA response and in cooperation with Member States, the IAEA organizes and facilitates the conduct of large scale international exercises to practice cooperation and coordination. This presentation outlines in detail the specific functions of the IAEA IEC during a response.

BEYOND DESIGN BASIS SEVERE ACCIDENT MANAGEMENT AS AN ELEMENT OF DID CONCEPT STRENGTHENING

M. KUZNETSOV
FSUE VO "Safety",
Moscow, Russian Federation
Email: kuznetsov_mv@vosafety.ru

Abstract

The 4th Level of DiD is ensured by management of beyond design basis accidents which is achieved by implementation of the Beyond Design Basis Accidents Management Guidance (BDBAMG) and, if necessary, by additional technical devices and organizational measures at NPP Unit. BDBAMG is located between Levels 3 and 5 in DiD and is related to them. It is connected with Level 3 by means of conditions generated at this Level and according to which BDBAM should be initiated (Level 4). It is associated with Level 5 by conditions which necessitate implementation of Emergency planning. Both types of conditions should be identified in BDBAMG. BDBAs including the phase of severe damage of fuel and protective barriers (severe accidents) in accordance with Russian regulatory framework are a subset of all BDBAs set. In this connection, such accident scenarios meet the representativeness criterion for further analysis and development of Guidance for their management. BDBAMG availability, as it provides robustness of DiD as a whole, is an obligatory condition for obtaining a NPP operational license. In the process of BDBAMG development and implementation a feedback with technical and organizational measures, comprising Level 1 and, to a less extent, Level 2, comes up. BDBAMG verification is an important final stage of its development. Addressing severe accidents, it is a challenging issue for a full scope simulator and may require its software modernization to make it responsive to severe accident phenomena. The existing BDBAMGs should be updated due to NPP Unit modernizations and in conjunction with the latest knowledge on severe accident phenomenology and lessons learnt from known events (e.g. NPP Fukushima). Thus, improvements incorporated in BDBAMG, enhance the strength of DiD.

1. INTRODUCTION

The 4th Level of DiD is identified [1], [2], [3], as management of beyond design basis accidents, including phase of severe accident (SA), which is achieved by implementation of the Beyond Design Basis Accidents Management Guidance (BDBAMG) and, if necessary, by additional technical devices and organizational measures at NPP Unit. The availability of BDBAMG by the regulatory body (RB) is an obligatory condition to get the license for NPP unit operation. BDBAMG is located between Levels 3 and 5 in DiD and directly connected with Level 3 by means of conditions generated at this Level and according to which BDBAMG should be initiated (to go to Level 4) and with Level 5 caused by necessity to start the Emergency planning implementation. Both types of conditions should be identified in BDBAMG.

The DiD concept, in great extent, is based on reactor installation inherent safety features, conservative design decisions and is supported by deterministic and probabilistic safety analyses (PSA), which allows to optimize and to assess safety of the design. It relates to the first two Levels of DiD, which should prevent accidents and thus, are of the first priority.

BDBAMG development begins for the existing design that is why a feedback with technical and organizational measures, comprising Level 1 and, to a less extent, Level 2, comes up in the process of the guide development and implementation. The design basis of the unit is revised with regards not only to safety systems and components (SSC) but also for systems of normal operation, auxiliary systems and safety analyses. It may result in improvements and corresponding unit's modernizations.

BDBAMG verification (checking) is an important final stage of the development. Verification in particular concerning severe accidents may require full-scale simulator software model modernization which takes into account SA phenomenology and possibility calculation in real time regime.

BDBAMG development is a process which is finalized by implementation at the unit. However, even after its implementation BDBAMG has to be revised in case of unit modernization or new knowledge appearance and lessons learnt from severe accidents (e.g. SA at "Fukushima" NPP). It may results in reconsideration of some DiD characteristics (e.g. system of I&C), featured in the unit design. The Guidance, as a part of operation documentation should be in the correspondence with the actual state of the unit, and thus with DiD realized in its design.

It is rather evident, that availability of effective BDBAMG will assure the 4th Level strength and it's qualitative preparedness for development and then development which is related to some safety aspects on different DiD's Levels may contribute for their strengthening. The concept of BDBAMG as well as its development in compliance with this concept providing strength of 4 Level and DiD strengthening as whole are reported in this paper.

2. RUSSIAN REGULATORY REQUIREMENTS

The definitions and tasks of Level 4 DiD are established in *it. 1.2.3.* [3], as beyond design basis accidents management in the course of which accident propagation should be prevented and its consequences mitigations be assured. This should be achieved, in particular, by defence of hermetic enclosure from damages and keeping its functionality. The final task is to return the unit in a control state when chain fission reaction is terminated, permanent nuclear fuel cooling and keeping radioactive substances in established boundaries are provided.

There is no severe accident definition in [3], however there is definition No 62 of SEVERE BEYOND DESIGN BASIS ACCIDENT, as beyond design basis accident with fuel elements damage exceeding maximal design limits (established in [4]) which may result in achievement of maximum permissible accidental release of radioactive substances to environment.

Thus, in accordance with Russian regulatory framework Russian severe accidents – are a subset of all BDBAs set, i.e. those BDBAs which include phase of severe fuel and protective barriers damages and with this connection corresponds to representative's criteria [5]. Analysis of BDBAs consequences including accidents with core melting is a basis for Emergency planning of personnel and population protection preparation, as well for BDBAMG development (as *it. 1.2.16* [3]), which in turn permits to manage such accidents, so assured Level 4 strength.

In relation to SA on NPP "Fukushima", it is established in *it. 4.1.6.* [6], that for the site located on sea coast or water body, it is necessary to determine probability of tsunami (seiche) initiation and maximal height of tsunami wave considering seism tectonic conditions and a shore configuration.

3. BDBAMG DEVELOPMENT – AS "STRESS TEST" FOR UNIT DESIGN

BDBAMG development for a new unit is launch when its design development is finished (or mainly finished). During BDBAMG development, as it will be demonstrated bellow, the revision of design basis of some elements composing DiD Levels, should be carried out. This procedure is named "stress test" [1] now. The revision of DiD and "stress test"

[1] Term "stress test" appeared after accident on NPP "Fukushima" to name procedure for design basis of NPPs revision in point of external impacts and SA.

fulfilment were carried after SF on NPP "Fukushima". The re-evaluation results may be the basis for unit modernization, i.e. BDBAMG development may also influence on the design, thus strengthening DiD realized in the design.

3.1. Preparation for development (connection with Levels 1 and 2)

The effectiveness of personnel activity per guidance is formed during the phase of preparation for its direct development. Preparation contains two main components:

(1) evaluation of safety substantiation calculations fulfilled, including PSA;

(2) investigation and consideration of NPP Unit capabilities and the site of its location.

3.1.1. Evaluation of safety substantiation calculations presented in SAR and PSA

3.1.1.1. Evaluation of representative BDBA scenarios selection

a. The substantiation of representative BDBA scenarios selection for AM measures analysis and definition and development of plans arrangements for personnel and population protection is attained by *postulating of NPP unit levels of severity state*. The possible combinations of protective barriers states, each of which identifies the corresponding *unit's levels of severity state,* are generated with the help of combinatorial analysis. The physical realizability of each barrier damage rate is identified with revealing a mechanism of such damage, as well as reasons which may cause it (e.g. extreme IE). The following barriers structure should be considered for NPP units with VVER-1000, which mainly corresponds to those identified in [1]:
    - fuel matrix and fuel cladding (combined in term nuclear fuel);
    - first circuit boundary (excluding reactor vessel) ;
    - reactor vessel;
    - hermetic enclosure (for VVER-440) or containment (for VVER-1000).
b. Application of PSA results should be evaluated for vulnerability places identification through minimal cross sections of event/failure tree, as it is necessary for identification of BDBA initiation reasons, it progression and transition to severe phase. The PSA results should be obtained for the complete list of initiating events which are personnel errors or causing NPP components failures, on site EI - fires and flooding, external impacts of nature and anthropogenic character. All EIs should be considered, if they are physically not excluded at the place of unit location. If some scenario is of very low probability or even not considered in PSA, it should not be a reasons for exclusion from BDBAs list. Severe accidents management measures should be developed irrespective for calculated hazards frequency, taking into consideration uncertainties in severe accidents scenarios (*it.2.12.* [7]).
c. The analysis of selected BDBA scenarios and their consequences should be presented in SAR [5]. Those scenarios should be selected, which provide coverage of all physically possible severe states of a unit and meet following representativeness criteria:
    - maximal dose rate for personnel and /or population;
    - maximal intensity of radionuclide's release;
    - maximal integral radionuclide's release;

- maximal scale of systems and components damage on the plant;
- maximal input in cumulative core damage frequency for given group;
- more quick progression of accident events (minimal float in personnel disposal to undertake accident management measures);
- the worst conditions for personnel and equipment performance.

The evaluation of calculation scenarios selection may result in necessity of its changes.

3.1.1.2. Representative scenarios calculations for strategies and instructions substantiation

a. Realistic (best estimate) method. 3-D codes application: BDBAs calculation analysis for BDBAMG strategies and instructions substantiation (as for any accident instructions) should be performed in frame of so called realistic (best estimate) method which provides AM on the basis of realistic symptoms of unit state and evaluates available resources of existing unit's systems and equipment serviceability and efficiency as well as personnel capabilities for control of such equipment. Based on calculations results design basis safety margins (e.g. departure from the nucleate boiling ratio criterion) in the frame of which *operation with deviations* is still possible, are checked. 3-D codes application is necessary when local effects are significant and processes in the core are asymmetrical.
b. Consideration of uncertainties: calculation analysis results should be accompanied by demonstration of uncertainties analysis. Consideration should be given to uncertainties of calculation methods, equipment characteristics, instrumentation sensitivity and other uncertainties, taken into account in the evaluation of the result.
c. Results of calculations and analyses usage: on the basis of calculations and analyses the following is identified, then to be used:

    - specific symptoms of levels of severity;
    - criteria of transition to severe phase;
    - timing of accident scenario progression;
    - parameters for identification of success/not success of personnel actions;
    - radiation consequences in compartments and on the site.

d. Elaboration of auxiliary calculation means: results of calculations and analyses, if necessary, may be used for elaboration on their basis auxiliary calculation means, which may be used for indirect parameters assessment, in case of unavailability of technical means of measurements, and also for checking the authenticity of obtained information.

3.1.2. Investigation of NPP Unit capabilities and site location

3.1.2.1. Means and methods of information acquisition for AM

The following is to be checked and assessed:

a. Design control and instrumentation devices with respect to their applicability for acquisition of information required for accident management [8], including:

- capabilities of control room and reserve control room, information calculated system/safety panel (if exist), local control desks, means of measurements in reactor shaft, in containment;
- correspondence of their measurement ranges to AM aims, gauges and cable lines operability in SA conditions at places of their location, the required processing speed;
- the capability of measurement systems to provide minimal required information (parameters) content necessary for tracking unit state signs and identification of accident level of severity, control of AM actions success;
- provision of required technical systems control.

b. Possibilities to compensate for failures of design measurements channels, e.g. by information acquisition through indirect methods, such as: noise, steaming, position of regulatory devices pillar position of locking devices etc. which may defined at places of location, in case radiation conditions permit. The possibility to use non-stationary (hand-held, transportable) measurement means should be considered.

c. Methods for indirect assessment of missing parameters by carrying out operational calculations or by auxiliary calculated means which forecast required parameters value with the help of physical processes mathematical models;

d. Methods of identification and screening of false information coming from measurement channels, which may be damaged in BDBA conditions.

Such investigation may result in recommendations on modernization of measurement channels, e.g. installation of additional gauges or replacement of existing ones.

3.1.2.2. Technological equipment of the unit

In relation to technological equipment (including equipment of SS):

a. Equipment should be revealed, which can be used for AM and also beyond the scope of its design dedication and/or qualification limits, it is check if it will be operable in these conditions and how long, what will be its performance beyond the design range of operation;

b. It should be identified if adverse conditions of environment and external and internal impacts (including mechanical) of severe BDBA will influence the equipment operability;

c. Effect of auxiliary and supporting systems failures should be assessed;

d. Alternative equipment needed for realization of actions in the frames of defined strategy should be identified, as well time required for putting it in operation;

e. Assessment of both the necessity and possibility of main and alternative equipment to operate jointly[2] should be performed.

[2] The assessment is performed by additional calculations; on results of which it should be defined whether it is necessary to continue recovery of main equipment operability and for what time.

3.1.2.3. Ensuring electricity supply [3]

The reasons of complete electricity supply failure (station "black-out", i.e. diesel generators are not operable) should be defined and in case of all sources of alternating-current loss the relevant measures of it restoration should be developed. Such means of restoration as delivery of portable generators, increasing of battery energy storage capacity, installation of alternative alternating-current sources, connecting up to external nets, should be studied.

3.1.2.4. Containment[4]

The strength of containment in BDBA conditions is assessed and real non-tightness of hermetic enclosure. Penetrations, hatches, doors, locks and their embedded fittings as well insulating devices are investigated for the results to be considered in BDBAMG. Special attention should be given to systems for containment depressurization and for algorithms of their actuation (in particular of sprinkler system in presence of hydrogen in containment atmosphere).

Containments of NPPs with VVER reactors are equipped with passive H_2 recombiners. Their sufficiency and places of location in design of unit should be assessed.

As a part of long term accident management, the means for water feeding in containment should be provided with pressure equal maximum permissible containment pressure and with capacity sufficient for residual heat remove [9].

It should be checked the necessity and admissibility of direct discharge of radioactive substances from containment through special filtered venting for severe accidents.

3.1.2.5. Utilization of site and neighbouring unit's technical means

The possibility to utilize technical means (materials and equipment) from other units should be considered for multiunit site with conditions, that it is not hazardous for their operation safety ensuring. It should be considered if it will be necessary or not shut down neighbouring unit (or units).

3.1.2.6. Conditions of possibility technical means using

The investigation should be carried out in respect to possibility of and accessibility to technical means for personnel actions execution considering conditions which may be in compartment and on the site as a result of initial event or in the course of accident progression (radiation consequences, fire, possible blockages, building construction's destruction, flooding, steaming).

Such investigation may result in auxiliary measures directed on the risk reduction and improvements of physical accessibility. The necessity of some plant system or areas of work modification (e.g. through addition of protections) should be studied.

[3] Electricity supply provision is a top-priority task of accident management since without electricity supply any actions are impossible.

[4] The problem of "containment bypass" due to leak from prime circuit to secondary and unclosing of relief valve (BRU-A) is not considered in the section.

3.2. Development of strategies and actions (connection with Levels 3 and 5)

3.2.1. Transition to BDBAM actions (connection with Levels 3)

In case of unsuccessful prevention with help safety systems and relevant accident procedures transition of initial events in design basis accidents and design basis accidents to beyond design basis accidents, it is necessary to start with BDBAMG execution (Level 4). The *criteria* (parameters, conditions) giving evidence, that Level 3 is surmounted (or there is a hazard of it surmount) should be defined in Level 3 instructions and in BDBAMG. Fact of BDBA beginnings is identifying on noncompliance of appeared symptoms with symptoms of design basis accidents and/or on deviations from design accident progression and systems and equipment behaviour anticipated according instructions for design basis accidents elimination on the unit, or from other instructions for prevention of progressing and for elimination of normal operation violation.

Actions in frames of BDBAMG for safety functions (SF) state analysis may be initiated in parallel with Level 3 instructions execution, e.g. after scram.

3.2.1.1. Immediate actions

The immediate actions should be stipulated after transition to BDBAMG, which relating to: "Control of reactivity and ensuring of reactor sub criticality", i.e. reactor should be shut down and keeping in sub critical condition. Next on priority is SF "Core cooling (heat removal from reactor)".

3.2.1.2. Strategy and actions on prevention (of severe accident) phase

Strategy on prevention phase is directed at SF restoration. It should provide identification of state of the unit (levels of accident severity) and correspondent to them SF, based on directly observe or indirectly assessed parameters (symptoms), and also combine all developed actions for recovery and ensuring of SF.

The sequence of actions for SF protection and recovery should be identified in strategy with consideration of this function prioritization. The necessity of simultaneous actions implementation of different SFs should be defined on the basis accidents analysis.

3.2.1.3. Strategies and actions on "mitigation of consequences" stage

The criterion of BDBA transition to severe phase and subsequent transition to strategies on stage of severe accident management should be defined. Strategies may be derived from 'candidate high level actions' [7], which should provide protection of physical barriers (body of reactor vessel, steam generator pipes, containment) as well restoration of core cooling to the maximum possible extent or fragments of core (derrises) cooling.

The limited number of parameters to be used for accident management and for identification of format and priorities of diagnostics should be defined on the base of severe accidents investigations.

The following should be envisaged in the development of personnel actions:

- Possible negative consequences of actions and also cliff edge effects;
- Limitations for implementation of actions coursed by doze, physical, psycho-emotional loads on personnel and those who are involved in AM;

- Actions, resulting from insufficient[5] number of personnel to carry management actions.

3.2.2. Radiation situation and start of emergency planning of personnel and population protection (connection with Level 5)

The procedure ordering introduction of Emergency planning of personnel and population protection should be specified in BDBAMG in case of BDBA occurrence (it. 4.11. [4]), i.e. transition on Level 5. Numerical values of effective dose rates and (or) I^{131} volumetric activity in compartments air, on NPP's site, in sanitary protective zone and zone of radiation tracking, which corresponds to conditions of "Emergency preparedness" and/or "Emergency situation" [10] are criteria for the introduction.

3.2.3. Organizational structure of accident management.

3.2.3.1. Administration and NPP operations staff

Analysis of the existing on NPP organizational structure for normal operation should be carried out for its maximal application in BDBAM implementation. Allocation of rights, duties and responsibilities of individuals from operations staff should be defined for participation in BDBAM. The procedure should be developed to provide continuation of accident management in case if a new shift of NPP personnel and involved persons are not able to come on the NPP, in particular in long term of accident progression, which should identify the method of shift exchange.

3.2.3.2. The means of communication and warning

The following is checked:

- sufficiency of existing communication means, including duplication ones for organization of NPP management and systems of warning in conditions of normal operation, design basis and beyond design basis accidents (it. 1.2.23 [3]);
- means for communication with external and internal accident centers for NPP management in conditions of BDBAs for assessment of situation and decision making (it. 2.4.28.[4]).

3.2.3.3. Involvement of external organizations for BDBAM and elimination of consequences

Tasks distribution between personnel and involved organizations defined in BDBAMG for realization of measures directed at accident consequences mitigation, chain fission reaction termination and nuclear fuel cooling in reactor. In particular, NPP administration cooperation with Team for emergency assistance to nuclear plants (OPAS) is defined by requirements in Annex 20 (obligatory) to [10].

The issues of personnel and public protection in case of accidents at nuclear plants are settled in Russia in the frames of acting Unified National System for Prevention and Mitigation of Emergencies, which, in details described in [11]. Overview of these issues is not the subject of this paper.

[5] As a result of injury, overexposure, death, desertion, etc.

3.3. Checking (verification[6]) of applicability: use of simulator

The final stage of BDBAMG development is verification of its applicability to confirm that BDBAMG is technically correct and provides proper consideration of human factor.

3.3.1. Verification tasks

Verification means resolving of two main tasks:

- to check usability, that means from one hand sufficient specification level, and from another simplicity of understanding of instructions and other provisions in Guidance;
- to check correctness (precision) of instructions and provisions in Guidance, which should confirm it compatibility with technical means of the particular unit and also compatibility with personnel capabilities.

3.3.2. Usage of full-scale simulator

Different methods and means may be used for BDBAMG checking. Method of modelling on full-scale simulator (method MFSS) is mostly preferable from them due to that MFSS is based on software enabling modelling initial state of the unit and also accident progression, including relevant personnel actions [12].

However, it should be considered, that in SA phase there are some challenges for MFSS applications, connected with limitations and uncertainties in severe accidents phenomenology knowledge, as well with the level of software verification in relation to some separate effects (e.g. steam explosion possibility, repeated criticality, hydrogen generation and distribution, including possibility of it detonation or deflagration, thermo shock). Moreover, the software of simulator should be able to model severe accident phase progression and NPP response in *scale of real time* mode. *This may result in full-scale simulator software reprocessing.*

Verification results may have feedback with BDBAMG, resulting in correspondent changes in it. For instance, if cliff-edge effects possibilities had not been investigated during preparatory phase, additional sensitivity analyses may be an input for this investigation. Possibilities of cliff-edge effects should be investigated as a result of possible degradation of equipment performance and of alternative mitigation strategies for a common plant symptom and containment challenge [13]. Supplemental analyses should also include a small set of cases examining damage plant states resulting from low frequency, high-consequence scenarios.

4. PERSONNEL TRAINING TO BDBAMG ACTIONS (CONNECTION WITH LEVEL 1)

Personnel training for BDBAMG actions are carried out on the basis of a special training program which should include two sections – theoretical and on-the-job (exercises) training. Theoretical training provides for the development of knowledge which would serve as the basis for adequate decision-making with regard to BDBAM under conditions of uncertainties characteristic of such kind of accidents that is supposed that BDBAM will be based not only on skills but also on knowledge. Exercises should be carried out on a periodic

[6] It means verification and validation in terminology of IAEA documents, e.g. [8]. However, in Russian regulatory framework term *validation* does not exist.

basis and include actions of personnel both in control room or reserve control room, as well as outside (simulator, for example).

Exercises outside control room should provide for the development of skills of personnel dislocation to areas of a unit relevant for AM in conditions as close as possible to what could be expected during an accident (poor visibility, fumigation, no light, flooding/destruction, increased level of radiation).

AM training at a severe stage should be included, on a periodic basis, in the scope of exercises on implementation of personnel and public protection action plans. *Thereby, the personnel qualification is maintained /improved.*

5. CONCLUSIONS

The qualitative implementation of all stages of preparation for development and development BDBAMG provide the guidance effectiveness (strength of Level 4) and at the same time provide strengthening of DiD as a whole. The interrelations between elements forming the Levels of DiD and elements of BDBAMG preparation and development stages are presented in Fig.1.

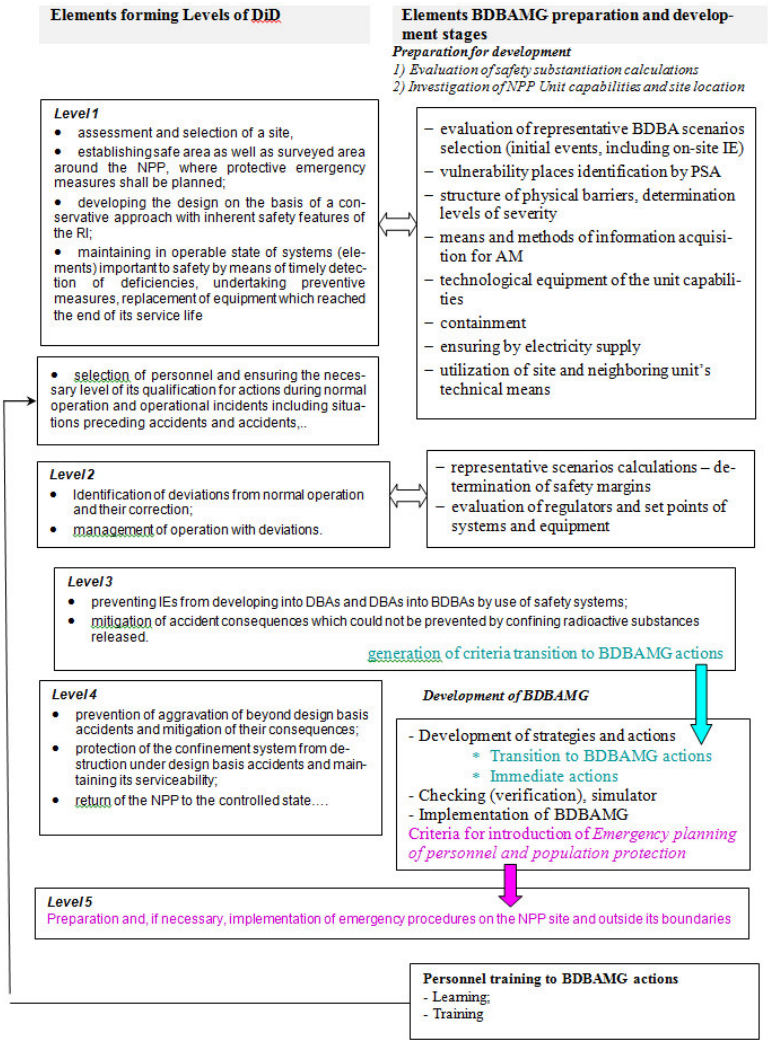

FIG.1. Scheme of interrelations between elements forming Levels of DiD and elements BDBAMG preparation and development stages.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[3] GOSATOMNADZOR OF RUSSIA, General Provisions for NPP Safety Assurance (OPB-88/97), NP-001-97 (PNAE G-01-011-97).

[4] GOSATOMNADZOR OF RUSSIA, Rules of Nuclear Safety of Nuclear Power Plant Reactor Installations, NP-082-07.

[5] GOSATOMNADZOR OF RUSSIA, Requirements for the Content of the Safety Analysis Report for Nuclear Power Plants with VVER Reactors, NP-006-98.

[6] GOSATOMNADZOR OF RUSSIA, Nuclear Power Plant Siting: Basic Safety Criteria and Requirements, NP-032-01.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards, Safety Guide No. NS-G-2.15, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementation of Accident Management Programmes in Nuclear Power Plants, Safety Reports Series No. 32, IAEA, Vienna (2004).

[9] European Utility Requirements for LWR Nuclear Power Plants. Volume 2. Generic Nuclear Island Requirements. Chapter 1. Safety Requirements. Revision C. April (2001).

[10] GOSATOMNADZOR OF RUSSIA, Standard Content of an Action Plan for Personnel Protection in Case of a Nuclear Plant Accident, NP-015-2000 with Amendment of 30 August 2002 No. 1.

[11] Fifth National Report of the Russian Federation on the Fulfilment of Commitments Arising from the Convention on Nuclear Safety for Period 2008 - 2010.

[12] GOSATOMNADZOR OF RUSSIA, Requirements for Full-Scale Simulators for Training NPP Control Room Operators, NP-003-97.

[13] AREVA NP Inc. The Operating Strategies for Severe Accidents Methodology for the U.S. EPR™ Technical Report. ANP-10314, Revision 0, August (2010).

IMPROVEMENTS IN DEFENSE IN DEPTH IN FRENCH NUCLEAR POWER PLANTS FOLLOWING FUKUSHIMA ACCIDENTS

J. BARBAUD*, X. POUGET-ABADIE**
* EDF SEPTEN,
Villeurbanne Cedex, France
** EDF DIN Headquarters,
Saint-Denis, France
Email: jean.barbaud@edf.fr

Abstract

The accidents which occurred in the nuclear power plants in Fukushima-Daiichi resulted in a complementary safety assessment (CSA or stress-tests) of all French NPPs to confirm their compliance with their design bases and to evaluate their behaviour beyond it. They have shown that nuclear facilities have a satisfactory level of safety, but it had been decided to significantly improve their robustness to extreme situations, beyond the safety margins they have already. Planned improvements include several parts, where the main ones are the implementation of a hardened safety core (HSC) of key components for the management of extreme situations resulting from a hazard beyond the design and deployment of a nuclear rapid response force (FARN). The hardened safety core aims to avoid massive releases and lasting effects in the environment. It relies on existing or new components designed or verified to hazards with significant margins compared to the design levels of NPP beyond. It also includes provisions allowing crisis management, including crisis centre and communication means. The FARN complements the HSC and the crisis organization to bring from off-site sufficient human and material resources to increase the autonomy of the site. All these improvement contribute to a better defence in depth.

1. INTRODUCTION

Following the severe accidents which started in the Fukushima NPP on 11 March 2011, CSA of all French NPPs, as all 140 existing European reactors were decided. CSA was more important, and made in a shorter time, than safety reviews undertaken after each important event, such as Blayais flooding, in 1999.

Facing this challenge, French NPPs have specific advantages, such as a high degree of standardization which provides margins, and a regular practice of Periodic Safety Review (PSRs). They are already equipped with Passive Autocatalytic Recombiners (PARs), and Containment Filtered Venting (CFV) which reduce significantly the risk of long-lasting releases. However the CSA revealed the possibility to increase the robustness of the plant to face hazards beyond the design.

2. COMPLEMENTARY SAFETY ASSESSMENT

2.1. General Context and Planning

Less than two weeks after Fukushima event, European authorities requested that a comprehensive safety assessment, in light of preliminary lessons learned from the accident, be performed on all EU nuclear plants. The stress tests specification validated in May requires analysis on 6 items: earthquake, flooding, other natural hazards, total loss of electrical supply, total loss of heat sink, and management of severe accidents. It includes a first part with description of the current design basis, and check of conformity of the installation, and an evaluation of behavior of the plant beyond the design basis, in order to identify possible cliff-edge effects and propose ways to increase plant robustness.

The CSA was completed in September by EDF and reviewed by Institut de Radioprotection et de Sûreté Nucléaire (IRSN). The opinion of ASN is summarized in a national report, which was itself the object of peer-reviews performed by Safety Authorities of the 17 participating countries. The process is achieved by editing technical prescriptions from ASN to EDF, in June 2012.

2.2. Earthquake Analysis

The original design requirement for ground motion was determined according to French Standard RFS I.2.c. This RFS was updated in 2001 and the needs to upgrade the plants were checked during PSRs. The design requirement of a plant is called SMS. For the design of standard parts of a given series, an envelope response spectrum which bounds all the possible SMS and soil conditions of the series sites is defined. It is called Design Basis Spectrum, which in practice provides margins against SMS for a large part of the sites of a series.

Beyond the design, evaluations where already performed on two sites: a full Seismic Margin Assessment (SMA) in Tricastin, and a seismic Probabilistic Safety Assessment (sPSA) in Saint-Alban. Standardization of nuclear island enables to extend a wide part of the conclusions to other sites of the same series.

For the purpose of CSA, a new analysis was performed to evaluate the behaviour of the plant to about 1.5 SMS. Seismic walkdowns were performed on each reactor. Only the minimum set of equipment needed in case of SBO, around 200 components, was checked considering the limited time to perform the evaluations, the results of the previous evaluations, and the obligation to consider SBO in other parts of CSA. The main conclusion of these evaluations is that seismic capacity of SSCs needed is generally larger than 1.5 SMS. However, the capacity of some specific equipment needs to be further checked and eventually reinforced for this severe level of earthquake to increase robustness of the units, mainly secured make-up to Emergency Feedwater (EFW) storage tank, to Reactor Water Storage Tank (RWST) and to Spent Fuel Pond (SFP), Emergency Control Center, and sand bed filter.

2.3. Flooding Analysis

The original design requirement for design basis flooding was determined according to French Standard RFS I.2.e. It defines a design reference level called CMS, which depends on the type of site (river or sea side). Following the Blayais flooding (1999), a comprehensive reassessment of the flooding risk where undertaken. It included an update of the risks listed in RFS, taking into account the last available data, complemented with 7 additional hazards: deterioration of a water storage in case of earthquake, intumescence, rainfall, ground water, failure or equipment item and influence of the wind on the river, on intake channel, or on the sea (i.e., wave swell) according to the type of site. Combinations are also considered if dependency links exist between them.

For the sites where the platform level was not sufficient according to the revision of CMS and its combinations, a peripheral protection (i.e., dikes) was erected or over elevated. Moreover, as a first protection against ground water and defence in depth protection against other hazards, a volumetric protection was implemented. It consists in a leak-tight envelop including the volume of all the building sheltering safety related equipment, up to the platform level. All the piping, cable or underground penetrations were plugged using tested materials. For a few sites, where presence of water cannot be excluded on the platform and where a delay for implementing protection is guaranteed, this protection has been extended over the platform using mobile protection equipment.

For the purpose of CSA, the hazards levels have been increased using fixed coefficients, to provide an important margin while remaining plausible:

- The flow rate used for CMS of rivers have been increased of 30 %.
- Storm surge have been increased by 1 m for coastal or estuary sites.
- Rain flow rates have been doubled.
- Additional failures over the platform due to heavier earthquake have been considered.

The main conclusion is that all sites have margins with respect to updated design basis, once the protective works decided as a result of analysis following Blayais event are completed in due time. However, some sites have no margins or even negative margins with respect to CSA assumptions. The quantity of water brought by rain or failures over platform is generally limited to a few cm or dm. But increase in CMS may reach up to 2 m for few sites. For these sites, three types of conditions may be triggered: Loss of Ultimate Heat Sink (LUHS), Loss of Off-Site Power (LOOP), and SBO.

To increase robustness of these sites, measures are being considered such as reinforcements or rising of peripheral dikes, elevation above the platform level of the volumetric protection, or limit the additional protection to a set of key functions needed to reach and maintain the unit in a safe state, in a watertight protection when the platform is flooded. A study is in progress to check if for some sites an important earthquake upstream the site could cause the break of more than one dam (the most penalizing one is already in design basis).

2.4. Other Extreme External Hazards

The external hazards linked to the risk of flooding, and not fully examined in the previous chapter were examined, that is hail, lightning and wind. Direct effect of extreme winds and lightning are already considered in the design basis, and wind induced projectiles were considered through PSR. The standard design of structures against an external explosion of 5 kPa provides an important margin against direct effect of extreme winds. Robustness against indirect effect of extreme winds combined with LOOP of 6 hrs and LUHS has been assessed leading to protection of specific equipment. Robustness of equipment sensitive to hail has been confirmed.

No cliff edge effect has been identified for these hazards. Additional studies are being performed to increase robustness of plant to extreme winds: assessment of the resilience of the CFV, and identification of equipment needed for the emergency plan to be reinforced.

2.5. Loss of Electrical Power and Cooling Systems

LOOP is included in the original design of the plant, and subsequent modifications enabled to take into account more complicated situations such as SBO and LUHS. Autonomy for LOOP is around 3.5 days for the fuel tank, and it is at least 100 hours for LUHS when only one unit of a site is concerned. This value may be reduced in case of accident concerning all units, but the minimum value was increased during last PSR to 24h for coastal sites and 60h for others.

In case of SBO, coping means are the EFW turbine driven pump and the turbine driven generator (called LLS) to supply Chemical and Volumetric Control System (CVCS) hydrotest pump for Reactor Coolant Pump (RCP) seal injection and minimum Instrumentation and Control (I&C). Minimum autonomy is about 24 h before core uncover.

Beyond the design, no recovery of these means was considered, and additional cases where studied: SBO + loss of any other on-site backup electrical power, without external hazards, and SBO + LUHS, with CSA type hazards. Additional studies will be performed to assess the possibility for LLS and EFW turbine driven pump to continue to operate after 24 h even if ventilation systems are lost, and to check by tests the behaviour of existing RCP seals at high temperatures. Other cliff edge effects may appear due to decrease in pressure of Steam generators (SGs), to insufficient quantity of water in EFW tanks, and shared components between units.

To improve the behaviour of the units, the main improvements being studied are the increase of battery autonomy, the implementation of additional generator sets for each unit, and the addition of ultimate ways to recharge water in EFW system and in SFP that are unlimited in nature (drilling, basins...).

2.6. Severe Accidents

Severe accident management was introduced progressively in the plants through the PSRs, taking into account the feedback from foreign accidents and the results of research and development (R&D) programs EDF participate in this field. The main provisions available on the units are the CFV using sand bed filter outside the containment and metallic prefilter inside, against slow pressurization, PARs inside containment building, and reliable depressurization of reactor cooling system (RCS) to avoid pressurized core melt and induced SG tube rupture (being implemented),

The main measures studied to improve the behaviour of the plants are:

- To strengthen the electrical back-up of ventilation filtration system of the control room to improve its habitability.
- To systematically ensure a basic pH of water in containment in case of core melt to limit iodine emissions, thus reducing the short term impact of the situation.
- To improve the filtration of organic iodine.

3. THE SAFETY IMPROVEMENTS

3.1. General

At the end of the CSA, ASN considered that the NPPs have a sufficient safety level that enables her not to require immediate shutdown of any of them, but also considered that it is necessary to increase their robustness against extreme situations, beyond the safety margins they already have and detailed the measures intended to be required from the licensees.

These requirements were prescribed to EDF, with about 30 prescriptions per site, but a wide part of them is common to all sites. They recall the main improvements and additional studies proposed by EDF in its CSA, as indicated in chapter 2, and supplemented by recommendations issued by the safety advisory group. In particular, operators will have to set up a HSC to face event of great magnitude, to create the FARN, and correspondingly adapt the crisis organization. EDF submitted its Post-Fukushima Action Plan to ASN mid 2012. It comprises over 500 actions identified, which will induce considerable work involving a particular investment and human resources and skills. A 3 steps program is defined.

Step 1 is composed of short-term actions intended to be deployed from 2012 to 2014/2015. It includes crisis means and interim features for beyond design SBO and LUHS (several units, long durations) such as “Plug and Play” connections for air, water, and electricity re-supply on each NPP, on-site mobile or temporary installed equipment to be deployed by the site staff before 24h (additional emergency diesel groups,…), and 1st part of emergency organization improvements enabling multi units events management. It includes also the FARN deployment with human resources and mobile equipment coming from offsite.

Step 2, composed of midterm actions is intended to be deployed from 2014 to 2018/2020. It includes definitive design means of the HSC (ultimate diesel generators and water make-up). The first two steps enable a significant safety benefit, by already managing extreme situations beyond the framework of the referential, directly induced by the lessons of Fukushima.

Step 3 composed of long term covering actions is intended to be deployed from 2019. It consists of the ultimate HSC preventing, in most extreme deterministic beyond design situations, large and long-lasting radioactive releases in the environment. It includes severe accidents primary injection pump, improved “feed and bleed” design, improved containment venting and filtration (or additional containment cooling).

3.2. Hardened Safety Core

It is composed of physical and organizational provisions robust for extreme situations to prevent or limit the progression of an accident with fuel melt, mitigate large-scale radioactive releases, and allow the operator to perform its crisis management missions. It is preferably composed of independent and diversified Structures, Systems and Components (SSCs) in relation to the existing ones to minimize common-mode. Use of undiversified or existing SSCs shall be justified.

For EDF, the HSC constitutes an ultimate safety net which will be used only in the hypothetical case the previous parts of the comprehensive approach to safety are not sufficient:

- The deterministic sizing of the plant, which remains the cornerstone of nuclear safety,
- Margins and additional features which enable to improve the behaviour beyond the design. EDF recalls that parts of the Post-Fukushima actions include improvements of this aspect.

This role enables to include in the HSC only a limited number of key functions, making it possible to improve their robustness to high levels of hazards and taking account of all effects induced by the whole installation on these components. In this logic, the objective of this ultimate line of defence is for EDF to avoid massive releases and the lasting effects in the environment. EDF estimates that more realistic rules than those used for sizing may be used.

The perimeter of HSC has been proposed by EDF and may be subject to additional prescriptions from ASN:

- Ultimate Additional Back-up Diesel (DUS), batteries, electrical connections.
- Instrumentation to diagnose the state of the plant, assess and predict the radiological impact of releases on the workers and the people (weather and environmental measures), control the HSC.
- Diversified EFW to the SGs.
- Depressurization of the RCS, and sufficient injection capacity to maintain vessel integrity.
- Reinforced water make-up supply to SFP and reactor pool.
- Containment isolation.
- New Local Crisis Centre (LCC).
- Mobile devices and means of communication essential to emergency management.

Implementation of the DUS is one of the main and hardest points. The objective is to implement it by 2018, but a first improvement will be already operational mid-2013 with lighter generator sets and mobile devices for make-up water.

New LCC will be deployed between 2016 (Flamanville) and 2020. This standard building will be large enough and equipped to manage the crisis on a long term basis, taking into account all its aspects. It will include plant data supervision room with essential data, intervention facilities, crisis management equipment, mobile equipment storage and offer living conditions (rest, food, hygiene). It is designed for a capacity of 100 people (x2 during

shift turn-over), to remain accessible and habitable at all times and to handle a multi-unit crisis.

The proposed loading cases for HSC are derived from those considered in CSA. SSCs belonging to HSC are to be protected from effects induced by these extreme situations, either internal like load falls, fires, explosions, or on the dangerous installations located in the vicinity of the plant, such as important fires, explosion, or toxic gases.

For earthquake, EDF decided to take into consideration, in addition to the increases already considered for the CSA, the rules applicable to other dangerous classified installations. This choice leads to apply to some sites an increase up to 100% SMS (for instance Fessenheim, Bugey and Blayais) or even 200% (St Alban). Spectral shapes associated with these acceleration levels remain defined according to RFS.

The HSC will also take into account other natural phenomena, namely lightning (maximum load of 300 kA with a specific energy of 45 MJ/Ohm), hail (50 mm diameter with a speed of 32 m/s and a density in the range of 0.9), and an EF4 tornado.

3.3. The FARN

Less than two months after the Fukushima event, EDF decided to implement a FARN, able to quickly provide assistance from off-site to a plant facing big difficulties, with human and equipment support. Deployment began late 2012 and will be completed in the year 2015. The objective of the FARN is to be able to arrive on a NPP site in accident conditions within 12h in order to bring skilled operators on site to help the local shift, and possibly take over from the personnel of the site, if partially or totally unavailable. If on-site equipment is no more available, the FARN will supply its own mobile equipment to re-establish or maintain core and spent fuel pool cooling, to avoid as much as possible core melt or significant release, or limit them. It ensures supply chain and technical support. The autonomy goals are as follows:

- Use of the existing fixed equipment remained available and implementation of local mobile equipment to be deployed by the teams on site will allow site autonomy of at least 24 h.
- After 24h, the FARN, with its own dedicated human resources and dedicated mobile equipment, will supply the site to guarantee autonomy of at least 72 h.
- After 72h, additional resources of the EDF Group, and if necessary from partners, will guarantee the durability of the safe situation.

The FARN design considers that only one site out of the 19 sites faces a severe accident, that infrastructures may have experienced major destructions, including access to the site, and that the work environment may include radiological and/or chemical hazards.

FARN is fully included in the EDF national crisis organization. Decision of FARN alerting is made by nuclear fleet Director, on request of the NPP management, advised by a FARN headquarters member.

FARN organization has National and Regional means. The national level comprises about 30 on-call people, who allow advising at national crisis centre, constitution of 5 on-call reconnaissance teams of 4 individuals each, and management of the whole organization. It has also a national equipment base, with long term equipment and rear bases modules. The regional level is deployed on 4 NPP sites. Each of these FARN services is staffed by about 70 on call people, who allow constituting 5 rescue teams of about 14 individuals each, including team leaders and different skills (operation, maintenance, safety, radioprotection and logistics). Each reconnaissance or rescue team is country wide intervention.

FARN regional centres people share their working time between the NPP (to maintain and develop competencies and qualification skills) and FARN. 50 % of their activities are dedicated to the FARN. It includes training, exercises, maintenance and periodical test of mobile equipment, documentation.

3.4. Defence in depth improvement

Reference [1] describes the concept of defence in depth, introducing 5 different levels:

1) The first one consists in prevention of anticipated operational occurrences and of failure of items important to safety, which would lead to accidents.
2) The purpose of the second level is to prevent anticipated operational occurrences from escalating to accident conditions.
3) At the third level of defence, accidents are postulated to occur, and the purpose of this level is prevention of damage to the reactor core and significant off-site releases from these accidents.
4) The purpose of the fourth level of defence is to mitigate the consequences of accidents that involve significant core damage. The most important objective for this level is to ensure the confinement function, thus reducing consequences as low as reasonably achievable.
5) The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accident conditions.

Reference [2] proposes in addition to subdivide level 3 between 3a and 3b, corresponding to single initiating events and multiple failure events. For the purpose of this paper, this distinction will be considered, as the loss of functions considered in CSA are multiple failure events.

Generation III power plants integrate all these levels in their original design, while level 3b and 4 were introduced and reinforced progressively on the French fleet, through PSR process, considering deterministic and probabilistic inputs. This introduction reinforces the robustness of the plants in prevention of core damage (3b) and prevention of large releases if core damage occurs (4). Other levels were also reinforced trough PSR process.

EDF's Post-Fukushima Action Plan also reinforces defence in depth, mainly levels 1, 3b, 4 and 5.

Level 1 is mainly reinforced when additional protection is made against the hazards, for instance increase of entrance levels to prevent water entrance in buildings, of rise in peripheral dikes. Improved assurance of good behaviour or reinforcement of existing SSCs such as RCS or SFP to HSC loads contribute to prevention of accidents and thus belongs to level 1.

Plug and play and mobile components, as well as HSC or FARN constitute a response to situations where a lot of fixed devices of the plant are lost. So they mainly belong to level 3b and 4. Part of the added means are intended to prevent core melt, such as make-up to SFP or to EFW and can be considered as 3b, while other ones are intended to mitigate consequences of core melt situations, such as assurance of a basic pH of water in containment, thus belonging to level 4. The DUS and the FARN organization are used in both situations.

LCC and crisis means such as communication belongs mainly to level 5, but LCC will also be used for other levels, including 3a. As it is used to protect on-site mobile equipment, it brings a wide contribution to levels 3b and 4.

As far as reasonably possible, these new equipment and organization are independent from the existing ones, thus providing a good efficiency of the increase in defence in depth.

4. CONCLUSIONS

The CSA confirm the benefit of EDF fundamentals, for instance

- the action as architect-engineer and operator which enable mastering the design and improvement of plants,
- the high degree of standardization of the EDF fleet, which enables to take benefit from operating feedback of more than 1,700 reactor-years,
- Regular PSR which enable to systematically take into account national and international feedback and make improvements on the plant accordingly.

The CSA confirm also the analysis previously made by EDF for its Long Term Operation program. A wide part of the main post Fukushima items (water ultimate supply; new ultimate diesels…) were part of this program prior to Fukushima. The CSA led to accelerate the implementation of these major improvements, but also introduced new concepts, mainly the HSC including a limited number of key safety SSCs protected against beyond design extreme external hazards, and the FARN, new crisis human and equipment means to cope with an event on all the reactors of a site.

The CSA enables EDF to confirm the current good safety level for all its nuclear reactors. It also leads EDF to propose supplementary measures, taking into account potential extreme situations on a deterministic basis. These analyses and modifications will reinforce defence in depth and continue to improve even more the safety of EDF's nuclear fleet.

However, the implementation of this program constitutes a challenge. It causes an important workload for EDF engineering teams, and also for EDF main suppliers, and care should also be brought to the impact of such an industrial program on the sites, with many evolutions of the operating documents (Tech. Spec., EOPs, SAMGs …).

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

[2] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), Safety of new NPP Designs, Report (2013).

STRENGTHENING DID IN EMERGENCY PREPAREDNESS AND RESPONSE BY PRE-ESTABLISHING TOOLS AND CRITERIA FOR THE EFFECTIVE PROTECTION OF THE PUBLIC DURING A SEVERE EMERGENCY AT A LIGHT WATER REACTOR OR ITS SPENT FUEL POOL

T. MCKENNA, P. VILAR WELTER, J. CALLEN, E. BUGLOVA
International Atomic Energy Agency (IAEA), Department of Nuclear Safety and Security,
Wagramer Strasse 5, P.O. Box 100, 1400 Vienna, Austria
Email: T.Mckenna@iaea.org

Abstract
Defence in depth can be divided into two parts: first, to prevent accidents and, second, if prevention fails, to limit their consequences and prevent any evolution to more serious conditions. This paper will cover the second part, by providing tools and criteria to be used during a severe emergency to limit the consequences to the public from a severe accident. Severe radiation-induced consequences among the public off-site are only possible if there is significant damage to fuel in the reactor core or spent fuel pools. Consequently, the tools and criteria have been specifically developed for individuals responsible for making and for acting on decisions to protect the public in the event of an emergency involving actual or projected severe damage to the fuel in the reactor core or spent fuel pool of a light water reactor (LWR). These tools and criteria, developed by the IAEA's Incident and Emergency Centre (IEC), will facilitate the implementation of the 'Emergency Response' defence in depth concept.

1. INTRODUCTION

A severe emergency at a nuclear power plant (NPP) that involves damage to fuel in the reactor core or in a spent fuel pool can cause deaths and severe health effects due to a radiation exposure, as well as have psychological, social and economic consequences affecting the public. To effectively prevent or mitigate those effects, specific protective actions and other response actions need to be implemented in some cases before or shortly after the beginning of a severe release of radioactive material to the environment.

Experience gained from past emergencies, including Three Mile Island (1979), Chernobyl (1986) and Fukushima (2011), have shown the importance of predetermined criteria and available tools to effectively protect the public during a severe reactor emergency. Decision makers during these emergencies were often unable to act promptly to implement protective actions and other response actions, because of: (a) the lack of predetermined criteria and available tools[1], (b) the lack of reliable information, (c) the lack of understanding of severe emergencies, their consequences and how to mitigate them, and (d) heightened emotions and mistrust of officials and of the scientific community [1, 2, 3].

In accordance with the defence in depth [4] objective 'to protect the public and the environment from harm in the event that these barriers[2] are not fully effective', the latest Emergency Preparedness and Response (EPR) series publication [5], outlines objectives in the event of a severe emergency at a LWR or its spent fuel pool, which are to:

- Prevent radiation-induced injuries and deaths by initiating urgent[3] protective actions for the public within 3 to 5 km, before a severe release, by acting promptly when conditions are detected in the plant that can lead to severe damage to the fuel;
- Keep the doses to the public below the international generic criteria [6] at which protective actions and other response actions are justified to reduce the risk of stochastic effects (radiation induced cancers); and

[1] That could not be established effectively ad hoc at the time of the emergency, due to the need to make decisions promptly.
[2] Fission product barriers.
[3] A protective action that, in the event of an emergency, needs to be taken promptly in order to be effective.

- Prevent or reduce psychological, economic and sociological effects, also known as 'non-radiological' effects [7], which are typically the most severe consequences of the emergency.

The tools and criteria that have been developed in order to achieve these objectives are as follows:

- An emergency classification system based on emergency action levels (EALs) for promptly (within minutes) triggering appropriate protective actions and other response actions off-site based on the status of the plant (e.g. status of the safety functions);
- Operational intervention levels (OILs) that can be used immediately and directly (without further assessment) to determine the appropriate protective actions or other response actions on the basis of environmental monitoring and sampling; and
- Radiological health hazard charts for placing measured quantities (e.g. μSv/h or Bq/kg) in perspective of the associated radiological health hazard. The charts were developed for communication with decision makers and the public to reduce the non-radiological consequences by answering the public's principle concern: 'Am I Safe?'

The underlying assumption of this paper, supported by research and experience [5, 8], is that following severe damage to the fuel in the core or spent fuel pool, severe releases can occur that warrant taking urgent protective actions promptly off-site. Severe releases may result in radiation-induced injuries and deaths within hours for those located within about 3 to 5 km of an NPP[4] if protective actions, such as evacuation and iodine thyroid blocking, are not taken before a release [5]. These injuries would be the result of exposure to the radioactive material in the plume (mainly by inhalation and external exposure), or from exposure to radioactive material deposited on the ground (mainly by inadvertent ingestion and external exposure). Further away from the NPP, within about 15 to 30 km, inhalation of the radioactive material in the plume could result in a detectable increase in the cancer incidence, and to be effective in preventing this detectable increase, protective actions may need to be taken before or shortly after a release. Past experience has demonstrated the effectiveness in protecting the public when taking actions based on conditions at the NPP [9], as taking this action has resulted in no radiation-induced health effects being detected amongst the public [10].

The failure of off-site decision makers to act promptly to initiate urgent protective actions (e.g. evacuation or taking an iodine thyroid blocking agent) on being notified by the operators at the plant of the detection of conditions that could lead to damage to the fuel, and thus before a release, could result in the occurrence of avoidable severe health effects due to a radiation exposure (i.e. injuries, deaths or a detectable increase in the cancer incidence).

2. EMERGENCY CLASSIFICATION SYSTEM

To allow prompt implementation of off-site protective actions upon the detection of damage to the core or spent fuel pool, a system needs to be in place so that those off-site will be informed when conditions at the NPP require the public to be protected. This system needs to include an emergency classification system so that those off-site understand the level of the hazard and the appropriate protective actions and other response actions to be taken. An emergency classification system is based on increasing levels of radiological hazard for those

[4] With power levels greater than about 100 MW(th).

on and off-site, and tied to the response needed for the protection of workers, helpers, the public and others.

An emergency is declared when an emergency action level (EAL) is exceeded. An EAL is a predetermined criterion that is observable by the control room operators, which if met, triggers the appropriate classification of the emergency and corresponding response actions. International requirements [6] and guidance [11] provide four classification levels in order of increasing levels of hazard: Alert, Facility Emergency, Site Area Emergency and General Emergency. The declaration of a General Emergency triggers immediate actions to protect the public off-site.

The control room operators can project fuel damage before it occurs, but cannot preclude or predict the timing or size of most severe releases warranting urgent protective actions off-site [5]. Therefore, a General Emergency is declared for events projected to result in severe damage to the fuel or for events that have resulted in such damage. Example events resulting in the declaration of a General Emergency are provided in Table 1.

To be effective, the classification system must include criteria (e.g. status of safety functions, water levels and trends, fuel temperatures, in-plant radiation levels) that can be observed and monitored by the control room staff. If the observable criteria are found to have been exceeded it will result in the classification of an emergency and thus triggering the appropriate protective actions and other response actions. These specific plant instrument readings, equipment status or other observables must be developed and integrated into the control room operating staff's procedures.

The basic system for developing EALs for the declaration of a General Emergency is illustrated in Figure 1. The goal is to project actual or significant fuel damage as soon as possible and not to wait for a release to the environment to implement protective actions off-site. EALs need to be developed in stages in order of the following: first, to detect a loss of auxiliary functions such as AC/DC power that will result in a loss of safety functions needed to protect the core or spent fuel; second, to detect the loss of a safety function needed to protect the core or spent fuel; third, to detect actual or imminent damage to fuel in the core or spent fuel pool; and finally, to detect a major release off-site by environmental monitoring. The latest research [12] indicates that, in most cases, there will not be a major release for several hours after detection of conditions that will lead to severe fuel damage. This will allow classifying the emergency several hours before a potential release and to implement off-site protective actions before the release occurs (as experience has shown [4]). Ref. [6] provides an example of a classification system for LWRs.

TABLE 1. EXAMPLE EVENTS RESULTING IN A GENERAL EMERGENCY CLASSIFICATION

Class	Example events resulting in this classification [5]

General Emergency	• Actual or projected severe[a] damage to the fuel in the reactor core or the spent fuel pool[b].
	• Loss of safety functions projected to result in severe damage to the fuel in the reactor core or spent fuel pool, including loss of the ability to perform the following safety functions:
	  o Shut the reactor down (establish reactor criticality control);
	  o Keep the core covered (cool the fuel pins);
	  o Remove decay heat from the reactor and the containment;
	  o Maintain vital auxiliaries (e.g. AC/DC power and control systems, and instrumentation).
	• Inability to control safety functions needed to protect the reactor core or spent fuel pool.
	• Detection of radiation levels off-site indicating actual severe damage to fuel (e.g. more than 100 μSv/h)

[a] Damage to fuel in the reactor core or spent fuel pool that can result in release warranting urgent protective action and other response actions off-site.

[b] Containing fuel requiring active cooling.

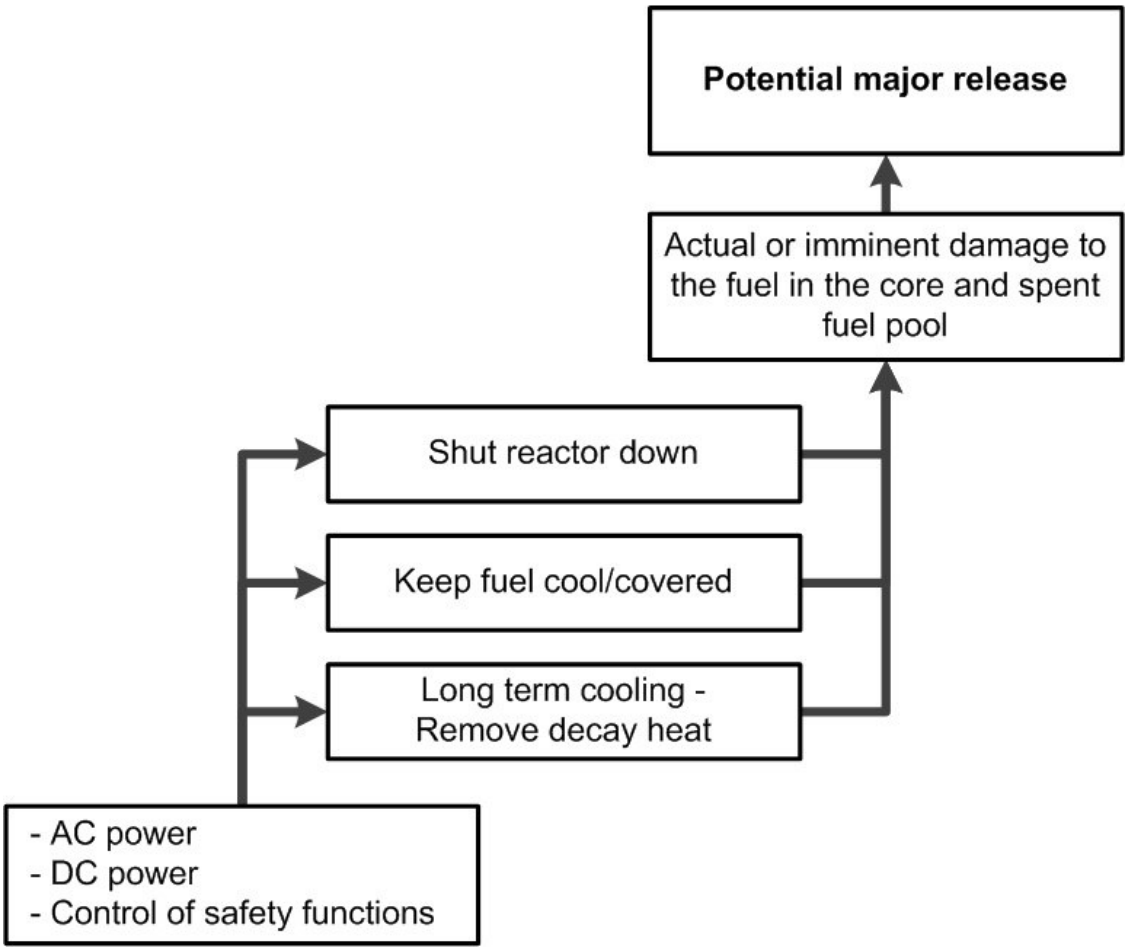

FIG.1. Structure for a system of EALs for the classification of a General Emergency.

3. OPERATIONAL INTERVENTION LEVELS (OILS)

Following a release of radioactive materials from the reactor core or spent fuel pool, additional decisions on protective actions and other response actions may need to be taken based on environmental monitoring and sampling. International guidance [6] has established generic criteria (GC), which are: (a) projected doses at which taking protective actions (e.g. evacuation, relocation, or food replacements) and other response actions (e.g. public reassurance) is justified[5], and (b) received doses at which taking medical actions to detect and effectively treat radiation induced health effects is justified[5]. However, GC cannot be used directly in an emergency, because they are in terms of dose and not in terms of quantities that are measurable in an emergency, such as dose rate. Therefore, predetermined default operational triggers, called operational intervention levels (OILs) have been developed for quantities that are measured by a field monitoring instrument or determined by laboratory analysis.

Predetermined default OILs are used to trigger particular protective actions and other response actions consistent with the GC. These OILs can be used immediately and directly (without further assessment) in an emergency to determine the appropriate protective actions

[5] Meaning that it does more good than harm in its broadest sense, including the consequences of any protective or other response actions.

and other response actions. OILs have been developed for LWR releases [13] for assessment of:

- Ground deposition based on the ambient gamma dose rate at 1 m above ground level;
- Radioactive material on the skin based on the gamma dose rate at 10 cm from the skin;
- Concentrations in food, milk, and water based on the activity of samples; and
- Presence of radioactive iodine in the thyroid based on the gamma dose rate above the thyroid.

The OIL values and the associated response actions to be taken if they are exceeded are provided in Ref. [5], along with a plain language explanation for use in describing how these OILs provide for protection of the public.

4. RADIOLOGICAL HEALTH HAZARD CHARTS

Experience from past nuclear and radiological emergencies shows that placing the radiological health hazard into perspective is required, to help answer the public's principal concern during an emergency ("Am I safe?") and help explain what protective actions and other response actions are warranted to prevent members of the public, those responsible for protecting the public (i.e. decision makers), and others (e.g. medical staff) from taking inappropriate and damaging actions that are not justified based on the radiological health hazard [3, 5, 14, 15, 16]. These actions were often taken by the individuals concerned in the belief that they are protecting themselves, their family members or the public, and were often the result of failure to answer "Am I safe?" To answer this question, what is considered to be 'safe' in an emergency must be defined and tools developed (i.e. charts) that relate quantities measured/ reported (e.g. dose rate) during an emergency to the radiological health hazard (i.e. is it safe or not). The definition of 'safe' has been developed and is available in Ref. [5].

For potential radioactive releases from a LWR core or its spent fuel pool, all the factors determining the possible radiological health hazard are understood and can be reasonably bounded. Consequently, calculations have been performed for severe releases resulting from emergencies at a LWR and its spent fuel pool that relate measured quantities to the possible radiological health hazard and the results presented in a set of charts, and provided in Ref. [5]. The charts have been developed to assess the radiological health hazard resulting from:

- Living in the affected area, based on the gamma dose rate at 1m above ground level.
- Having fission products on the skin, based on the gamma dose rate at 10 cm from skin.
- Consuming food, milk and water, based on the concentration of the marker radionuclides ^{131}I and ^{137}Cs in samples.

These charts can be used to directly relate a measured quantity to a radiological health hazard and will:

- Facilitate answering the public's principal concern during an emergency ("Am I safe?").
- Help the public, decision makers and others understand what protective actions and other response actions are appropriate/ inappropriate for ensuring the safety of everyone during the emergency.
- Help to identify those members of the public who might need a medical screening, examination or further assessment, in order to determine possible radiation induced health effects.

These tools were developed for the severe emergencies at NPPs and spent fuel pools of current designs. New reactor designs may warrant a significant revision of the overall emergency preparedness and response arrangements.

5. CONCLUSIONS

This paper provided information on the tools and criteria developed by the IAEA's Incident and Emergency Centre, which include an emergency classification system, EALs, OILs and radiological health hazard charts that can be used as a last defence barrier to ensure effective protection of the public in the event of a severe emergency at a LWR or its spent fuel pool. Application of these tools and criteria will support the defence in depth strategy to limit the potential consequences of an emergency.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, The International Chernobyl Project Technical Report, Vienna (1991).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Lessons Learned from the Response to Radiation Emergencies (1945-2010), EPR-Lessons Learned, Vienna (2012).

[3] GOVERNMENT OF JAPAN, Final report of the Investigation Committee on the Accident at the Fukushima Nuclear Power Stations of Tokyo Electric Power Company, Tokyo (2012).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, International Nuclear Safety Advisory Group, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Actions to Protect the Public in an Emergency due to Severe Conditions at a Light Water Reactor. Emergency Preparedness and Response Series EPR-NPP Public Protective Actions, IAEA, Vienna (2013).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[8] KIMURA M., TAKAHARA S., HOMMA T., Evaluation of the precautionary action zone using a probabilistic consequence analysis, Journal of Nuclear Science and Technology, 50:3, 296-303 (2013).

[9] NAIIC NATIONAL DIET OF JAPAN FUKUSHIMA NUCLEAR ACCIDENT INDEPENDENT INVESTIGATION COMMISSION, The official report of The Fukushima Nuclear Accident Independent Investigations Commission, The National Diet of Japan, Tokyo (2012).

[10] UNITED NATIONS SCIENTIFIC COMMITTEE ON THE EFFECTS OF ATOMIC RADIATION, Report of the United Nations Scientific Committee on the Effects of Atomic Radiation, Fifty-ninth session, (21-25 May 2012), General Assembly, Official Records, Sixty-seventh session, Supplement No. 46, A/67/46, United Nations, New York, (2012).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL LABOUR ORGANIZATION, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, Safety Standard Series No. GS-G-2.1, IAEA, Vienna (2007).

[12] US NUCLEAR REGULATORY COMMISSION, State-of-the-Art Reactor Consequence Analysis (SOARCA) Report, NUREG-1935, USNRC, Washington, DC (2012).

[13] MCKENNA T., KUTKOV V., VILAR WELTER P., DODD B., BUGLOVA E., Default Operational Intervention Levels (OILs) for Severe Nuclear Power Plant or Spent Fuel Pool Emergencies, Health Phys 104(5):459-470 (2013).

[14] TRICHOPOULOS D., ZAVITSANOS X., KOUTIS C., DROGARI P., PROUKAKIS C., PETRIDOU E, The victims of Chernobyl in Greece: induced abortions after the accident, British Medical Journal 295: 1100, (1987).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Goiânia, IAEA, Vienna (1988).

[16] VANO E., OHNO K., COUSINS C., NIWA O., BOICE J., Radiation risks and radiation protection training for healthcare professionals: ICRP and the Fukushima experience, J. Radiol. Prot. 31 (285) (2011).

CROSS-CUTTING ISSUES IN THE IMPLEMENTATION OF DEFENCE IN DEPTH (TOPICAL SESSION 4)

INVITED PRESENTATION

DEFENCE IN DEPTH: ASSESSMENT OF COMPREHENSIVENESS AND FURTHER STRENGTHENING OF THE CONCEPT

J. MISAK
Prague, Czech Republic
Email: Jozef.Misak@ujv.cz

Defence in depth concept based on multiple levels of protection of the workers, public and the environment against radiation harm is and should remain an essential strategy for ensuring safety of nuclear power plants. This strategy should be comprehensively implemented through all stages of the plant lifetime, from the siting through construction and operation up to decommissioning. First part of the presentation will introduce a screening method developed by the IAEA as a tool facilitating the assessment of the comprehensiveness of defence in depth and will indicate further possibilities for using and updating the approach by taking into account recent lessons learned.

Although it is clear that it is not possible for any industrial facility including nuclear power plants to fully eliminate the risk, further strengthening the defence in depth in particular at level 4 dealing with design extension conditions gives very high confidence in prevention and effective mitigation of severe accidents so that they are either practically eliminated or their consequences are limited in area and time. Second part of the presentation will discuss several issues associated with current efforts for strengthening the defence in depth, including the issues of practical elimination, independence and diversity of safety provisions at different levels of defence.

INVITED PRESENTATION

NEA'S PLANS FOR STRENGTHENING INTERNATIONAL IMPLEMENTATION OF THE APPLICATION OF DEFENCE IN DEPTH PHILOSOPHIES IN NUCLEAR POWER COUNTRIES

N. BLUNDELL
Nuclear Safety Division, OECD NEA,
Paris, France
Email: Neil.BLUNDELL@oecd.org

Following the Fukushima Daiichi Accident the OECD NEA established and delivered three tasks related to Defence in Depth for its member states. These consisted of:

- A review of member state and NEA activities directly related to the accident by the Fukushima Senior Task Group set up by the OECD NEA Committee for Nuclear Regulatory Activities (CNRA).
- An international expert review of the NEA's wide ranging joint nuclear safety research portfolio.
- A joint workshop on 'Challenges and Enhancements to Defence in Depth (DiD) in light of the Fukushima Daiichi Accident' on 5th June 2013 by both the OECD NEA Committee for Nuclear Regulatory Activities (CNRA) and Committee for the Safety of Nuclear Installations (CSNI).

These tasks encompassed firstly, how the NEA member states understand the concept of DiD and its value within Nuclear Safety. Secondly, how DiD is implemented at present, focussing on how it is implemented to deal with external events, and finally what future areas the NEA members considered NEA as a whole should be carrying forward to enhance the understanding and implementation of Defence-in-Depth.

Such areas included:

- Exploring what the DiD safety goal concept "practically eliminate large and early offsite releases" means and how is it implemented.
- Independence and margins in the implementation of DiD.
- Human interventions considering catastrophic external events effects on emergency response and recovery.
- Detailed identification of additional safety research after Fukushima.

This presentation provides a summary of those tasks and NEA's international programme of activities to bring its members together in those areas they highlighted to deliver enhancement in the understanding and implementation of defence in depth.

INVITED PRESENTATION

DEFENCE IN DEPTH - APPLIED TO THE NUCLEAR SYSTEM

M. WEIGHTMAN
United Kingdom
Email: mike_weightman@hotmail.com

Normally, the Defence in Depth concept is applied to the technical barriers that provide protection to the public and workers from nuclear accidents. This allows designers, operators and regulators to challenge (along with using other design principles such as independence, redundancy, diversity, single point failure, etc) the technical systems provided to see whether more needs to be done to provide adequate defence in depth to ensure risks are reduced so far as is reasonably practical.

Post Fukushima, much thought has gone into reconsidering whether the effectiveness of the defence in depth concept can be enhanced by, for example, rebalancing the attention between prevention and mitigation or enhancing the independence of protective measures such as providing extremely robust standalone emergency cooling capability. This presentation argues that Fukushima teaches us a more fundamental lesson - that the defence in depth concept (along with other design principles') should be applied to the nuclear system to see whether more should be done to enhance the institutional barriers in any particular nuclear system. These barriers are at three main levels: industry, regulators and stakeholders each with sub-barriers. It reinforces the need for industry and regulators to be independent, open and transparent so that the nuclear system can work effectively. Examples are given where the application of the model identifies areas for improvement in existing systems.

INVITED PRESENTATION

WANO ACTIONS TO REINFORCE THE OPERATORS' SAFETY CULTURE WORLDWIDE

J. REGALDO
WANO, London, United Kingdom
Email: jacques.regaldo@edf.fr

WANO's mission is to maximize the safety and reliability of nuclear power plants worldwide by working together to assess, to benchmark and improve performance through mutual support, exchange of information and emulation of best practices.

Fukushima accident strongly impacted the nuclear community and it also brought WANO to question its positioning and scope of activities. Five strategic actions have hence been decided to strengthen WANO's role, aiming to bring a more consistent, transparent and integrated response to the nuclear operators.

WANO peer review process, which constitutes its core-business, has been intensified including corporate and pre start up peer reviews and, for Japanese plants, restart reviews. WANO also decided to expand its scope of activity to include elements of design, based on the principle that the role of a nuclear operator is not only to operate safely, but also to be sure that the plant he is operating is safe.

WANO aims to cooperate strongly at both regional and international levels with all international safety organizations, being convinced that trust can be recovered with a strong safety commitment and credibility of both regulators and operators.

All operators, without exception, are WANO members; if membership is voluntary, members have to fulfil strict obligations. Safety supposes that no operator feels isolated, or refuses openness and permanent self-questioning; it requests as well for WANO to ensure that cultural and sometimes political barriers do not hinder safety culture – the accident of Fukushima is from this perspective rich in teachings.

In WANO, we believe that management system and practices are at the centre of safety culture, and a full involvement of top management (CEOs) of our members is absolutely requested. Through its commitments and rules, WANO pressures its members and help them reaching the highest possible standard of safety.

We consider that we rely on each other to improve safety!

INVITED PRESENTATION

IAEA ASSISTANCE IN HELPING MEMBER STATES DEVELOP EFFECTIVELY INDEPENDENT AND ROBUST REGULATORS FOR NUCLEAR INSTALLATION SAFETY

A. NICIC
International Atomic Energy Agency (IAEA), Department of Nuclear Safety and Security, Wagramer Strasse 5, P.O. Box 100, 1400 Vienna, Austria
Email: A.Nicic@iaea.org

The International Conference on Topical Issues in Nuclear Installation Safety will be focused on the exchange of information on the latest thinking and advances in the implementation of the concept of Defence-in-Depth (DID) in nuclear installations, and the associated challenges. The focus will be on operating nuclear installations, including nuclear power plants, research reactors and fuel cycle facilities, and on how lessons learned from operating experience and recent events (e.g. the Fukushima Daiichi accident) are used to enhance safety. The implementation of DID covers a number of elements that are directly related to the different states and phases of a nuclear facility.

This presentation will discuss the importance of the regulatory body in its oversight role as a cross-cutting element of DID in helping to assure the safety of nuclear installations. Taking note of the numerous challenges in developing an effectively independent and robust regulatory body, the presentation will describe how the IAEA assists Member States in their development of the appropriate regulatory infrastructure and necessary capacity to carry out their regulatory responsibilities – consistent with the IAEA Safety Standards.

The presentation will describe the importance of the self-assessment process which serves as a starting point for helping Member States gain an understanding of what support they need and when the support should be provided as they develop into a competent regulatory authority. The presentation will discuss recent improvements in the self-assessment process and related IAEA services in this regard.

Once regulatory bodies are established, it is essential that they seek continuous improvement. In this regard, the presentation will describe the IAEA's assistance provided through the Integrated Regulatory Review Service (IRRS) and recent activities to improve the IRRS, consistent with the IAEA's Action Plan on Nuclear Safety.

INVITED PRESENTATION

THE IAEA RESPONSE AND ASSISTANCE NETWORK (RANET) AND THE NEW NUCLEAR INSTALLATION ASSESSMENT AND ADVICE FUNCTIONAL AREA

P. KENNY, J. CHAPUT
International Atomic Energy Agency (IAEA), Department of Nuclear Safety and Security, Wagramer Strasse 5, P.O. Box 100, 1400 Vienna, Austria
Email: P.Kenny@iaea.org

The Incident and Emergency Centre (IEC) of the International Atomic Energy Agency (IAEA) is the global focal point for international preparedness and response to nuclear and radiological safety or security related incidents, emergencies, threats or events of media interest.

The Convention on Assistance in Case of a Nuclear Accident or Radiological Emergency (Assistance Convention) and the Convention on Early Notification of a Nuclear Accident (Early Notification Convention) are the prime legal instruments that establish an international framework to facilitate the exchange of information and the prompt provision of assistance in the event of a nuclear accident or radiological emergency. They place specific obligations on the Parties and the IAEA, with the aim of minimizing consequences for health, property and the environment.

Parties to the Assistance Convention have agreed to cooperate with each other and with the IAEA to facilitate prompt provision of assistance in case of a nuclear or radiological emergency, in order to mitigate its consequences. As part of the IAEA's strategy for supporting practical implementation of the Assistance Convention and in order to coordinate a global response, the IEC manages the IAEA's Response and Assistance Network (RANET). RANET aims to facilitate assistance in case of a nuclear or radiological incident or emergency in a timely and effective manner on a regional basis. States Parties shall, within the limits of their capabilities, identify and notify the Agency of experts, equipment and materials which could be made available for the provision of assistance and register these capabilities in RANET. These capabilities are registered in eight difference Functional Areas which are grouped by the type of assistance that could be provided.

Experience gained from past emergencies and based on feedback and direction clearly received from Member States under the IAEA Action Plan on Nuclear Safety resulted in the inclusion a new Functional Area for Nuclear Installation Assessment and Advice in EPR-RANET 2013. Under this functional area assistance may be provided to assess the nature of the event, the plant status, the possible evolution, and to provide advice to assist in the mitigation on-site. This area also covers the potential use of specialized equipment and technology, such as robotics and unmanned aerial vehicles that may be required to perform some on-site mitigation tasks in areas that may be uninhabitable by man (e.g. high dose rates, high temperatures and unstable environments).

This presentation describes RANET and explains the new Functional Area and the eight new capabilities: Nuclear power reactor design advice; Nuclear power reactor operations advice; Nuclear power reactor accident analysis; Research reactor assessment and advice; Fuel fabrication facility assessment and advice; Spent fuel storage assessment and advice; Spent fuel reprocessing assessment; and Operation of specialized technology.

TECHNICAL INSIGHT OF THE HIGH LEVEL SAFETY GOAL FOR THE NPPs BUILT IN CHINA'S THIRTEENTH FIVE-YEAR PERIOD (2016-2020)

G. SHI, W. ZHAN, Q. MEI, D. SUN
Shanghai Nuclear Engineering Research and Design Institute, SNPTC
Shanghai, CHINA
Email: shi@snerdi.com.cn

Abstract

The "Nuclear Safety Planning" has been published in Oct. 2012 in China, which stipulates the safety goals for the NPPs which will be built in the future. As for the NPPs which will be built in China's Thirteenth Five-Year (2016-2020) and later, the high level safety goal is described as "the possibility of the large radioactive release should be practically eliminated by design". A thorough investigation has been performed at SNERDI to explore the technical insights of this high level safety goal by using MEDP hierarchical safety goal approach. The definition of large release is proposed accordingly, DID requirements and probabilistic requirements are derived from this high level safety goal.

1. INTRODUCTION

In the mainland of China, the construction of the first nuclear power plant began in 1993. One year later, the National Nuclear Safety Administration (NNSA) was established, and a set of nuclear safety regulations, safety guides and criteria were published gradually, and updated accordingly. In this decade, due to increasing concerns about air quality, climate change and fossil fuel shortages, nuclear power has been looked into as an alternative to coal power. As of 2013, there are 17 nuclear power reactors spread out over 4 separate sites, and 28 nuclear power reactors are under construction.

During the development process of Nuclear Power Plants, the Chinese government has paid a great attention to nuclear safety. On March 16th, 2011, immediately after Fukushima nuclear accident, China's State Council decided to perform a comprehensive safety inspection of the operating NPPs and NPPs under construction, and suspend the construction permit issuance process for new NPPs. The compiling process of Nuclear Safety Planning was also pushed. After the safety inspection, the operating NPPs and NPPs under construction were required to implement backfits for prevention measures of external hazards and mitigation measures of severe accidents. In Oct. 2012, the State Council approved Nuclear Safety Planning [1], which stipulates the safety goals for the NPPs which will be built in the future. The high level safety goal for the Twelfth Five-Year (2010-2015) is described as follows: severe accident prevention and mitigation measures should be considered thoroughly in the design, and core damage frequency and large release frequency should be assessed to be lower than 1E-5/reactor-year, 1E-6/reactor-year respectively. As for the NPPs which will be built in China's Thirteenth Five-Year (2016-2020) and later, the high level safety goal is described as "the possibility of the large radioactive release should be practically eliminated by design".

How to explain the high level safety goal for Thirteenth Five-Year is the focus subject of the NNSA and nuclear industry in China. A thorough comparison and investigation has been performed at SNERDI, and then the technical insight of this safety goal was explored. In section 2, MDEP hierarchical safety goal approach was introduced, safety goals of nuclear organizations and several countries were described in section 3, and the technical insight of this safety goal was provided in section 4.

2. MDEP HIERARCHICAL SAFETY GOAL APPROACH

The Multinational Design Evaluation Project (MDEP) is a group of ten regulatory bodies from countries of North America, Europe and Asia, which have firm plans for new

nuclear programs. As part of their aim to get greater harmonization of regulatory requirements and practices, a group was tasked with considering how to harmonize Safety Goals. A report [2] has been produced and published, which set out a hierarchical approach, as provided in Figure 1. The hierarchy starts from a top level safety goal and a set of high level safety goals, that can be used to integrate the elements of safety desired to protect health and safety during normal operation and accident conditions for the whole plant life. The high level safety goals need to be developed in a coherent and consistent manner into lower level safety goals and targets that can be applied within the design and operation of reactors with a clear connection between the different levels. This structured approach is technology-neutral and is sufficiently flexible that it can be used for developing and applying safety targets for water-cooled and non-water cooled reactor designs.

3. SAFETY GOALS OF NUCLEAR ORGANIZATIONS AND SEVERAL COUNTRIES

3.1. Safety goals of IAEA

In 2006, the International Atomic Energy Agency (IAEA) published its revised Fundamental Safety Principles [3], which importantly states that "the fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation". The main current basis for the consideration of quantitative Safety Goals for NPPs is INSAG-12 which was published in 1999 [4]. The CDF for new NPPs should be lower than 1E-5/reactor-year and accident sequences that could lead to large early release could be practically eliminated. Many countries refer to this report as a basis for their national framework for quantitative Safety Goals. NS-G-1.10 [5] provides the detailed requirements for containment design considerations for severe accidents. For new plants, the consideration of severe accidents should be aimed at practically eliminating the certain conditions. And the definition for practical elimination was provided, as follows: "the possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high level of confidence to be extremely unlikely to arise."

3.2. Safety of New NPP Design proposed by WENRA

Compared to currently operating nuclear power plants, WENRA expects new NPPs to be designed, sited, constructed, commissioned and operated with the objectives covering the following areas [6]: O1) Normal operation, abnormal events and prevention of accidents; O2) Accidents without core melt; O3) Accidents with core melt; O4) Independence between all levels of defence-in-depth; O5) Safety and security interfaces; O6) Radiation protection and waste management; and O7) Management of safety. Safety objective "O3) Accidents with core melt" states that accidents with core melt which would lead to early or large releases have to be practically eliminated, for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public and that sufficient time is available to implement these measures.

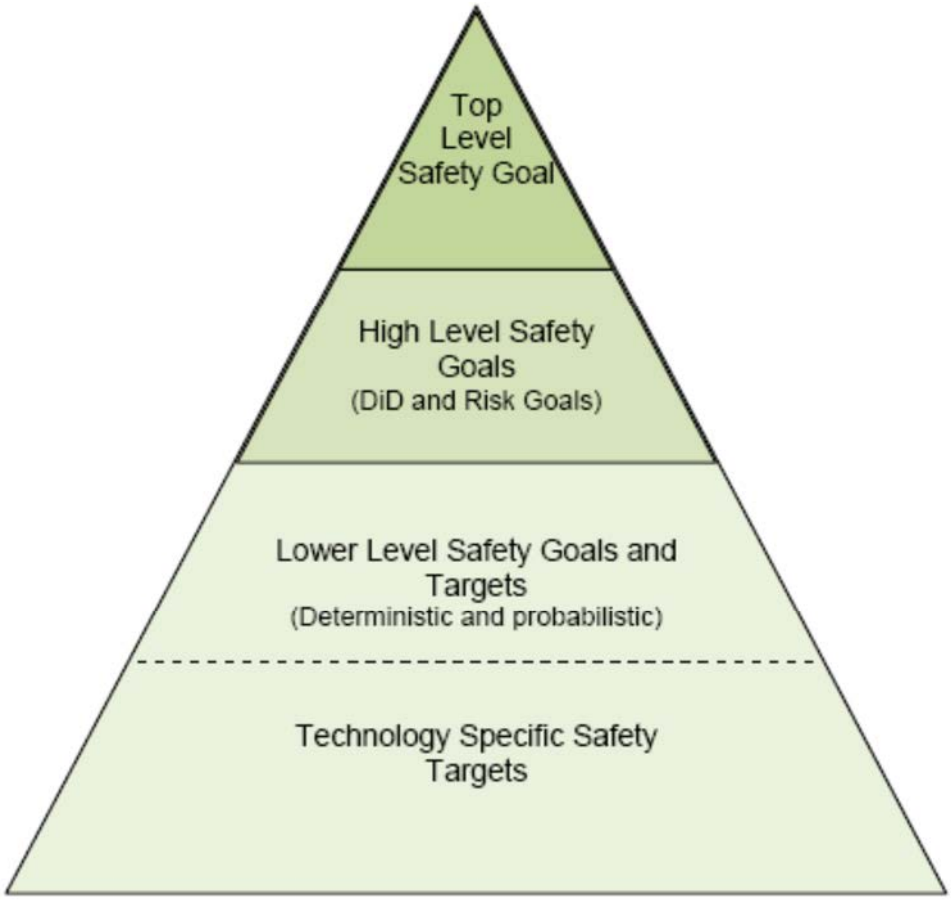

FIG.1.MDEP Hierarchy of Safety Goals.

3.3. Safety goals established by US NRC

In 1986, the US NRC issued a policy statement. The policy includes two qualitative goals which are supported by two quantitative health objectives (QHOs), in such a way that nuclear risks are not a significant addition to other societal risks. The US NRC adopted subsidiary quantitative objectives to act as surrogates for the QHOs that focus on designs. The surrogates are a core damage frequency (1E-4/reactor-year) and large release frequency (1E-5/reactor-year) for use in regulatory decisions on operating reactors. In the context of new reactors, the US NRC expects new reactor designs, such as AP1000 and ESBWR, should provide a higher level of safety comparing with the current operating plants in the US.

From lessons learnt from 9/11 event, US NRC issued 10 CFR 50.150 “Aircraft impact assessment” in 2009. Six months after Fukushima accident, the near-term task force (NTTF) published “Recommendations for enhancing reactor safety in the 21st century”. In April 2012, Commissioner George Apostolakis and his team published “A proposed risk management regulatory framework” [7]. As given in Figure 2, besides the adequate protection category, the team defined a number of the desirable characteristics for the design-enhancement category, and the remaining scenarios belongs to the residual risk category.

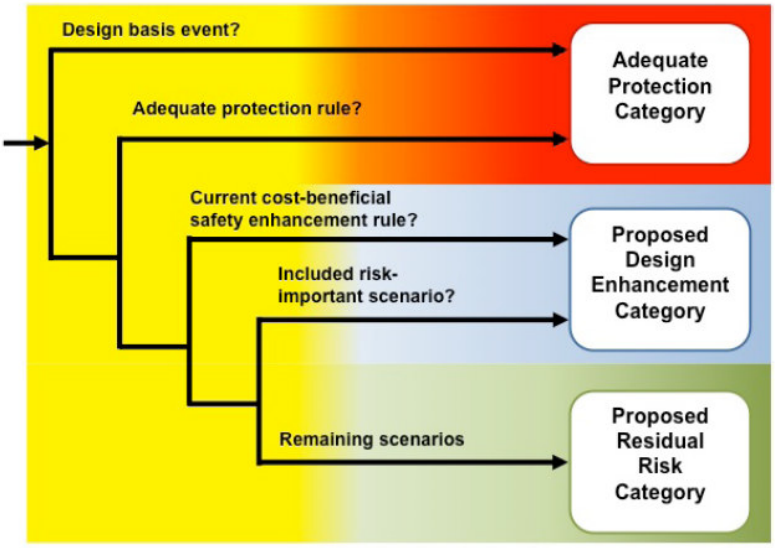

FIG. 2. Regulatory Framework for Nuclear Power Reactors.

3.4. Safety goals for design of EPR

In 2000, "Technical guidelines for design and construction of the next generation of NPPs with PWR" was published after the GPR/German experts' plenary meetings [8]. It states that accident situations with core melt which would lead to large early release have to be practically eliminated: if they cannot be considered as physically impossible, design provisions have to be taken to design them out. This objective applies notably to high pressure core melt sequences, accident sequences involving containment bypass, global hydrogen detonations, and etc. Low pressure core melt sequences have to be dealt with so that the associated maximum conceivable release would necessitate only very limited protective measures in area and time for the public. This would be expressed by no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, and no long term restrictions in consumption of food.

4. HIGH LEVEL SAFETY GOAL FOR THE NPPS BUILT IN CHINA'S THIRTEENTH FIVE-YEAR AND ITS TECHNICAL INSIGHT

4.1. High Level Safety Goal for the NPPs Built in China's Thirteenth Five-Year

In October 2012, Nuclear Safety Planning, approved by the State Council, stipulates the safety goal for the NPPs which will be built in Thirteenth Five-Year (2016-2020) and later as "the possibility of the large radioactive release should be practically eliminated by design". This is a high level safety goal, reflects the lessons learned from Fukushima accident, large radioactive release resulted in no immediately radiation effect on people but a large scale of people withdrawal is not acceptable, and this high level safety goal supports the top safety goal of protecting people and the environment from harmful effects of ionizing radiation. It was explained by Mr. Li Ganjie, Vice Minister of Environmental Protection and Administrator of the National Nuclear Safety Administration (NNSA), as follows: "the possibility of the large radioactive release should be practically eliminated by design, and effective confinement of radioactive materials even in the case of core melt accident should be ensured, consequently to protect people and the environment from unacceptable effects [9]."

4.2. Large radioactive release

As for large radioactive release, there are many definitions. For example, the release of 100TBq Cs-137 is defined as the limit of the large radioactive release in regard of the limited protective measures in area and time in Europe. As explained by NNSA administrator, the standpoint of the high level safety goal is to ensure the confinement of radioactive materials even in the case of core melt accident, therefore 5.0E14 Bq of I-131 equivalent, the low radioactive release limit of INES (International Nuclear Event Scale System) level 5, is proposed as the limit of large radioactive release. For the advanced NPPs with low containment leak rate, such as AP1000 and EPR, the radioactive release is below this quantitative value in the case of core melt accident with intact containment condition. In such case, the frequency of large radioactive release equals to the frequency of containment failure to confine the radioactive materials. Considering the radioactive release from spent fuel pool, the frequency of spent fuel melt should be added. Accordingly to calculation result, the release of 5.0E14 Bq of I-131 equivalent would result in whole body dose of less than 20mSv in one week at the boundary of site, therefore no emergency evacuation is required according to GB18871 [10]. It is also consistent with the requirement of SSR-2/1 [11]: plant event sequences that could result in high radiation doses or radioactive release must be practically eliminated, an essential objective is that the necessity for off-site intervention measures to mitigate radiological consequences be limited or even eliminated in technical terms.

4.3. Lower level safety goals corresponding to the high level safety goal

The high level safety goals need to be developed, in a coherent and consistent manner, into lower level safety goals and targets. The practical elimination of the large radioactive release should be supported by DID requirements and assessed using deterministic and probabilistic methods.

4.3.1. DID requirements

Application of the concept of DID in the design of a nuclear power plant provides several levels of defence aimed at preventing harmful effects of radiation on people and the environment, and ensuring adequate protection from harmful effects and mitigation of the consequences in the event that prevention fails. The independent effectiveness of each of the different levels of defence is an essential element of DID and this is achieved by incorporating measures to avoid the failure of one level of defence causing the failure of other levels. For the safety systems (DID level 3), which copes with design basis accidents, minimum redundancy (N-1) is required. Based on the overall safety goal and the frequency of the initiating events, the corresponding reliability of the mitigation systems could be estimated, and then additional redundancy or diversity could be considered. The mitigation measures（DID level 4）should be specifically designed for fulfilling the functions required in postulated core melt accident, and specific assessments should be performed to prove their effectiveness. EOP and SAMG should be available for accident prevention and mitigation. Additionally, Specific measures should be designed against external hazards and beyond design basis external hazards, for example, malevolent airplane impact and external flooding. EDMG shall be available to instruct the actions of operator in such cases.

The following situations should be practically eliminated: severe accident conditions that could damage the containment in an early phase as a result of direct containment heating, steam explosion or hydrogen detonation; severe accident conditions with containment bypass,

such as conditions relating to the rupture of a steam generator tube or an interfacing system LOCA; severe accident conditions with an open containment — notably in shutdown states; severe accident conditions that could damage the containment in a late phase as a result of base-mat melt-through or containment over-pressurization; total loss of core/containment cooling resulted from external hazards; spent fuel melt in spent fuel pool.

Specific accident mitigation measures shall be implemented besides the prevention measures. For example, the reliable depressurization measures should be installed to depressurize RCS even in case of the severe accident conditions, and no direct path is available for melt dispersion to the bulk of the containment, therefore severe accident conditions that could damage the containment in an early phase as a result of direct containment heating are considered as practically eliminated. As for practical elimination of the large release in late phase, the melt retention and the decay removal from the containment are the focus points. IVR or core catcher is the recommended engineering measure for the melt retention, the containment decay heat removal system independent of the systems used to prevent melting of the core, or passive containment heat removal system should be installed. The technical specific measures and target should be derived more, “Technical guidelines for design and construction of the next generation of NPPs with PWR” is a good reference; however, the design features of plants with passive safety system, such as AP1000 and ESBWR should be considered.

4.3.2. Probabilistic requirements

PSA differs from the deterministic method in that it provides a methodological approach to identify accident sequences that can follow from a broad range of initiating events and it includes the systematic and realistic determination of accident frequencies and consequences. This methodology, which has now reached a relatively mature level of sophistication, provides an integrated and systematic examination of safety aspects of design and operation, identification of weakness, and measures of overall risk, etc.

As mentioned above, large radioactive release results from containment failure to confine the radioactive materials in severe accidents and spent fuel melt, while, practical elimination means extremely unlikely to arise with a high level of confidence if it is not physically impossible. Therefore, LRF from the containment and LRF from the spent fuel pool should be extremely unlikely with a high level of confidence.

The probabilistic requirement of 1.0E-6/reactor-year or 5.0E-7/reactor-year is proposed as quantitative Safety Goals in several countries, which corresponds with the high level safety goal of practical elimination of large early release; as we know, late release is the main contributor to the failure of the containment. For the high level safety goal of practical elimination of large early release and late release, 1.0E-7/reactor-year (point estimated value, single unit) is proposed as PSA LRF target for the NPPs which will be built after the year of 2016. This reflects the extremely low residual risk, and 10 times lower than the probabilistic requirements for the NPPs which will be built in China's Twelfth Five-Year.

The quality and scope of the PSA are important issues. The PSA should be developed for level 1 and level 2 including all modes of operation, all relevant initiating events, including internal fire, internal flooding and all external hazards. PSA of spent fuel pool should be included. It is important to note that PSA shall be performed according to up-to-date proven methodology, and taking into account international experience currently available.

5. CONCLUSIONS

After the Fukushima nuclear accident, a comprehensive safety inspection of the operating NPPs and NPPs under construction has been performed. The State Council approved Nuclear Safety Planning in October 2012, which stipulates the safety goals for the NPPs which will be built in the future. As for the NPPs which will be built in China's Thirteenth Five-Year (2016-2020) and later, the high level safety goal is described as that “the possibility of the large radioactive release should be practically eliminated by design”. A thorough investigation has been performed at SNERDI to explore the technical insight of this high level safety goal by using MEDP hierarchical safety goal approach. The quantitative value of large radioactive release is proposed as 5.0E14 Bq of I-131 equivalent. DID requirements and probabilistic requirements are derived from this high level safety goal. As for DID, the independent effectiveness of each of the different levels of defence is an essential element of DID and this is achieved by incorporating measures to avoid the failure of one level of defence causing the failure of other levels. 1.0E-7/reactor-year (point estimated value, single unit) is proposed as PSA LRF target for the NPPs which will be built after the year of 2016. The technical specific measures and target shall be investigated and developed further. It shall be pointed that NNSA has the responsibility for explanation of Nuclear Safety Planning in China; we hope this paper provides useful information for NNSA to explain the policy or publish the corresponding safety guide.

REFERENCES

[1] 环境保护部（国家核安全局），核安全与放射性污染防治“十二五”规划及2020年远景目标，2012年.

[2] The Structure and Application of High-level Safety Goals, http://www.oecdnea.org /mdep/ publications/ MDEP-SAHLSG-Jan2011.pdf

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Basic Safety Principles for Nuclear Power Plants, INSAG-12, IAEA, Vienna (1999).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for NPPs, IAEA Safety Standards Series, Safety Guide No. NS-G-1.10, IAEA, Vienna (2004).

[6] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (WENRA), Safety of New NPP Design, March (2013).

[7] US NRC, A proposed risk management regulatory framework, April 2012.

[8] GPR, Technical guidelines for design and construction of the next generation of NPPs with PWR, 2000.

[9] 坚持科学发展 确保核与辐射安全, 核安全, 李干杰, 2012年12月.

[10] 中华人民共和国国家质量监督检验检疫总局，电离辐射防护与辐射源安全基本标准，GB 18871-2002，2002年10月.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

SOME LESSONS LEARNT FROM THE FUKUSHIMA DAIICHI ACCIDENT, AS REGARDS DEFENCE IN DEPTH AND ITS IMPLEMENTATION IN NEW OR EXISTING DESIGNS – AN INDUSTRY EXAMPLE

B. DE L'EPINOIS, F. BOUTEILLE, N. NICAISE
AREVA, Paris, France
Email: bertrand.delepinois@areva.com

Abstract

Defence-in-Depth (DiD) concept has been the overarching principle of the nuclear safety since the design of the first power reactors and it remains so more than ever. The Fukushima accident, characterised by a massive common mode failure induced by the flooding due to the tsunami, reminds the need for a very careful implementation, in the engineering, construction and operation of nuclear facilities, of the principles and rules concerning DiD. In particular, this accident highlights the need for appropriate consideration of DiD in two domains: protection against external hazards and severe accident management. In terms of external hazards, Fukushima reminds that the site design basis hazards must be as complete as possible and incorporate all relevant, including new, knowledge. In addition, in case nature would reveal to be more imaginative than us, or in case some hazards would have been under-evaluated despite all precautions, adequate extra margins should be ensured beyond the design basis hazards, as a defence in depth provision to avoid cliff edge effects. In other words, a minimal set of essential safety functions needed to prevent a severe accident or to mitigate its consequences should show sufficient robustness and safety margins to cope with external hazards exceeding the design basis hazards. Concerning severe accident, comprehensive R&D has been performed for several decades, the occurrence of such situations has been included in the DiD principles (level 4 as defined by INSAG 10) and has led to substantial safety improvements at many plants. Fukushima reminds the importance of a thorough implementation of these mitigation provisions. These two DiD provisions can be expressed as the need to show that the nuclear facilities and the crisis organizations can cope with extreme, beyond design hazards or accidents, precluding unacceptable offsite radiological impact and contamination. The development of Gen 3+ reactors targeted a significant safety step, by reducing both the severe accident probability and the consequences of a severe accident, should it occur. This paper therefore analyzes, in the light of Fukushima, the DiD approach followed in the design of the EPR and ATMEA reactors in terms of accident prevention, common mode failure prevention and mitigation, protection against natural hazards and severe accident management. Insight is given, from a designer point of view, on the topics on which the Fukushima lessons learnt are implemented. The paper also exposes to what extent and in which fields the approach followed for new reactors can be applied to operating nuclear power plants.

1. INTRODUCTION

On March 11, 2011, the Great East Earthquake and tsunami devastated the coast of Honshu, killing around 20 000 people. Villages and the regional infrastructure were destroyed. Power lines were broken and the means of communication severally damaged and wide areas turned into swamps. The whole region underwent an unprecedented overall devastation.

One major characteristic of the Fukushima accident is the massive common mode failure induced by the tsunami flooding: complete loss of AC power, DC power (immediate or progressive according to the reactors) and ultimate heat-sink. This led to the loss of decay heat removal at three NPP units, to severe reactor core damage, to the loss of containment integrity and to massive radioactive releases.

The level of devastation and isolation of the site and the multiple unit aggravating effects come out as new features in the accident knowledge and referential. In this extreme, unprecedented situation, the operators were left with almost no means of understanding what was happening and controlling the situation.

In terms of safety philosophy, the focus of regulatory systems has traditionally and legitimately been on radiation-related impacts on public health. The Fukushima Daiichi accident shows that the safety approach must also take into account the long term impact on the environment, in addition to the radiological effects on the health. Indeed, events that do not have extensive radiation-related health consequences can still generate considerable environmental impact and social disruption.

As set by the 2nd exceptional meeting of the Nuclear Safety Convention, in August 2012, an environmental objective deserves to be shared globally: "nuclear power plant should be designed, constructed and operated with the objective of preventing accidents and, should an accident occur, mitigating its effects and avoiding [large, long term] off-site contamination".

Not everything is yet known about the accident: data gathering and analysis remain needed and a continued effort of all involved parties must be pursued. It may take up to ten years. Meanwhile sufficient knowledge is already gathered to draw lessons learnt and implement the appropriate upgrades without further delay, as it is ongoing all over the world.

2. MAIN FUKUSHIMA LESSONS LEARNT IN TERMS OF DEFENCE IN DEPTH

2.1. Fukushima stresses the need to ensure sufficient robustness of the critical safety systems against external hazards significantly higher than the design basis hazards.

The Great East Japan Earthquake and the subsequent tsunami were, at the time of the accident, not covered by the design basis, although studies were on going in this field. The Fukushima accident reminds us that the site design basis hazard definition must be as complete as achievable, include adequate margins and be updated according to new knowledge.

In addition, as a defence in depth provision, in case that nature would reveal to be more imaginative than us or in case of some mistake in the hazard evaluation, extra margins and robustness should be ensured for the vital safety functions, in case of natural hazard significantly exceeding the design basis. The objective of these provisions and margins is, as far as reasonably practicable, to avoid cliff edge effects in order to prevent a severe accident and, should a severe accident occur, to avoid large and long term off site contamination. In other words, a minimal set of essential safety functions needed to prevent a severe accident or to mitigate its consequences should show sufficient robustness and safety margins to cope with natural hazards significantly more severe than the design basis hazards.

Assessing and ensuring robustness beyond the site hazard referential, in order to avoid cliff edge effects and catastrophic consequences, does not mean defining a new referential; the design basis hazards are to remain the referential. Beyond design natural hazards situations are dealt with best estimate analysis methodologies and safety criteria less conservative than those traditionally used for the design basis accidents.

Without delaying any of the above, international cooperation remains necessary to define guidelines as regards beyond design hazards. Those should in particular address the methodologies to assess the actual margins of the structures, systems and components in place at the existing facilities and the level of margin to be sought beyond the design basis.

2.1.1. Some insights on earthquakes

Several beyond design earthquakes struck nuclear power plants in the last years (Kashiwasaki Kariwa, Great East Japan and North Anna earthquakes). They showed an overall good resistance of the affected plants to the earthquakes.

This confirms that credit is not only due to the care put in the evaluation of the design basis events, but also as importantly to the quality of the design against seismic hazards and the associated margins taken in the various stages of the design, construction and operation. Priority is therefore to be maintained on the quality of the seismic design and construction, in order to ensure important margins above the safe shutdown earthquake (SSE).

2.1.2. Some considerations on flooding

As shown by the events in Le Blayais (1999) and Fort Calhoun (2012), flooding can be caused by a variety of phenomena which can occur in many places of the world. These are not all as outstanding as the major cataclysmic tsunamis which stroke Fukushima. The lessons learnt in the field of flooding are to receive a particular focus as flooding is the main cause of the Fukushima Daiichi accident and as it is among the main common cause failure potentialities.

Flooding ignores the concepts of independence between the levels of defence in depth, redundancy, diversity or safety classification: it aggresses without distinction every non protected systems, whatever their nature or their ranking in the defence in depth.

The dry site concept remains the overarching requirement: it must be demonstrated with high confidence and sufficient margins that the platform will endure no flooding should the highest water levels defined in the design basis requirement occur. In addition, as a defence in depth provision, unless it can be clearly excluded given the site location, it is our view that a potential flooding of the platform should be deterministically considered and that adequate water-tightness should be provided to the buildings protecting the vital safety functions.

2.2. The Fukushima Daiichi accident highlights the need for an effective implementation of severe accident mitigation in the defence in depth.

The matter that a severe accident can occur was not revealed by Fukushima; severe accident management is an important issue since the WASH 1400 report, TMI and Chernobyl, encompassing design, hardware, procedures, crisis organization and training. It is included in the international standards as the level 4 of defence in depth, as set by INSAG 10.

Containment has for long been recognized as the critical item in severe accidents, being the last barrier to prevent radioactive releases and to protect the people and the environment. Comprehensive R&D was performed and is continuing on the physics involved in severe accidents and means have been developed to mitigate radiological consequences, including hardware, procedures and training.

Hardware solutions to maintain containment integrity, as primary circuit depressurization, hydrogen risk mitigation and prevention of containment over-pressurization, were known to be available prior to Fukushima. The range of the practicable solutions obviously varies between what can be done on new reactors and what can be back-fitted on operating plants.

Fukushima reminds and strengthens the need to share and implement globally the objective of incorporating severe accident mitigation in the safety approach, in particular by implementing the recognized means to protect the containment integrity in the course of a severe accident.

The general objective to avoid, should a severe accident occur, large and long term offsite contaminations, as stated by the CNS, can be derived along the following lines, as in the IAEA SSR 2-1 and the WENRA safety objectives:

- Scenarios which would lead to early and large releases should be practically eliminated.
- For core melt accident not corresponding to the above, provisions are to be taken so that only limited protective measures, in area and time, may be needed for the public (no permanent relocation, no need for evacuation outside the immediate vicinity of the plant, no long term restrictions in food consumption) and sufficient time is available to implement these measures.

Without delaying any of the above, international cooperation remains necessary to further model some of the key physical phenomenon, to harmonize their safety appreciation, to formalize a common understanding of the "practical elimination" concept, to update and harmonize the industry best practices and to further standardize the regulatory approach.

2.3. Some complementary insights on safety systems

2.3.1. Vital functions

At Fukushima, the tsunami primarily impaired the electrical systems - generation and distribution, AC and DC - and deprived the operators of all means of control over the plant. Any non AC powered, non-water proof systems (e.g. turbine driven pumps, diesel driven systems, powered valves…) located in floodable areas would have endured the same fate; flooding can put out of use all equipment which is not water resistant.

Indeed, any power plant ultimately needs a minimal set of vital functions to prevent or mitigate severe accidents. They may vary according to the design: active, passive, AC powered, steam driven, DC controlled etc. Minimal Instrumentation and Control, residual heat removal means and containment integrity mastering equipment are among those, including their support systems.

A key lesson from Fukushima is to define adequately those functions, for each facility, and to protect them in such a way that their availability is ensured in extreme situations.

2.3.2. I&C

The most crucial point of the Fukushima Daiichi accident probably relates to the progressive loss of all instrumentation and control over the plant. The instrumentation and control means were ultimately powered by DC, the loss of which proved to be at the heart of the catastrophic evolution of the accident.

The extent and features of the vital Instrumentation and Control is to be defined with care, according to the exact characteristics of each design. It must be protected, hardened and supported in such a way to be available under all circumstances.

The nuclear industry appears in this field in the same situation as many of the other industries dealing with safety, the aviation industry being one of the other major examples.

In modern technologies, electricity (fiber optic data transmission being included in this category) represents the undisputed media to circulate information and orders. The wisest safety approach seems to recognize the ultimate need for some electrical generation and distribution in this field, and to implement the adequate provisions to prove its availability in all circumstances.

2.3.3. Heat sink

The ultimate heat sink generally includes a water intake and can be challenged in two ways by natural hazards, both having occurred in Fukushima: (1) the systems attached to the heat sink (e.g. pumping stations) can be impaired or (2) the water source can become unusable (e.g. the water can turn into mud, can be drawn apart, can be loaded with unmanageable amount of debris, ice, spilled oil, etc).

Indeed, the heat sink is both a system and a part of the environment. The protection of the system may not suffice in all cases of extreme natural situation, because it cannot prevent

a major change of the environment itself. Due consideration of an alternate heat sink hence seems an important feature in the defence in depth, as a lesson learnt from Fukushima

2.3.4. Spent fuel pool

The Fukushima Daiichi accident also highlighted the need for increased attention to spent fuel pools. As a severe degradation of the fuel stored in the pool would generally have unbearable consequences, one has to show practical elimination of such a scenario; the pool structural integrity, sufficient water-tightness and residual heat removal must be ensured in all cases.

3. GEN III REACTOR GENESIS AND SAFETY OBJECTIVES

3.1. Genesis

The safety objectives and main options of the EPR reactor, and more generally of what was later called the Gen 3 or Gen 3+, were set in the 1990s and early 2000s, which are a key period in the nuclear safety history and developments. This period was characterized by the lessons learnt from the Three Mile Island and Chernobyl accidents, the outcomes of probabilistic safety studies and the return of experience of 15 years of large nuclear fleets operation.

Three Mile Island had generated a deep evolution of the ideas in the field of human factor (I&C, control room ergonomy, accident management procedures, team organisation). Three Mile Island had also considerably accelerated the R&D concerning severe accident physics and their incorporation in the safety approach. Substantial ideas to improve reactor behaviour in case of severe accident had been identified in the following two decades. Significant modifications had been performed on the French operating fleet in these two domains.

The Chernobyl catastrophe had put forward that the consequences of large radioactive releases in the environment do not limit to the direct effect of ionizing radiations on health, but can also lead to a profound and wide psychological and social disruption.

The probabilistic safety studies as well as the return of experience had put forward means to significantly improve the prevention and reduce the core damage frequency. In addition, the probabilistic safety studies had put a specific emphasis on the shutdown states, the mastering of the boron dilution, the common cause failures potentialities as well as the relative weight of external hazards in the balance of the various accident causes.

The safety objectives and the main features of the EPR reactor takes full account of these major trends in the safety analysis and knowledge.

3.2. Safety objectives

The following high level safety objectives were set by the French and German safety authorities for the Gen 3 reactors:

- Reduce the core damage frequency by a factor 10, both by the reduction of the initiating event frequency and an improved availability of the safety systems.
- Limit the radiological consequences in case of an accident:
    - For the design basis accidents and more generally accidents without core melt, no protection measures should not be necessary for the neighbouring population.

- Practical elimination of severe accident sequences leading to large and early releases.
- In case of a core melt, only protection measures limited in time and space are acceptable.

- Simplify the operations:
  - Reduce the radiological doses (operation and maintenance), the normal releases and waste.
  - Optimize the in service inspection and the maintenance.
  - Prevent the human error risk.
- Reinforce the reactor against external hazards, including terrorist attacks and air plane crashes (this objective being particularly developed after the 9 /11event).

These safety objectives were progressively adopted globally, for example by the IAEA (SSR-2/1) or by WENRA. They set the standard for what is often called the Gen 3 or 3+ reactors. The major and new characteristic is the requirement to include severe accidents in the safety approach and to develop in the design a specific and extensive set of means devoted to their mitigation. This represents a major improvement in the defence in depth (level 4).

More generally, Gen 3 reactors are to include Design Extension Conditions in their design: common cause failure situations, severe accident. This step forward seems fully up to date and relevant after Fukushima.

4. GEN III CHARACTERISTICS AS REGARDS FUKUSHIMA LESSONS LEARNT

4.1. Robustness towards beyond design natural hazards

4.1.1. Earthquake

As regards earthquakes, the standard EPR is consistent with and a 0.3 g PGA DBE. This level of standard design covers most of the regions of the world. Specific adaptation would be performed for EPR projects arising on a site where the design basis earthquake should exceed this value.

The seismic approach is from the start significantly enhanced:

- The reactor, fuel and safeguard buildings are built on a common basemat, hence limiting their differential movements and subsequent mechanical constraints.
- All support systems are seismically classified.
- It is demonstrated that in case of earthquake no support system or not seismically classified system would jeopardize safety systems.

Margin assessments show, as expected when the state of the art seismic design rules are implemented, significant margins beyond the design spectrum. They indicate with a reasonable level of confidence that safety systems would remain operational after an earthquake of a level up to 0.5 or 0.6g.

4.1.2. Flooding

Protecting the reactor against external hazards, including malevolent actions, led to bunkerize the auxiliary buildings (safeguard buildings, main control room, diesel generator buildings, fuel pool building). The very strong, explosion proof, doors would resist the shock and water level of a tsunami.

Should an EPR have been placed in a Fukushima situation, these provisions would have, with a high level of confidence, provided the nuclear island buildings with leak-tightness appropriate to protect the diesels, electrical distribution, I&C and the safety systems.

As a lesson learnt from Fukushima, comprehensive verifications and some minor modifications are being performed in this domain, bringing to the standard EPR a generic waterproof feature to cope with a 4m flooding above the platform.

4.2. Severe accident mitigation

Severe accident mitigation constitutes an extra line of the defence in depth (level 4) of the EPR reactor. It is fully integrated in the design, from its inception, as part of the design extension conditions (DEC). A comprehensive safety demonstration is devoted to severe accidents, based on a deterministic approach complemented by probabilistic safety assessments (PSA), along the major objectives set by the safety authorities. In line with the DEC methodologies, the studies are based on realistic assumptions. They mobilize the data and modelling produced by the extensive international and national R&D over three decades, in a holistic and system wide approach.

EPR is designed according to very strong principles and objectives as regards the containment robustness. An outer shell provides protection against external hazards, including the crash of a large commercial aircraft. The pre-stressed, 1.8 m thick, wall of the containment can resist to pressures significantly higher than the previous generations of reactors. A stainless steel liner adds to its leak-tightness. Any residual leakage would be collected and filtered by the annulus ventilation.

4.2.1. Hydrogen risk management

- passive autocatalytic recombiners (qualified under severe accident conditions),
- appropriate design of the inner containment, which drives the H2 concentration,
- openings in the inner containment rooms, to avoid local H2 concentration,
- a comprehensive modelling of the severe accident sequences to show that, at no point in the course of the accident, H2 concentration would reach detonation thresholds, and
- the containment resistance to H2 deflagration.

4.2.2. Steam explosion risk management

- it is shown that corium / coolant interaction inside the vessel would not jeopardize the containment,
- the corium melt through the vessel is deterministically postulated, given all uncertainties and doubts concerning the possibility to demonstrate in all cases in vessel retention for large reactors, and
- as R&D does not rule out the possibility of large, very powerful steam explosions which could result from a corium pouring in a flooded vessel cavity, the vessel cavity is designed to remain free of water in accident conditions (dry pit).

4.2.3. Direct containment heating (DCH) risk management

Two sets of pressurizer discharge valves prevent the core melt under pressure: two discharge valves are dedicated to the severe accident conditions, in addition to the pressure

relief valves. They are supplied from a different technology and they can be triggered by a dedicated alternate I&C.

As in the operating French fleet, very clear criteria define entering into the SAMG, the first action of which consist in opening the discharge valves to avoid high pressure core melt.

4.2.4. Residual heat removal from the containment

The EPR safety objective requires (1) to ensure residual heat removal from containment without any need to vent the containment, and (2) to fulfil this function through dedicated systems. Hence, a specific line of systems is dedicated to spraying, recirculating and cooling water into and from the containment under severe accident conditions.

These systems can be powered by the SBO diesels and controlled by the severe accident I&C. They are qualified under severe accident conditions. In addition, the reactor building robustness ensures passive containment robustness up to 3 days in the absence of residual heat removal. This ultimate period of grace further reinforces the Defence in Depth concerning severe accidents, allowing recovery action.

Post Fukushima, mobile equipment and connections are being implemented to provide the crisis organisation with means of recovery and appropriate resilience (level 5 of DiD).

4.2.5. Corium concrete interaction

Corium concrete interaction is prevented through a core catcher, the opening and the cooling of which are triggered by the progression of the corium, without any I&C intervention.

These examples intend to show that the mitigation of severe accident is to be, from a safety philosophy point of view, and can be, from a technical point of view, included in the design. It deserves a comprehensive approach, in which the core, the NSSS and the containment form a system to be designed and modelled as such. It requires mobilization of the full scientific knowledge as regards severe accident physics. The stakes associated with the safety objectives set by WENRA and the IAEA deserve a deterministic safety demonstration.

4.3. Some complementary insights on EPR DiD and Fukushima lessons learnt

It is not the purpose of this paper to address the features implemented in the field of prevention of incidents or accidents of the design basis, even caused by internal or external hazards, neither to develop the mitigation means to cope with design basis accidents.

Based on an evolutionary design, drawing the lessons from the operational fleet, probabilistic safety studies and progress of the technology, the EPR design achieves a very significant step in these fields. In addition to severe accident (DEC-B) addressed supra, a great care is also brought, still in the design extension conditions, on common mode failures (DEC-A). For DBC 2 and “frequent” DBC 3 events, it is demonstrated that the loss of all redundant trains of a safety function does not lead to core damage.

4.3.1. Power supply

In case of loss of offsite power, four emergency diesel generators power each of the four 100%, physically separated, safety trains. They are located in two distinct bunkerized buildings.

Two diversified station black-out diesels can each power the vital safety functions (emergency feedwater, safety injection, severe accident decay heat removal from containment, spent fuel pool cooling, I&C, control room survivability). Two sets of 12 H batteries ultimately power the severe accident dedicated I&C, the containment valves and the control room lighting and air control.

4.3.2. Heat sink

The safety system access to the ultimate heat sink is particularly robust. The cooling circuit between the main water intake and the reactor are redundant. An alternate heat sink and a diversified cooling circuit can support the ultimate safety function. In addition, the reactor is provided with important water reserves in case of total loss of ultimate heatsink (IRWST, four emergency feedwater tanks, large water reserve to refill the latter). They are earthquake resistant and safety classified. The EPR reactor is therefore granted a residual heat removal capacity over one week in case of total loss of ultimate heat sinks (initial state : power or closed primary circuit).

4.3.3. Spent fuel pool

The spent fuel pool is characterized by its robustness towards external or internal hazards, including severe earthquakes and large commercial aircraft crashes. These features ensure a great confidence in the pool structural integrity under severe situations and hazards.

Several lines of defence in depth ensure the cooling:

- two redundant safety classified cooling trains,
- a diversified cooling chain, powered by the SBO diesels and cooled by the alternate heat sink,
- several means to ensure water make-up in the pool, supplied by large water reserves, allow to ultimately cool the pool by evaporation.

After Fukushima, to further strengthen the Defence in Depth, mobile water-make up and the corresponding connection points are being implemented, as well as a steam exhaust opening.

4.3.4. I&C

The EPR I&C benefits from:

- the overall protection of the buildings and power supply from external and internal hazards,
- very firm design rules concerning redundancy and physical separation between the trains,
- dedicated battery power supply (2H batteries, 12H severe accident batteries),
- a hardened core of redundant I&C developed in a diversified technology,
- a severe accident dedicated I&C,
- a remote panel in case of main control room evacuation or unavailability.

4.3.5. Post Fukushima enhancements

In addition to the enhancement of water-tightness (cf supra), a comprehensive set of connecting points is being implemented. The role of these connecting points is to allow mobile means to supply power to the vital systems, to supply water to the emergency feed-water, to the primary circuit or to the spent fuel pool, and to spray water in the containment (pressure control).

Longer autonomy towards offsite supplies (eg fuel for the diesel generators) will also be provided. These two sets of modifications are dedicated to support the Emergency Response in extreme situations. They belong to the level 5 of DiD.

5. CONCLUSIONS

After Fukushima, the standards defined for the new generation of reactors, for example the technical guidelines published by the French and German safety authorities for the EPR, the IAEA SSR 2-1 and the WENRA safety objectives, appear to be robust and valid. Appropriate updating is being performed where need be.

Fukushima raises the objectives and standards concerning protection of the vital safety systems towards natural hazards significantly exceeding the design basis referential. It seems to be the main new lesson learnt in terms of safety approach in the field of design.

The accident reminds the importance of the Defence in Depth provision concerning severe accident mitigation (level 4 of DiD). Avoiding large and long term offsite contaminations, even in extreme situations, is a major objective to be shared globally, in addition to the objective of protecting health. It also stresses the importance of certain systems as I&C and spent fuel pools, as well as some specific considerations concerning the ultimate heat sink.

Human factors, organisation and crisis management constitute a field of major importance in the post Fukushima evolutions. Although this field is not addressed in this paper dedicated to design, some of the main post Fukushima hardware considerations, as the I&C robustness, the control room survivability, the interest for on site hardened crisis centres, the mobile means and connection points, are devoted to support the implementation of the lessons learnt in these essential fields.

As an example and a safety pioneer among the Gen 3+ reactors, the EPR underwent comprehensive safety assessments in the countries where projects are developed, which show a good robustness and behaviour of the reactor in extreme, Fukushima like situations.

Upgrades are nevertheless being implemented to the EPR in the aftermath of Fukushima, mainly to further complement its water tightness, to increase its autonomy towards offsite supplies (e.g. diesel fuel) and to put in place mobile means and their connecting points.

In addition to these considerations concerning new reactors, global acknowledgement is growing that a plant in operation will benefit from gradual upgrades during its lifetime. Periodic safety assessment are viewed as a good practice in this field, as they allow a comprehensive benchmark of a facility with its design referential (compliance), with the newer technical knowledge (e.g. natural hazards) and with the evolution of the safety approach (standards for new facilities).

In particular, many of the technical solutions to protect the containment in case of severe accident can be backfitted on operating plants.

In the same manner, a lot of initiatives aim to increase the protection of operating reactors against natural hazards, in particular flooding, to install additional fixed and bunkered safety systems or power supplies where need be, physically separated, diverse and well protected, to provide plants with alternate heat sinks or water reserves, to implement mobile means and corresponding connection points, to complement and strengthen the I&C etc.

Indeed, much has been done to upgrade plants since their commissioning. Much is being done and can be done to implement the Fukushima lessons learnt in operating plants and, more generally, to take into account the new reactor standards, in an ALARA and risk informed spirit.

WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION (WENRA) VIEWS ON DEFENCE-IN-DEPTH FOR NEW REACTORS

L. REIMAN*, T. ROUTAMO*, F. FÉRON**
* STUK,
Helsinki, Finland
** ASN, France
E-mail: lasse.reiman@stuk.fi

Abstract
WENRA published in 2010 a statement on safety objectives for new NPPs. Based on these objectives, WENRA decided to develop common positions, compiled in a booklet (available on www.wenra.org), on selected key safety issues for the design of new NPPs. One position presents WENRA's Defence-in-Depth approach, describing WENRA's expectation that multiple failure events and core melt accidents are considered in the original design of new nuclear power plants; another position presents expectations on the independence between different levels of Defence-in-Depth.

1. WENRA SAFETY OBJECTIVES FOR NEW NPPS

One of the objectives of the Western European Nuclear Regulators' Association (WENRA), as stated in its terms of reference, is to develop a harmonized approach to nuclear safety and radiation protection and their regulation. For NPPs, WENRA established a permanent working group: the Reactor Harmonization Working Group (RHWG) which reports to WENRA.

A significant contribution to this objective was the publication, in 2006, of a report on harmonization of reactor safety in WENRA countries. This report addresses the nuclear power plants (NPPs) that were in operation at that time in those countries; it includes about 300 "Reference Levels". These Reference Levels were last updated in January 2008. WENRA is at the moment revising and amending these Reference Levels based on the lessons learned from the TEPCO Fukushima accident.

Since the introduction of WENRA Reference Levels, the construction of new nuclear power plants has begun or is being envisaged in some European countries. Hence, it was considered timely for WENRA to develop the safety objectives for new nuclear power plants. The RHWG report "Safety objectives for new power reactors – study by RHWG – December 2009" was published as an interim step before WENRA issued the "WENRA statement on safety objectives for new nuclear power plants – November 2010" (www.wenra.org). The WENRA statement includes seven safety objectives, which were developed on the basis of a systematic review of the IAEA SF-1 Fundamental Safety Principles (2006) and are the basis for further harmonization work of WENRA. Based on these safety objectives, WENRA decided to develop common positions on selected key safety issues for the design of new nuclear power plants.

The seven WENRA safety objectives call for an extension of the safety demonstration for new plants, consistent with reinforcement of Defence-in-Depth (DiD). The scope of this demonstration has to cover all risks induced by the nuclear fuel, whether in the core or in storage, as well as the risks induced by other relevant radioactive materials.

The safety objectives address new civil nuclear power plant projects. However, these objectives should also be used as a reference to help identifying reasonably practicable safety improvements for "deferred plants" and existing plants during Periodic Safety Reviews.

The safety objectives are formulated in a qualitative manner to drive design enhancements for new plants with the aim of obtaining a higher safety level than that

expected from existing plants. WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated in line with these safety objectives.

2. WENRA REPORT ON KEY SAFETY ISSUES FOR THE DESIGN OF NEW NPPS

Based on these safety objectives, WENRA decided to develop common positions, compiled in a booklet, on selected key safety issues for the design of new NPPs. The work was initiated and also a major part of the work was carried out before the TEPCO Fukushima Daiichi accident. Therefore, the report discusses also some considerations based on the major lessons from the Fukushima Daiichi accident, especially concerning the design of new nuclear power plants, and how they are covered in the new reactor safety objectives and the common positions.

Among these common positions:

1) one (position 1) presents WENRA's Defence-in-Depth approach, describing WENRA's expectation that multiple failure events and core melt accidents should be considered in the design of new nuclear power plants; and
2) another (position 2) presents the expectations on the independence between different levels of Defence-in-Depth.

Other positions address multiple failure events to be considered in the design (position 3), design provisions to mitigate core melt accidents (position 4), the implementation of the concept of practical elimination (position 5), protection against external hazards (position 6) and intentional crash of a commercial airplane (position 7).

3. DEFENCE-IN-DEPTH FOR NEW REACTORS

The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents is the application of the concept of Defence-in-Depth. This concept should be applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions, so that if a failure were to occur, it would compensated for or corrected by appropriate measures.

Therefore, Defence-in-Depth is a key concept of the safety objectives established by WENRA for new nuclear power plants. The DiD concept should be strengthened in all its relevant principles. In addition to the reinforcement of each level of the DiD concept and the improvement of the independence between the levels of DiD (as stated in the WENRA safety objectives), this also means that the principle of multiple and independent barriers should be applied for each significant source of radioactive material. It shall also be ensured that the DiD capabilities intended in the design are reflected in the as-built and as-operated plant and are maintained throughout the plant life time.

The concept of Defence-in-Depth in the early stage included three levels only (prevention of abnormal operation and failures, control of abnormal operation and detection of failures, control of accident within the design basis). Then, the concept for the current operating reactors was further developed to take into account severe plant conditions that were not explicitly addressed in the original design (hence called "beyond design conditions"), in particular lessons learned from the development of probabilistic safety assessment and from the Three Mile Island accident (USA 1979) and from the Chernobyl accident (Ukrainian Republic of USSR 1986), which both resulted in a core melt accident. These developments led to two additional levels in DiD (INSAG 10 – 1996).

For new reactor designs, there is a clear expectation to address in the original design what was often "beyond design" for the previous generation of reactors, such as multiple

failure events and core melt accidents, called Design Extension Conditions in IAEA SSR-2/1. This is a major evolution in the range of situations considered in the initial design of the plant.

In the WENRA approach, the single initiating events and multiple failure events are two complementary approaches that share the same objective: controlling accidents to prevent their escalation to core melt conditions. It was therefore preferred to treat the multiple failure events as part of the 3rd level of DiD, but with a clear distinction between means and conditions (sub-levels 3.a and 3.b).

As the phenomena involved in accidents with core/fuel melt (severe accidents) differ radically from those which do not involve a core melt, core melt accidents should be treated on a specific level of DiD. In addition, for new reactors, design features that aim at preventing a core melt condition and that are credited in the safety demonstration should not belong to the same level of defence as the design features that aim at controlling a core melt accident that was not prevented.

Furthermore, in each level of DiD, some situations need to be practically eliminated as it cannot be demonstrated that, should they occur, their radiological consequences would be tolerable. Situations that could lead to early or large releases of radioactive materials have to be practically eliminated.

The refined structure of the levels of DiD proposed by WENRA is therefore bringing change to level 3 and 4 of the "usual" DiD table, as shown in Table 1.

4. INDEPENDENCE BETWEEN DIFFERENT LEVELS OF DEFENCE-IN-DEPTH

4.1. Basic safety expectations on the independence between different levels of Defence-in-Depth

According to the 2010 WENRA "Statement on safety objectives for new nuclear power plants" WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated with the objective, among others, of "*enhancing the effectiveness of the independence between all levels of defence-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately…), to provide as far as reasonably achievable, an overall reinforcement of defence-in-depth*." (Objective O4: "Independence between all levels of defence-in-depth").

TABLE 1. STRUCTURE OF DID LEVELES 3 and 4 AS PROPOSED BY WENRA

Levels of DiD		Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 3	3.a	Control of accident to limit radiological releases and prevent escalation to core melt conditions	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact	Postulated single initiating events
	3.b		Additional safety features, accident procedures		Postulated multiple failure events
Level 4		Control of accidents with core melt to limit off-site releases	Complementary safety features to mitigate core melt, management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)

The basic safety expectations of WENRA on the independence between different levels of DiD are as follows:

1) There shall be independence to the extent reasonably practicable between different levels of DiD so that failure of one level of DiD does not impair other levels of DiD involved in the protection against or mitigation of the event.

   "Reasonably practicable" should be taken to mean that, in addition to meeting the normal requirements of good practice in engineering, further safety or risk reduction measures for the design or operation of the facility should be sought and that these measures should be implemented unless the utility is able to demonstrate that the efforts to implement the proposed measures are grossly disproportionate to the safety benefit they would confer.

2) The adequacy of the achieved independence shall be justified by an appropriate combination of deterministic and probabilistic safety analysis and engineering judgement.

   For each postulated initiating event (starting with DiD level 2), the necessary SSCs should be identified and it shall be shown in the safety analysis that the SSCs credited in one level of DiD are adequately independent of SSCs credited in the other levels of DiD.

3) Appropriate attention shall be paid to the design of I&C, the reactor auxiliary and support systems (e. g. electrical power supply, cooling systems) and other potential cross cutting systems. The design of these systems shall be such as not to unduly compromise the independence of the SSCs they actuate, support or interact with.

Means to achieve independence between SSCs are adequate application of:

- physical separation, structural or by distance;
- functional isolation;
- diversity.

4.2. Implementation of the basic safety expectations

In applying the above basic expectations, the following considerations shall be taken into account:

1) SSCs fulfilling safety functions in case of postulated single initiating events (DiD level 3.a) or in postulated multiple failure events (DiD level 3.b) should be independent to the extent reasonably practicable from SSCs used in normal operation (level 1) and/or in anticipated operational occurrences (level 2).
2) SSCs fulfilling safety functions used in case of postulated single initiating events (DiD level 3.a) should be independent to the extent reasonably practicable from additional safety features used in case of postulated multiple failure events (DiD level 3.b).
3) Complementary safety features specifically designed for fulfilling safety functions required in postulated core melt accidents (DiD level 4) should be independent to the extent reasonably practicable from the SSCs of the other levels of DiD.

4.3. Specific considerations

4.3.1. Emergency AC power supply

The emergency AC power supply belonging to DiD level 3.a may be used also in DiD level 2. An additional diverse emergency AC power supply shall be designed for DiD level 3.b because the common cause failure of the primary (non-diverse) emergency AC power sources is postulated. The emergency power supply on DiD Level 3.b may be also used for DiD level 4.

4.3.2. Separation of cables

Since principles of separation of cables already exist between the divisions of redundant systems and between safety and non-safety systems, it may not be reasonably practicable to introduce additional separation on the basis of levels of defence.

4.3.3. Reactor protection system and other I&C aspects

The reactor protection system (RPS) shall be adequately independent from other I&C systems and must be functionally isolated from them. The RPS may have I&C functions on other DiD levels than 3, e.g. the scram system may be actuated by the RPS for specific DiD level 2 events. Diverse I&C means shall be designed for DiD level 3.b in case the common cause failure of the RPS has to be postulated.

Limitation and control systems (not the RPS) for the actuation of systems needed to handle level 2 events may be combined with I&C for normal operation.

4.3.4. Containment

On each level of defence there is a need for confinement as a safety function. This safety function may be accomplished for example by the use of the containment in combination with other SSCs. The containment is thus an example of a structure which is used on different levels of defence and for which it would not be reasonably practicable to require independence for different levels of Defence-in-Depth.

SAFETY CULTURE AS A PILLAR OF DEFENSE-IN-DEPTH IMPLEMENTATION AT THE EXPERIMENTAL FUEL ELEMENT INSTALLATION, BATAN INDONESIA

H. HARDIYANTI, B. HERUTOMO, G. K. SURYAMAN
Center for Nuclear Fuel Technology – National Nuclear Energy Agency (BATAN)
Tangerang, Indonesia
E-mail: hrdyanti@batan.go.id

Abstract

Defence-in-depth (DID) needs to be implemented not only in a nuclear power plant, but also in a non-reactor nuclear facility. The application of safety culture in a nuclear facility is one way of DID implementation. Safety culture aims at the performance of safe works, the prevention of deviation, and the accomplishment of quality operation. It is in accordance with the first level of DID concept which is the prevention of abnormal operation and failures that is done through conservative design and high quality in construction and operation. Experimental Fuel Element Installation (EFEI) is a non-reactor nuclear facility that belongs to BATAN (the National Nuclear Energy Agency of the Republic of Indonesia) that functions as its research and development facility on power reactor fuel production. The objective of safety culture implementation in the EFEI is to encourage workers to have a stronger sense of responsibility on safety and to contribute actively for its development. The enhancement of safety culture in the EFEI refers to the attributes of a strong safety culture listed in the IAEA Safety Standard Series No.GS-G-3.5 (The Management System for Nuclear Installations Safety Guide). The strategies performed were: a) Internalization of safety values through activities such as briefings, "coffee morning", visual management, workshops, and training; b) Enhancement of leadership effectiveness through activities such as senior management visits, safety leadership training, and personnel qualification training; c) Integration of safety into all work processes through activities such as setting up HIRADC (hazard identification, risk assessment, and determining controls) documents, setting up WHA (workplace hazard assessment), and routine housekeeping; d) Learning about safety through activities such as occupational health and safety inspections, safety self-assessments, open reporting on safety incidents, and participation in the FINAS (fuel incident notification and analysis system); e) Enhancement of safety performance accountability through activities such as ensuring open and timely reporting to the regulatory agency, evaluation of the SPI (safety performance indicators), and defining clear roles and responsibilities for each worker.

1. INTRODUCTION

1.1. Defence in Depth

Defence in Depth in Nuclear Safety is the implementation of several levels of equipment and procedures to ensure the effectiveness of physical barriers which limit the interaction between radioactive materials with workers, public and environment. The physical barriers are intended to protect the workers, public and environment in normal operation condition, anticipated operational occurrences, and accident conditions. Defence in Depth concept is implemented through design and operation of the installation. This concept is very important for nuclear installations. As was stated in the Basic Safety Principles for Nuclear Power Plants (INSAG-10) in relation to the safety of nuclear power plants, "*All safety activities, whether organizational, behavioural or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defence in depth...*" [1].

The main object of the defence in depth concept is the levels of protection barrier. Those barriers include the barrier whose main function is to prevent radioactive releases to the environment. The objectives of defence in depth concept are as follows:

1) To compensate for potential human and component failures.
2) To maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves.
3) To protect the public and the environment from harm in the event that these barriers are not fully effective.

The defence in depth concept is explained in Basic Principles for Nuclear Power Plants (INSAG-3) [1].

The strategy for defence in depth is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions.

Defence in depth is generally structured in five levels. Should one level fail, the subsequent level comes into play. The objective of the first level of protection is the prevention of abnormal operation and system failures.

If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response [1].

The safety provisions at Level 1 are taken through the choice of site, design, manufacturing, construction, commissioning, operating and maintenance requirements such as:

1) The clear definition of normal and abnormal operating conditions.
2) Adequate margins in the design of systems and plant components, including robustness and resistance to accident conditions, in particular aimed at minimizing the need to take measures at Level 2 and Level 3.
3) Adequate time for operators to respond to events and appropriate human-machine interfaces, including operator aids, to reduce the burden on the operators.
4) Careful selection of materials and use of qualified fabrication processes and proven technology together with extensive testing.
5) Comprehensive training of appropriately selected operating personnel whose behaviour is consistent with a sound safety culture.
6) Adequate operating instructions and reliable monitoring of plant status and operating conditions.
7) Recording, evaluation and utilization of operating experience.
8) Comprehensive preventive maintenance prioritized in accordance with the safety significance and reliability requirements of systems.

Point number 5 of the safety provision at level 1 shows that qualified personnel which has good safety behaviour is needed to achieve reliable and safe operation of the installation. So, the safety culture [2, 3] is very important to enhance the safety behaviour of every personnel in the installation.

For the effective implementation of defence in depth, some basic prerequisites apply to all measures at Levels 1 to 5. These prerequisites, which are interrelated and are fulfilled as part of policy for safe design and operation, are appropriate conservatism, quality assurance and safety culture [1].

1.2. Defence in Depth in the Experimental Fuel Element Installation (EFEI)

The Experimental Fuel Element Installation (EFEI) is one of the nuclear installations in BATAN that supports the research and development of the production technology of nuclear fuel. EFEI is designed to convert yellow cake into nuclear grade UO_2 powder. This

installation also has the ability to turn the nuclear grade UO_2 powder into Heavy Water Reactor (HWR) type fuel bundle. According to production process, EFEI consists of several facilities such as purification and conversion facility, pelletisation facility, Fuel assembly facility, quality control laboratory, mechanical workshop, supporting and energy supply and safety systems. EFEI is designed to support two main activities on the development of power reactor fuel technology in BATAN:

1) Conversion of yellowcake into nuclear grade UO_2.
2) Fuel fabrication of Heavy Water Reactor (HWR) that uses natural UO_2; research and development of fuel fabrication and fuel rod PWR type. The equipment in the EFEI could be upgraded to produce other kinds of pellet based fuel elements for power reactors whether using natural UO_2 or enriched UO_2 with a maximum enrichment of 5% U-235.

Defence in depth concept is implemented in the EFEI. The objectives of the implementation of the concept are to prevent accidents and to give the appropriate protection for the workers, public and environment. The main aspect of this concept is the use of several levels of protection layers to prevent radioactive releases to the environment. The levels of protection back up each other if failures or accidents happen.

The Defence in Depth concept for non-reactor nuclear installations is generally the same as that for nuclear reactors, but the implementation of this concept is slightly different.

The objectives of defence in depth strategies in the EFEI are: (a) to prevent accidents, and (b) in case an accident happens, to limit its radiological consequences and to prevent the evolution of the event to become worse. The application of defence in depth in a nuclear installation usually consists of five independent layers that a failure in one layer would not affect the others.

Defence in depth is applied in the EFEI in the following structures:

a) First Level of Protection

The prevention of abnormal operation and failures that is done through conservative design and high quality in construction and operation. All systems, structures, and components of the EFEI are of conservative design (such as the building that can endure a seismic load of 0.16g), having considered all potential hazards present (such as the ability to handle uranyl nitrate solution, the use of stainless steel tanks, etc), and having considered environmental factors in its construction. Regarding high-quality operation, the EFEI conducts the following administrative measures: (a) access control to the laboratories, (b) all instruments are operated below their safe operating conditions and following valid procedures, (c) maintenance programs are conducted on schedule, (d) operation and maintenance activities are done only by able and trained personnel, (e) safety based classification of systems, structures, and components, (f) implementation of quality management system and safety culture.

b) Second Level of Protection

The objective of the second level is to detect abnormalities and prevent the abnormalities from becoming accidents. For this reasons, EFEI is equipped with systems to detect abnormal operations and to protect the facility in case of failures, such as radiation/contamination detection system, smoke/fire detection, hydrogen/combustible gases leak detection, overpressure protection, over volume protection, and fire protection. An interlock system is installed in vital instruments. Besides that, the operation and maintenance procedures have to be available in EFEI. Those procedures have to be complied with and implemented in accordance with the applicable provisions.

c) Third Level of Protection

The objective of the third level is to control the accidents within the design basis so that the radioactive materials would not harm the workers and it won't be released to the environment. For this reason, IEBE is equipped with engineered safety features such as radiation shielding, ventilation system, etc. Besides that, the operation procedures in emergency conditions have to be available in EFEI. These procedures have to be done if accidents occur in the installation. A routine emergency preparedness exercise is conducted at least once a year.

d) Fourth Level of Protection

The objective of the fourth level of protection layer is to control accidents beyond the design basis which could cause radioactive releases to the environment. For this reason, EFEI is equipped with isolation systems (Including ventilation systems and building isolation) to prevent radioactive releases to the environment. Besides that, the accident management procedures in emergency condition have to be available and they have to be done if accidents happen in the installation. The objective is to mitigate the impact of accidents.

e) Fifth Level of Protection

The objective of the fifth layer is to mitigate the radiological consequences of significant releases of radioactive material to the environment if the fourth level fails. The emergency situation is assumed to go beyond the borders of the facility, hence the need for the involvement of related external organizations, such as local authorities, the national police, the military, nearby hospitals, and the regulatory agency [7].

2. DEVELOPMENT STRATEGIES

As stated above, safety culture has an important role in the implementation of DID. In addition, safety culture has to be implemented in every nuclear installation in Indonesia. As was stated in BAPETEN Chairman Reg. Safety Requirement NRNI, NO .11 [4]:

1. Operating organization should implement and enforce safety principles and processes to achieve an effective safety culture.
2. An effective safety culture as referred to in paragraph (1) shall include:
   a) Policy level commitment, including statement of safety policy, management structure, resources and self-regulation.
   b) Managers commitment, such as definition of responsibilities, definition and control of safety practices, qualification and training, rewards and sanctions, audit, review and comparison.
   c) Individual commitment, including questioning attitude, tenacious, careful, honest, and communicative.

The condition of the safety culture at EFEI up to the beginning of 2006 was still weak. This can be seen from the following indicators:

a) The attitude and behaviour of the individual and the organization still sees/prioritizes safety measures in operating nuclear installation as a provision or a regulation.
b) Individuals/personnel are not enthusiastic in involving themselves in daily safety activities.
c) Unsafe acts and unsafe conditions are often met in daily activities.
d) A lack of senior leadership visibility in the work floor.

Weak safety culture also results in low motivation and low productivity of the EFEI personnel. Therefore, in order to assurance safety and productivity, a program to strengthen safety culture must be developed. The main objective of the program is to increase understanding and personnel awareness of safety that will be reflected on the way of thinking, attitude and behaviour during daily activities (work) at EFEI.

In order to build the same understanding and increase personnel involvement, the first step that must be taken is the dissemination of key aspects of safety culture, and inviting all personnel to formulate the Vision, Mission, Core Values and Basic Principles regarding safety.

The vision is related to operating EFEI reliably and safely; "Operating EFEI for the wellbeing". The main meaning is to make sure nobody gets hurt and does not damage the environment. And the main mission is to make EFEI a workplace that is:

a) Offers safety and can provide safety assurance for all personnel, society, and the environment from radiological hazards due to EFEI operation.
b) Sustains productivity and can provide sustainable excellent services for the development of nuclear fuel technology for all stakeholders.

In order to achieve the Vision and Mission, all activities at EFEI must be supported by values, i.e. safety is the main and first priority, harmonious and synergic cooperation, responsible and accountable and continuous improvement and as a daily guidance in operating safely. Below are the basic principles developed at EFEI:

a) Incidents or work accidents can be prevented, and there is no tolerance towards an incident or accident.
b) There is no job that is so important or urgent that it cannot be executed safely. It is better to postpone or terminate a job when problems of safety are known.
c) Safety is an integral part of the working process so every hazard must be identified and its risks controlled.
d) Safety is the responsibility of every person. Assuring the safety of the person and the partner is a duty and obligation of each and every EFEI personnel.
e) Safety performance must be continuously improved, and the safety accountability must be performed.

The next step is strengthening safety culture at EFEI by applying implementable strategies. Five characteristics of safety culture in the IAEA Safety Guide No. GS-G-3.5 [5] are directly adopted as a strategy to develop safety culture at EFEI. The strategies and activities include:

a) Safety is a clearly recognized value. The main activities are: communication of safety values through socialization, safety culture training and workshops, sharing experience on the implementation of safety culture with other units in BATAN, pre-jobs briefing, coffee morning, safety posters or banners, and others.
b) Leadership for safety is clear. The main activities are: increasing the frequency of senior leader visits to the workplace (work-floor), leadership training to personnel especially supervisors, personnel qualification through the work permit from Regulatory Agency (Bapeten), engagement of personnel in occupational health and safety inspection, establishment of open two-way communication, and others.
c) Accountability for safety is clear. The main activities are: regularly report to the Regulatory Agency (BAPETEN) of the EFEI operating activities, the development of Safety Performance Indicators, definition and documentation of roles and responsibilities of each personnel, open reporting of safety problems, etc.

d) Safety is integrated into all activities. The main activities are: the implementation of the Hazard Identification Risk Assessment and Determining Control and Workplace Hazard Assessment, the internalization of the concept of STAR in work, strengthening of competence through training, development of behaviour based safety, morning briefing before work, housekeeping through voluntary work cleaning and tidying up the work place (5S), strengthening teamwork, etc.
e) Safety is learning driven. The main activities are: safety self-assessment, OHS inspection by personnel and management, open reporting of safety problems (near miss, incident, accident), participation in the IAEA-FINAS (Fuel Incident Notification and Analysis System), safety discussions during the coffee morning, exchange of experiences and information related to implementation of safety culture among the work units in BATAN, requalification training of personnel, facilitation of learning activities, etc.

The tools to evaluate progress in the implementation of safety culture at EFEI have also been developed, i.e.:

a) Safety Performance Indicators (SPI). These indicators have also been used as a bridge between the EFEI operator and the Regulatory Agency to assess the safety performance of EFEI. This SPI has been developed together between EFEI and the Regulatory Agency. The SPI of EFEI has been made a model by the Regulatory Agency for the development of SPI for Non Reactor Nuclear Installation (NRNI) in Indonesia.
b) Management System Inspection Tool (MSIT). This tool is used by the Regulatory Agency to assess the implementation of safety culture at EFEI.
c) Check list on OHS Inspection. This tool is used by personnel or workers appointed to assess the safe conditions of the working place. Starting May 2011, this tool has been equipped with Fire Risk Assessment as there is a large potential of fire hazards at EFEI.
d) Questionnaire on Safety Culture. This tool is used to assess the personnel's perception of the implementation of safety culture at EFEI. This tool has also been equipped with a quiz to assess the level of personnel understanding of the safety culture at EFEI. The uniformity of understanding of safety culture is the main capital to build a strong safety culture [2].
e) Check list of Behaviour Based Safety - BBS. This tool is used to assess the compliance and safety behaviour in daily activities at EFEI.

Self-assessment of safety culture at EFEI is held once a year. It is done based on three main tools, i.e. SPI, OSH inspection result, safety culture questionnaire and the result of the observation of BBS.

3. RESULTS AND DISCUSSION

The basic characteristics of safety at EFEI are represented by (a) a close connection among equipment, humans and the materials handled, (b) the variety of equipment and processes used, (c) the danger of radiology when under critical stage, (d) the existence of hazardous and toxic materials including nuclear materials spread in the installation, and (e) the risks for the security of nuclear materials. These characteristics show that safety in operating EFEI relies on human factors. Global statistical data show how human factors are the main cause of accidents. Therefore, safety culture must be implemented to support EFEI operation that is reliable and safe.

The implementation of safety culture is needed to support the reliable and safe operation of the EFEI. The high-quality operation of the EFEI will minimize abnormalities due to system and component failures. Therefore, the implementation of safety culture must be done continuously and in a measurable manner so that all EFEI personnel work in accordance with high quality standards. The enhancement of safety culture will result in safe behaviour of personnel and it is the first level of defence in depth.

In order to implement safety culture, EFEI-PTBN conducted activities within a group known as the Quality Improvement Team (QIT) with the subtheme Safety Culture. Among the activities are:

- Safety culture workshops, including HIRADC, WHA, and BBS workshops.
- Sharing of experience of implementing safety culture among working units at BATAN.
- Self-assessment of safety performance and installation safety (the implementation of safety culture).
- Facilitate coffee morning, morning briefings, safety training, etc.

All of the above activities carried out within the framework of socialization, internalization and enculturation of safe behaviour, as well as learning about the importance of safety culture in EFEI. Expected outcomes are increasing: (a) the involvement and active participation of personnel in enhancing safety culture activities, (b) increased motivation and safe behaviour; (c) the controlled potential dangers (hazards) and safety risks, (d) the internal and external communications, and (e) the safety commitment of individual at all levels.

Below are several important agendas that have been done to build strong safety culture at EFEI:

3.1. Increasing work motivation through walk time of senior leaders

The visits of senior leaders to work floor (Figure 1) improves work motivation and personnel discipline. This will give positive psychological impact to personnel that feel neglected by their leaders. The importance of visits by senior leaders is that leaders develop and influence culture by their actions (and inactions) and by the values and assumptions that they communicate. A leader is a person who has an influence on the thoughts, attitudes and behaviour of others. Leaders cannot completely control safety culture, but they may influence it.

FIG. 1. Routine visits by senior leaders.

3.2. Workshop on Safety Leadership

Leadership exists in everybody. Safety is the spirit that always clings to every work. Team work is the model chosen to build a superb safety performance with zero accidents and injury free workplace. The effectiveness of team work depends on the ability of the leader. Because safety has become number one, and each personnel is responsible for it, safety leadership must be developed continuously (Figure 2). Safety leadership constitutes all activities to influence, to move, to direct, and to empower working partners to work together to achieve zero accident and injury free workplace. Safety leadership is an act for a superb safety.

3.3. Hazard Identification Risk and Determining Control (HIRADC) adn Workplace Hazard Assessment (WHA) Workshop

Workshop on HIRADC and Workplace Hazard Assessment (WHA) is conducted twice a year (Figure 3). HIRADC is an analysis of potential hazards, risk assessment, prevention and ways to reduce hazards in a job, while the WHA is an analysis of potential hazards caused by tools or materials that are stored in the workplace, including ways to cope when an incident occur, and how to eliminate and reduce danger. The HIRADC and WHA workshops are also attended by personnel from other working units in BATAN Serpong. The main purpose of the workshop is that every personnel can conduct HIRADC and WHA as well as give inputs to the management on the plan of controlling hazards or risks. This activity is also to enhance teamwork and involvement of personnel – safety ownership.

FIG. 2. Workshop on Safety Leadership.

FIG. 3. Workplace Hazard Assessment (WHA).

3.4. Applying Standard Operation Laboratory in EFEI

Always make time for safety is the sentence in the poster assigned at the entrance of the laboratory. This list contains the SOP of working safely at EFEI in general, i.e. provisions for every personnel before they work: (a) Tasks/activities that will be done; (b) Hazards and risks of danger; (c) The cause or the event that causes the risks; (d) Controlling the event and overcoming the danger; and (e) Emergency procedures. The practical application is that every personnel that will work in the EFEI laboratory must fill a proposal form of the event first. This form is an analysis form of the safety of the task. It is simple but it is sufficient so it can be filled by all personnel. The main function of the form is to integrate the safety of the working process and also as a controlling device in running activities. Aside from that, personnel also need to fill a STAR form (stop-think-act-review) before, during and after the job.

3.5. Housekeeping - 5 S Volunteer Work (Sort, Set in order, Shine, Standardize, Sustain)

Volunteer work (Figure 4) is done by all staff members of EFEI to clean and tidy as well as check the working conditions at EFEI. It is done once a month on Friday morning. Through this volunteer work, it is expected that the working conditions at EFEI are kept clean and tidy. This is also to encourage team work and involvement of personnel ownership of the safety program.

3.6. First Aid and Fire Extinguisher Training

Every personnel is obliged to attend First Aid training (Figure 5) and Fire Extinguisher using light fire extinguishers. It aims to provide skills to EFEI staff members to be able to provide first aid assistance to their colleagues when an accident in the work place occurs. First aid training is held once a year and the trainers are physicians and nurses from the BATAN health care centre. The potential for fire hazards at EFEI is large as we bear in mind the types of material and the processes that take place. Light fire extinguishers are the only fire extinguishers that are available at the work place. Therefore, every EFEI personnel must be able to operate Light fire extinguishers to extinguish fire. It should be noted that in the EFEI laboratory, it is not allowed to extinguish fire with water as there is the possibility of a nuclear material undergoing criticality.

FIG. 4. Volunteer work in the laboratory.

FIG. 5. First Aid Training.

3.7. Workshop on Fire Risk Assessment (FRA)

Fire Safety is an important safety issue that must be addressed by management (Figure 6). It aims to minimize the risks of injuries and loss of life. Fire has the potential to injure or to kill in a short period of time. The objectives of Fire Risk Assessment are:

- To identify fire hazard potentials.
- To reduce the fire hazard risks.
- To determine measures to prevent fire hazard and to set up a fire safety management in case of accidents.

3.8. Occupational Health and Safety Inspection (OHS Inspection)

OHS Inspection (Figure 7) is done routinely every month on a rotating basis by all members of EFEI staff in order to create a safe, secure and comfortable working condition. The result of OHS inspection is used for self-evaluation every semester. Inspection is done in every room using an official check list of OHS inspection. The check list contains 60 (sixty) items or statements that have to be checked at the work place. Formal OHS Inspection is done by the EFEI management at least once a year. The inspection is led by the Head of Centre for Nuclear Fuel Technology (PTBN) as the Holder of the EFEI Operation Permit. This event is also intended to increase motivation, teamwork and involvement of personnel ownership.

FIG. 6. Workshop on Fire Risk Assessment (FRA).

FIG. 7. Personnel in OHS Inspection.

3.9. Coffee morning

Coffee morning (Figure 8) is a media to create open communication between the staff and management. Each staff member is asked to deliver any criticism toward colleagues or superiors while drinking coffee and enjoying refreshments. It is also used as a time to communicate work issues, so a solution can reached by all members of the staff.

3.10. Sharing of the implementation of safety culture

Sharing of the implementation of safety culture is done by visiting other working units (Figure 9) in National Nuclear Energy Agency (BATAN) and Oil Company (PERTAMINA). The purpose of the sharing is to support and give input on the implementation of safety culture in each working unit.

FIG. 8. The situation of coffee morning.

FIG. 9. EFEI Safety Culture Team engaged in sharing on the implementation of safety culture.

3.11. Morning briefing (Pre-Job Briefing)

Morning briefing (Figure 10) is done as a media for safety induction for all operators that work in the laboratory. The leaders of morning briefings are supervisors scheduled routinely every morning.

3.12. Implementation of Behaviour Based Safety (BBS)

BBS is observation done to personnel of the laboratory that are on duty (Figure 11). Observation covers:

- The use of self Personal Protection Equipment (PPE). The accuracy and the condition of PPE such as: gloves, masker, shoes, and lab coats, and other PPE.
- The position/acts of the workers when on duty.
- The response of the workers toward observation.
- Equipment.
- Housekeeping.
- Work procedures.
- Work authority.

When, under observation, unsafe acts conducted by workers are identified there will be direct intervention by the officer/observer so that the unsafe acts are immediately changed to safe acts.

FIG. 10. The situation at morning briefings.

FIG. 11. Behaviour Based Safety.

3.13. Participation of EFEI in IAEA- FINAS (Fuel Incident Notification and Analysis System)

FINAS (Figure 12) is a forum at the IAEA that contains lessons from incidents taking place in a nuclear installation. Every incident, no matter how small, is noted and reported to the management and to BAPETEN (the coordinator of FINAS Indonesia). Next, it is evaluated and analysed to discover the potential and the cause of the event and to propose solutions.

3.14. Personnel Qualification

Personnel qualification and training as required by Regulatory Agency (BAPETEN) has been continuously done (Figure 13). The qualification of EFEI personnel that are required to have a Working Permit from the Regulatory Agency are the NRNI Operator, NRNI Supervisor, Nuclear Material Inventory Officer, and the Officer of Radiation Protection. SIB (working permit) is valid for 3 – 4 years and when it expires, the holder of SIB is required to follow a requalification test held by the Regulatory Agency. As of today, all technical personnel of EFEI have SIB.

The main goal of personnel qualification is to assure: (a) the safety and the health of the workers, the community, and the living environment; (b) the safety and the security of the installation and the nuclear material; and (c) the use of nuclear material for peace purposes.

FIG. 12. Several events that are set as learning in FINAS.

FIG. 13. Personnel qualification improvement activities.

3.15. Self Assessment of Safety

Self Assessment is an activity of self evaluation for EFEI to assess and identify how far the safety culture at EFEI has been implemented. Self assessment is done by conducting three components:

(a) Filling in SPI (Safety Performance Indicator)

EFEI with BAPETEN has managed to develop SPI for NRNI. EFEI has appointed BAPETEN as the role model in Indonesia to fill the SPI for NRNI. The scope of SPI EFEI is:

(1) Nuclear safety

- High quality of operation.
- Triggering events.
- Mitigation system.
- Barrier Integrity.

(2) Radiation safety

- Radiation safety.
- Radiation and contamination of the working area and environment.
- Radioactive waste.

(3) Nuclear awareness

- Awareness and notification system.
- Nuclear emergency drill.
- Participation of members of the organization to be responsive.

(4) The management system and facility and activity

- The responsibility of management.
- The management of resources.
- Implementation process.
- Measurement, assessment, and repair.

(5) Nuclear safety

- Safeguard.
- Physical protection.

The overall score of SPI EFEI 2012 is 3.82 [max score 5]. The results show that the overall condition of the safety culture at EFEI is in line with the provisions required by Regulatory Agency. The operation at EFEI has been done consistently and fulfils the provisions and regulations. Most of the problems that occur can be solved quickly. Problems that cannot be solved immediately such as, default equipment, do not affect the safety of the workers, the community and the environment.

(b) The Result of Occupational Health and Safety Inspection (OHS Inspection)

The findings from the routine OHS Inspection (monthly) is immediately followed-up and solved when possible. All of the findings and repairs that have been done are reported in the self-assessment. Findings that have not been solved will be discussed and solved. The number of findings and percentage of solutions are the indicators of a successful OHS.

The real result of the execution of OHS inspection is the increase of the personnel's care toward their work space, especially in terms of cleanness and tidiness.

(c) The Result of questionnaire on safety culture

Every year, EFEI holds a survey on the perception of personnel on the implementation of safety culture at EFEI. The results of the surveys in 2011 and 2012 are stated in the radar chart shown in Figure 14.

The average value of all characteristics surveyed in the EFEI in 2012 was 7.06. It is in stage 2, just as the average value of 2011 (7.09). It shows that in the EFEI "Safety becomes an organizational goal". An organization at this stage considers safety to be an important organizational goal, even in the absence of external requirements. Although there is growing awareness of behavioural issues, this aspect is largely missing from safety management, which generally concentrates on technical and procedural solutions. Safety is dealt with in terms of targets or goals, with accountabilities for achieving the goals specified. Organizations at this stage often discover that after a period of time, when safety trends have improved, a plateau is reached [3].

3.16. Review with Management System Inspection Tool (MSIT)

BAPETEN has conducted a review of the implementation of safety culture at EFEI using MSIT. The review was done in 2010 and EFEI was the first to be used as a case study of the implementation of MSIT in the inspection by BAPETEN for nuclear installations in Indonesia. Review with MSIT aims to assure that:

- There is the same understanding of the aspects of safety culture in an organization.
- There is a way that the organization can support the individual and the team in completing the tasks well and safely, by considering the interaction among individuals, technology and the organization.
- The development of a study attitude and curiosity to ask at all levels in the organization.
- There is a way that the organization will try to develop and enhance safety.

The results of EFEI show that all components or criteria in MSIT can be fulfilled by EFEI, and MSIT is comprehensive enough as a tool for monitoring and evaluation of the implementation of safety culture in an organization.

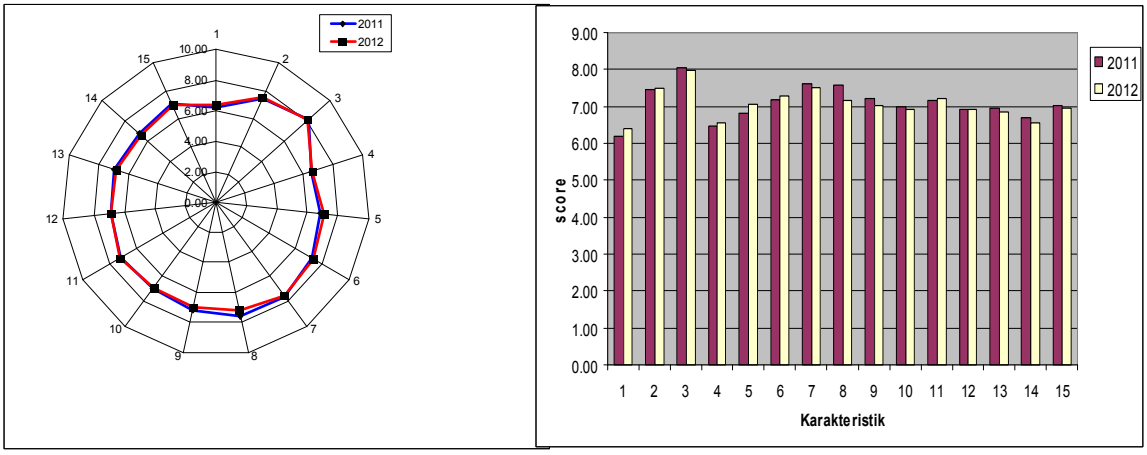

FIG. 14. Radar chart of safety culture survey.

4. CONCLUSIONS

Safety is priority and a main consideration in every activity at EFEI and safety should be maintained sustainably. In order to achieve strong safety culture at EFEI, cooperation and commitment is needed from the management and all personnel. The five characteristics of a strong safety culture in the IAEA Safety Guide No. GS-G-3.5 [5] were adopted as a strategy to develop safety culture in the EFEI. The implementation of strong safety culture is needed to support reliable and safe operation of the EFEI so that abnormal conditions can be minimized. The enhancement of safety culture will result in safe behaviour of all personnel so that a high quality operation of the EFEI can be achieved and it means that the first level of defence in depth works well. The agendas to enhance safety culture as the first level of defence in depth applied in the EFEI are as follows: senior management visits, safety leadership training, workshops on hazard identification, risk assessment, and determining controls (HIRADC), workshops on workplace hazard assessment (WHA), routine housekeeping, implementation of laboratory standard operations, first aid training, Workshop on Fire Risk Assessment (FRA), Coffee morning, pre-job briefing, Implementation of Behaviour Based Safety, participation in the fuel incident notification and analysis system (FINAS), personnel qualification training, and safety self-assessment using Management System Inspection Tool (MSIT). The EFEI puts a target that in 2015, its safety culture status is on Stage 3 of the IAEA-TECDOC-1329 [3]: "Safety can always be improved." An organization at this stage has adopted the idea of continuous improvement and applied the concept to safety. There is a strong emphasis on communication, training, management style and improving efficiency and effectiveness. People within the organization understand the impact of cultural issues on safety.

ACKNOWLEDGEMENTS

The authors would like to express appreciation for the help of support, to Mr Djarot S Wisnubroto as the head of National Nuclear Energy Agency (BATAN), Mr Budi Briyatmoko as the head of Center for Nuclear Fuel Technology, Mrs Yusri Heni as the pioneer of safety culture from Nuclear Energy Regulatory Agency (BAPETEN), colleagues of the safety culture team EFEI (Agus Sartono, Mugiyono, Torowati, Eko Yuli R, A S.Latief, Mu'nisatun, Erilia Yusnitha, Deni Mustika and Arief S Adhi), and all of personnel in EFEI.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Safety Culture, INSAG-4, IAEA, Vienna (1991).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Culture in Nuclear Installations, IAEA-TECDOC-1329, Vienna (2002).

[4] BAPETEN CHAIRMAN REG, Safety Requirement NRNI, NO .11, (2007).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System For Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2006).

POSTER SESSION

DEFENCE IN DEPTH BY DESIGN FOR THE ADVANCED GIII NPP IN CHINA

S. LIU, Y. ZHANG, X. ZHANG
Science and Technology on Reactor System Design Technology Laboratory
Chengdu, Sichuan, CHINA
Email: liusongtao.npic@gmail.com

Abstract

This paper describes the design of the advanced nuclear power plant ACP1000 in CHINA that keeps the principle of defence in depth. To enhance the safety of the new generation NPPs, passive and active engineering safety features are used. The reactor will be kept safe under design basis accidents by using active engineering safety features, such as the medium and low pressure safety injection systems, and the emergency feedwater system. Under beyond DBAs, the passive safety systems will be actuated to keep removing residual heat for more than 72 hours, and to keep the core melt retained and cooled in the vessel. After the Fukushima nuclear accident, there are six main design enhancements in ACP1000 to meet the demands of the China authorities.

1. INTRODUCTION

The safety of modern nuclear power plants is better than twenty years ago. The three reactor accidents (Three Mile Island 1979, Chernobyl 1986, Fukushima 2011) forced the nuclear designers and operators to improve the safety of plants. As a result modern plants have safety systems that use passive and active safety technology. In the case of a nuclear power plant, safety means that the design of the plant must ensure safety even in the case of a serious accident. The modern plants (among them the ACP1000) fulfil this criterion. The constructors have developed a huge number of accident prevention methods and the safety systems are built so that they can avert several types of accidents. The safety systems are prepared and the personnel are trained to be able to prevent emergency situations. Since it is impossible to consider all the possibilities there is a need for continuous safety enhancement measures and reviews. These are the basic requirements that the nuclear operators have to comply with, including the ACP1000 Nuclear Power Plant in China.

In nuclear power plants there is a large amount of radioactive material, against the radiation of which the workers must be protected and in an accident situation the release of these materials to the environment must be prevented. In an NPP, a large quantity of heat is generated even after shutdown due to the radioactive decay of the fission product isotopes.

Therefore, three basic safety conditions [1] must be fulfilled in a nuclear power plant:

- Efficient control of the nuclear chain reaction (reactivity control).
- Proper cooling of the reactor core.
- Prevention of the release of radioactive materials.

These safety functions are implemented in an NPP with the aid of the so-called defence-in-depth (DID).

2. WHAT IS THE DEFENCE-IN-DEPTH IN CHINA

Defence in Depth [2] is a safety philosophy that guides the design, construction, inspection, operation, and regulation of all nuclear facilities. The central tenet of Defence in Depth is to protect the health and safety of the public and plant workers. Other objectives include protecting the environment and ensuring the operational readiness of the facility. Successful Defence in Depth requires creating, maintaining, and updating multiple

independent and redundant layers of protection to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon.

Defence in Depth is an on-going approach toward ensuring public health and safety. This approach recognizes that imperfections, failures, and unanticipated events will occur and must be accommodated in the design, operation, and regulation of nuclear facilities. Defence in Depth is implemented through a number of measures, including robust physical barriers, redundant and diverse safety systems, strong physical security, and emergency response readiness.

2.1. Design and Construction

Defence in Depth requires a high-quality process for the design, procurement, fabrication, construction, inspection, testing, and licensing of a nuclear facility. State, and local laws regulate every step in this process.

2.2. Multiple Barriers

Facility designers incorporate multiple, successive barriers [3] to prevent the release of radioactive material. In nuclear power plants licensed in China, multiple physical barriers are present. The primary barriers are the fuel and cladding, which are designed to contain radioactive material under extreme conditions inside the reactor core. The secondary barrier is the reactor vessel, which contains the coolant used to carry away heat for generating electricity. The final barrier is the primary containment building, which is designed to mitigate the release of radioactive material in the event that both the primary and secondary barriers are compromised. The primary containment is designed to withstand the most severe, credible event (either internal or external) for the location of the plant.

2.3. Redundancy and Diversity

Engineered systems that are classified as being important for safety have very robust designs to ensure reliability. Nevertheless, in the event of a component failure, Defence in Depth requires that multiple backup systems are available to replace the safety-related function of the failed component. In addition, backup systems are designed based on different physical principals or mechanisms to limit the possibilities of common-mode failures.

2.4. Maintenance and Operations

Facility testing and maintenance procedures are implemented to ensure that each individual system operates to provide its intended function. For safety-related systems, normal plant operations are not permitted unless sufficient backup capabilities are available. In addition to supporting Defence in Depth, proper maintenance and operating procedures help ensure reliable, economic operation of the facility.

2.5. Physical Security

Even prior to 9/11, physical security has been an important component of Defence in Depth. A post 9/11 review of physical security emphasized the tightly interconnected nature of facility safety, physical security, and emergency preparedness. Although major changes were not required, enhancements have been made to improve access controls, training requirements, security exercises, and defensive capabilities. Now considering a large

commercial aircraft event, the inherent robustness of the shield building is improved to satisfy the requirement of aircraft impact assessment beyond design basis.

2.6. Emergency Preparedness

Emergency preparedness includes communication, sheltering, evacuation, and response plans. Nuclear facilities coordinate with local and state authorities to ensure that emergency preparedness plans are well defined and periodically tested through training exercises. Emergency preparedness plans are a licensing requirement for all nuclear facilities regulated by the regulatory authority of China.

3. DESIGN OF THE ACP1000 WITH DID

The current definitions and concepts of defence-in-depth have evolved over a long period of time in designing and regulating the current fleet of LWRs and have been modified in recent years to reflect the changes in philosophy brought about by risk-informed and performance-based regulation. While the NRC definitions of defence-in-depth have evolved, clarifications are still required to make the definition applicable to the ACP1000.

Plant capability Defence-in-Depth reflects the decisions made by the designer to incorporate defence-in-depth into the functional capability of the ACP1000 plant. These decisions include the use of multiple lines of defence and conservative design approaches for the barriers and SSCs performing safety functions associated with the prevention and mitigation of accidents. Plant capability Defence-in-Depth also includes the use of multiple barriers, diverse and redundant means to perform safety functions to protect the barriers, conservative design principles and safety margins, site selection, and other physical and tangible elements of the design that use multiple lines of defence and conservative design approaches to protect the public. For small reactors where economies of scale are not a primary economic opportunity, the design places a greater emphasis on prevention through inherent and passive features to reduce the dependence on active systems, thereby creating both safety value and economic value, without sacrificing defence-in-depth capability.

The approach combines the prevention of abnormal situations and their degradation with the mitigation of their consequences. The defence in depth concept consists of a set of actions, items of equipment or procedures, classified in levels, the prime aim of each is to prevent degradation that could lead to the next level and to mitigate the consequences of failure of the previous level. the principle can be simply summarized as follows: although the precautionary measures taken with respect to errors (incidents and accidents) are, in theory, such as to prevent their occurrence, it is nevertheless assumed that accidents do occur and provisions are made for dealing with them so that their consequences can be restricted to levels deemed acceptable.

3.1. Excellent intrinsic resistance

The ACP1000 was designed with excellent intrinsic resistance to specified hazards in order to reduce the risk of failure. This means that following preliminary delineation of the installation, an exhaustive study of its normal and foreseeable operating conditions be conducted to determine the worst (mechanical, thermal, pressure) stresses or those due to environment, layout, etc., for each major system and component, for which allowance must be made.

3.1.1. Nuclear design to increase the intrinsic safety

ACP1000 employs more fuel assemblies from 157 to 177, and decreases the average linear power density to 173.8 W/cm. The negative neutronics feedback effects are kept. The larger shutdown margin ensures improved reactor safety. In addition, a flattened core power distribution is incorporated for safety and flexible operation.

3.1.2. Fuel assembly design to increase the intrinsic safety

Self-reliance development of the CF3 fuel assembly has been validated by both extensive out-pile and in-pile irradiation tests. The N36 Zircaloy cladding is used for CF3, which has excellent performance for corrosion and abrasion. The special spacer grids for CF3 have improved thermal-hydraulic behaviour to increase the DNB margin.

3.1.3. Other design features to increase the intrinsic safety

There are some other design features to increase the safety of ACP1000 as follows:

- Advanced core instrumentation system.
  - *Penetrations from top of RPV.*
  - *Continuous on-line measurement.*
- Larger PRZ volume for flexible operation.
- Optimized PRZ surge line design to ease thermal stratification.
- Overpressure protection by PRZ safety valves at low temperature conditions: *PRZ safety valves provide the function of overpressure protection at low temperature conditions, while preserving the function as RHR safety valves. The overpressure protection measures are consolidated.*
- LBB technology: *By application of LBB technology, before crack propagation in the pipe to the critical crack size leading a sudden rupture, safety shutdown can be achieved, so there is enough time to repair or replace the leaking piping and avoid guillotine double end piping rupture.*
  By removing the pipe whip restraints, the maintainability and accessibility of a nuclear power plant can be improved and radiation dose to staffs can be reduced.
- Improved design seismic capability: *Peak Ground Acceleration (PGA) is increased to 0.3g and design seismic spectrum is updated according to RG1.60.*
  Improved seismic capabilities for systems and components and variant NPP siting conditions.

3.2. Control of accidents within the design basis

A series of incidents and accidents is postulated by assuming that failures could be as serious as a total instantaneous main pipe break in a primary coolant loop or a steam line, or could concern reactivity control. Therefore, it is required to install safety systems for limiting the effects of these accidents to acceptable levels. Start-up of these systems must be automatic and human intervention should only be required after a time lapse allowing for a carefully considered diagnosis to be reached. In the postulated situations, the correct operation of these systems ensures that core structure integrity will be unaffected, which means that it can subsequently be cooled. Radioactive releases to the environment will consequently be adequately limited.

The control of accidents within the design basis is achieved by using the emergency core cooling system to provide sufficient cooling to the reactor core in a LOCA accident. The

emergency core cooling system has active medium and low pressure safety injection sub-systems and passive accumulator injection sub-systems. There's no high pressure safety injection to give the operator more than 30 minutes to wait and judge the accident, especially under SGTR (steam generator tube rupture) condition.

A simulation shows that SGTR leakage stops at 1.2 hour after the accident with no SG overfilling (see Figure 1) and with radioactive release to the atmosphere less than the acceptance criterion.

The LB LOCA accident analysis shows that the peak cladding temperature is 998.6 °C, and has a safety margin of 17% compared with the limit value of 1204 °C.

3.3. Control of severe plant conditions including prevention of accident progression and mitigation of severe accident consequences

We have to consider the means required to contend with plant situations which have bypassed the first two levels of the defence-in-depth (e.g. cases of multiple failure) or which were considered as part of the residual risk (i.e. the likelihood of such accidents is extremely low). Such situations can lead to higher radioactivity release levels. The concern here is to reduce the probability of such situations by preparing appropriate procedures and equipment to withstand additional scenarios corresponding to multiple failures. Every endeavour would also be necessary to limit radioactive release due to a very serious occurrence and to gain time to arrange for protective measures for the population in the vicinity of the site. It is then essential that the containment function be maintained under the worst possible conditions.

3.3.1. Designed countermeasures against severe accidents

The main countermeasures against severe accidents are showed in Table 1.

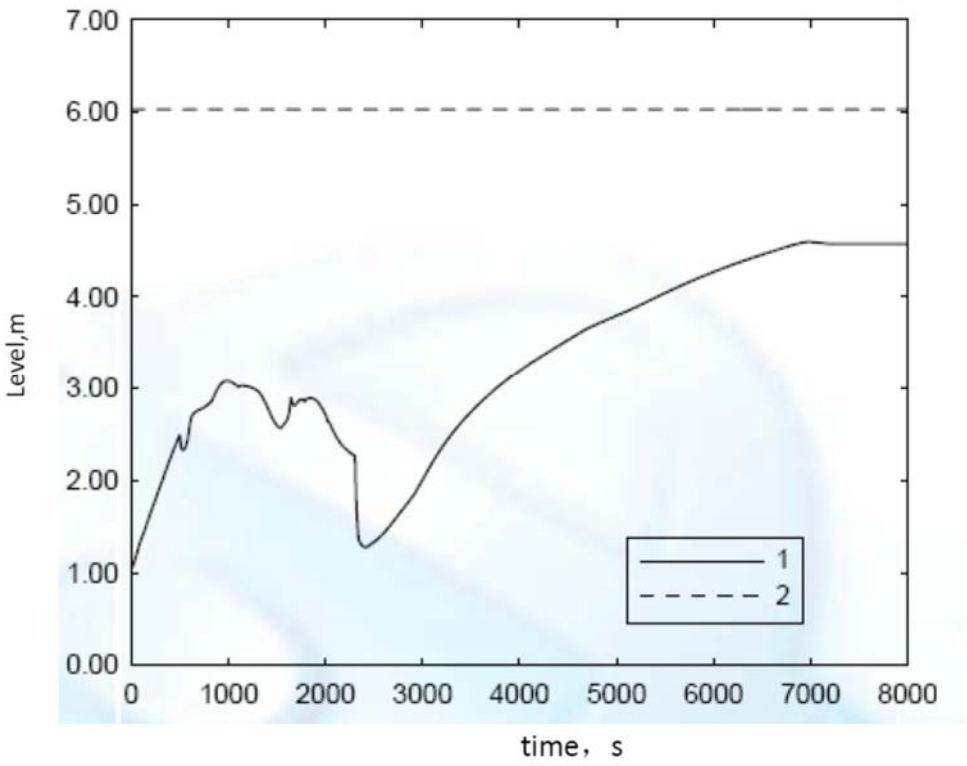

FIG. 1. The liquid level of ruptured steam generator.

TABLE 1. THE MAIN COUNTERMEASURES AGAINST SEVERE ACCIDENTS

Phenomena	Countermeasures
Hydrogen Detonation	Passive autocatalytic hydrogen recombiners
High pressure melt ejection, Direct containment heating	Fast depressurizing system of primary loop
Long-term overpressure	Passive containment heat removal system (showed as Figure 2), containment filtered and venting system
Basement melt-through	Reactor cavity injection and cooling system(showed as Figure 3)
Station Blackout	Passive residual heat removal system of secondary side(showed as Figure 4), additional backup power source
Other countermeasures for SAs	Reactor vessel high-point venting system, habitability of main control room, etc.

The ejecting of molten corium at high pressure (HPME) must be avoided by design, as it is a threat to the integrity of the containment. HPME accident is practically eliminated by a dedicated depressurization system to depressurize the RCS during a severe accident.

RPV high point venting system has the normal venting function at RPV high pressure. The non-condensable gases can be removed from the reactor vessel head by the operator in the main control room, to mitigate a possible accumulation of non-condensable gases in the reactor coolant system due to inadequate core cooling.

Other countermeasures to extreme the external events are the double-wall containment to protect against a large commercial aircraft crash.

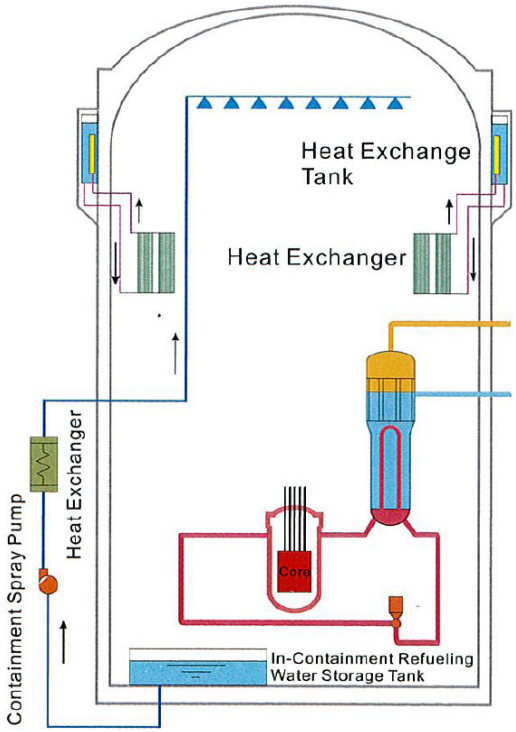

FIG.2. The passive containment heat removal system.

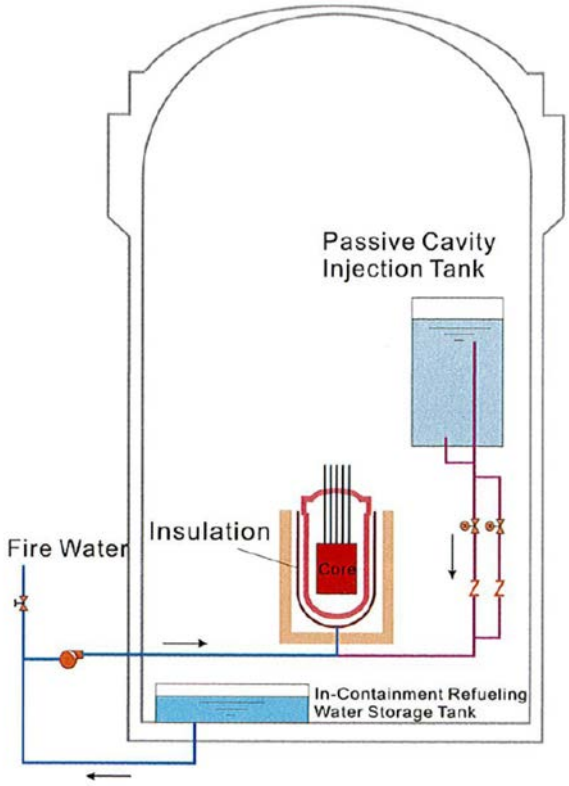

FIG. 3. The reactor cavity injection and cooling system.

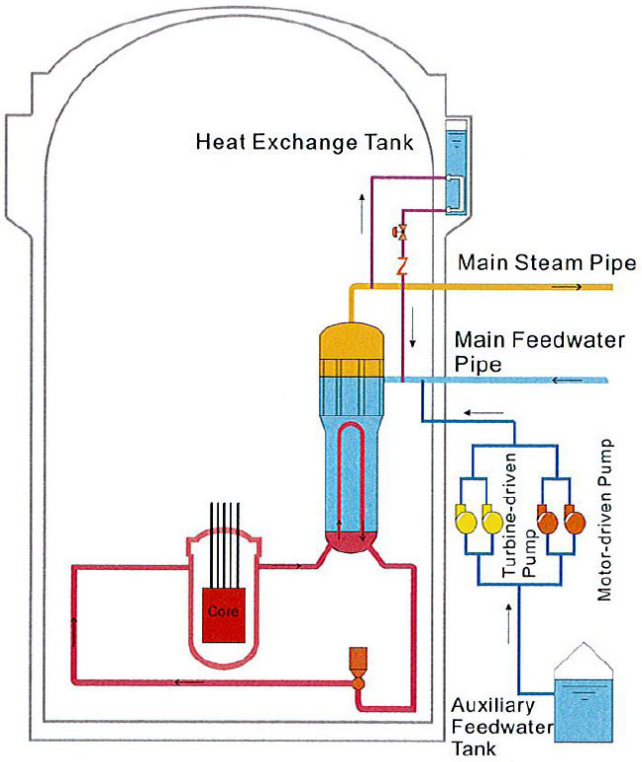

FIG. 4. The passive residual heat removal system of secondary side.

3.2.2. Feedback from Fukushima nuclear accident to enhance ACP1000

There are six main design enhancements incorporated in ACP1000 after the Fukushima nuclear accident [4]:

- Additional emergency water makeup.
- More conservative seismic margin.
- Spent fuel pool cooling and monitoring.
- Enhanced habitability and availability of emergency facilities.
- Extension of non-intervention period.
- Mobile power supply and power diversity consideration.

4. CONCLUSIONS

Population protection measures because of high release levels would only be necessary in the event of failure or inefficiency of the measures described above. The conditions of these measures are within the scope of the public authorities. They are supplemented by the preparation of long- or short-term measures for checking the consumption or marketing of foodstuffs which could be contaminated. Such measures are included in the external emergency plans. Periodical training drills are also necessary in this area to ensure adequate efficiency of the resources and linkups provided.

We have to note here that, according to the recommendations of the International Atomic Energy Agency, the principle is to be applied taking into account the characteristics of the installation. The national authorities should enforce implementation, but safety still remains the responsibility of the operating organization.

After the Fukushima nuclear accident, we should consider that local population have the right to join and give advice about how to protect the local environment.

REFERENCES

[1] INL, Next Generation Nuclear Plant Defence-in-Depth Approach, INL/EXT-09-17139, 2009.

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Defence in Depth for Nuclear Power Plants, Safety Reports Series No. 46, IAEA, VIENNA (2005).

[4] OMOTO, A., The accident at TEPCO's Fukushima-Daiichi Nuclear Power Station: What went wrong and what lessons are universal?, Nuclear Instruments and Methods in Physics Research A, 2013.

BASIC SAFETY CONSIDERATIONS FOR NUCLEAR POWER PLANT DEALING WITH EXTERNAL HUMAN INDUCED EVENTS

W. SALEM
Nuclear and Radiological Regulatory Authority, Egypt
Email: wafaasalem21@yahoo.com

Abstract

Facilities and human activities in the region in which a nuclear power plant is located may under some conditions affect its safety. The potential sources of human induced events external to the plant should be identified and the severity of the possible resulting hazard phenomena should be evaluated to derive the appropriate design bases for the plant. They should also be monitored and periodically assessed over the lifetime of the plant to ensure that consistency with the design assumptions is maintained. External human induced events that could affect safety should be investigated in the site evaluation stage for every nuclear power plant site. The region is required to be examined for facilities and human activities that have the potential, under certain conditions, to endanger the nuclear power plant over its entire lifetime. Each relevant potential source is required to be identified and assessed to determine the potential interactions with personnel and plant items important to safety.

1. INTRODUCTION

Facilities and human activities in the region in which a nuclear power plant is located may under some conditions affect its safety. The potential sources of human induced events external to the plant should be identified and the severity of the possible resulting hazard phenomena should be evaluated to derive the appropriate design bases for the plant. They should also be monitored and periodically assessed over the lifetime of the plant to ensure that consistency with the design assumptions is maintained.

Full consideration should be given at the stage of site selection to the possibility of disregarding locations having at present, or in the foreseeable future, a potential for severe external human induced events which may jeopardize the safety of the proposed plant and for which engineering solutions may prove unfeasible or impracticable.

2. OBJECTIVE

The external human induced events considered in these regulations are all of accidental origin. Considerations relating to the physical protection of the plant against wilful actions by third parties are outside its scope. However, the methods described herein may also have some application for the purposes of such physical protection.

The applicant shall follow IAEA code of practice; Safety Series No. NS- G-3.1 issued in 2002 and entitled "External Human Induced Events in Site Evaluation for Nuclear Power" and all other IAEA related documents [1, 2, 3]. The external human induced events considered in this document are all of accidental origin. Considerations relating to the physical protection of the plant against wilful actions by third parties are outside its scope.

3. TYPE OF POTENTIAL SOURCE

The sources of external human induced events may be classified as:

- Stationary sources, for which the location of the initiating mechanism (explosion centre, point of release of or toxic gases) is fixed, such as chemical plants, oil refineries, storage depots and other nuclear facilities at the same site.
- Mobile sources, for which the location of the initiating mechanism is not totally constrained, such as any means of transport for hazardous materials or potential projectiles (by road, rail, waterways, air, pipelines). In such cases, an accidental

explosion or a release of hazardous material may occur anywhere along a road or other way or pipeline.

4. COLLECTION OF DATA AND REQUIRED CRITERIA

The collection of information should begin early enough to enable the potential sources of external human induced events in the region to be identified at the stage of site selection. When a potential site has been identified, more detailed information may be necessary to identify reference hazards for external human induced events and to provide data for design basis parameters (the site characterization stage).

Furthermore, during the plant's lifetime (the pre-operational and operational stages), more data should be available from monitoring of the site to be used in the periodic safety assessments [4, 5, 6].

Information on such sources in the region should be collected to determine:

a) The locations of possible sources of external human induced events associated with transport systems.
b) The probability of occurrence and the severity of the events.
c) For surface transport: information should be collected on fixed traffic facilities in the region, including ports, harbours, canals, dredged channels, railway marshalling yards, road vehicle loading areas and busy junctions and intersections, and on traffic routes in relation to the site. Also, Information should be collected on the characteristics of traffic flows in the region, such as: the nature, type and quantities of material conveyed along a route in a single transport movement; the sizes, numbers and types of the vessels; speeds, control systems and safety devices; and accident statistics including consequences. Similar information should be collected for pipelines: on the nature of the substance transported, the flow capacity, the internal pressure, the distances between valves or pumping stations, safety features, and accident records including consequences.
d) For air traffic: The information collected on air traffic should include the locations of airports and air traffic corridors in the region, the airports' take-off, landing and holding patterns, the types of warning and control devices available, the types and characteristics of aircraft and their flight frequencies, restricted airspace, flight patterns and airport availability in case of accident. Information on aircraft accidents for the region and for similar types of airport and air traffic should be collected. Information should be collected for both civil and military air traffic. Of particular interest are military aircraft training areas which may show a comparatively high frequency of crashes in their vicinity and areas where low flying is practiced.
e) Source display maps should be prepared showing the locations and distances from the nuclear power plant of all sources identified in the data collection stage which may potentially affect the site. This map should reflect any foreseeable developments in human activities that may potentially affect safety over the projected lifetime of the nuclear power plants.
f) Installations which handle process or store potentially hazardous materials such as explosive, flammable, corrosive, toxic or radioactive materials should be identified as sources, even if associated with other on-site units under construction, in operation or undergoing decommissioning. The magnitude of the hazard may not bear a direct relation to the size of such facilities, but the maximum amount of hazardous material present at any given time and the process in which it is used should be taken into consideration. Furthermore, the progression of an accident with time, such as fire spreading from one tank to another, should also be considered. Pipelines for hazardous

materials should be included in the category of items to be identified. Other sources to be considered are construction yards, mines and quarries which use and store explosives and which may cause the temporary damming of water courses, with possible subsequent flooding or collapse of ground at the site.

g) At military installations, hazardous materials are handled, stored and used, and may be associated with hazardous activities such as firing range practice. In particular, military airports and their associated traffic systems, including training areas, should be considered potential sources.

h) Attention should be given to future human activities currently in the planning stage, such as for land with potential for commercial development. Such activities in the future may lead to an increased risk of radiological consequences or to sources of interacting events which do not exceed the screening probability level but may grow to reach that level.

i) Associated parameters, The human induced sources of events mentioned earlier may cause events that can generate effects such as:

- air pressure wave and wind;
- projectile impact;
- heat (fire);
- smoke and dust;
- toxic and asphyxia gases;
- chemical attack by corrosive or radioactive gases, aerosols or liquids;
- shaking of the ground;
- flooding or lack of water;
- ground subsidence (or collapse) and/or landslide;
- electromagnetic interference; and
- eddy currents into the ground.

Fires are one such type which may be common to a number of external human induced events. In particular, fires may be caused by an event such as an aircraft crash or a chemical explosion. External events which shall be evaluated include:

- *Fires*: A survey should be made at and around the site to identify potential sources of fire, such as forests, peat, storage areas for low volatility flammable materials (especially hydrocarbon storage tanks), wood or plastics, factories that produce or store such materials, their transport lines, and vegetation. The area to be examined for the possible occurrence of fires that may affect items important to safety should have a radius equal to the SDV.
- *Ship collision*: If the ship collision probability is found to be greater than the SPL, a detailed analysis should be conducted to assess the consequences of such an impact.
- *Electromagnetic interference*: It can affect the functionality of electronic devices. It can be initiated by both on-site (high voltage switchgear, portable telephones, portable electronic devices, computers) and off-site sources (radio interference, the telephone network). The presence of central telephone installations close to the site could give rise to specific provisions for the design stage, but usually such high frequency waves do not represent exclusion criteria for sites since specific engineering measures for the qualification of

equipment should be taken in the design stage and administrative procedures should be adopted on site to avoid local interference. In the site evaluation stage, potential sources of interference should be identified and quantified (for example, intensity, and frequency). They should be monitored over the lifetime of the plant for the purpose of ensuring the proper qualification of plant components.

5. DESIGN BASIS AND PARAMETERS

a) The information collected is initially used in a two-step screening stage to eliminate those sources which should not be considered further, on the basis of distance or probability. This preliminary screening may be carried out by the use of a 'screening distance value (SDV)' and/or, where the available data permit, by evaluating the probability of occurrence of the event.

b) Relatively simple procedures may be used in a preliminary screening of sources and interacting events. The starting point is the identification of all stationary and mobile sources of potential external human induced events in the region and all possible initiating events for each source.

c) After the previous step , a screening distance value (SDV) should be determined for each particular type of source (stationary and mobile) using a conservative approach such that the effects of interacting events beyond this distance should not be considered further . The determination of the SDV should take into account the severity and extent of the event, as well as the expected characteristics of the nuclear power plant to be located at the site. These characteristics may be assumed for the early stages of siting to be those corresponding to the standard plant design. If the site is outside the SDV for the initiating event under consideration, no further action is necessary. For sources generating effects of the same nature, a further screening could be performed which would depend upon an enveloping criterion and which should exclude those sources that generate interacting events that are enveloped by those for other selected sources, even if the site is inside the SDVs for these sources.

d) For aircraft crashes, the following criteria shall be used for estimating the SDV. The potential hazards arising from aircraft crashes are taken into account if: airways or airport approaches pass within 4 km of the site; airports are located within 10 km of the site for all but the biggest airports; for large airports, if the distance d in kilometres to the proposed site is less than 16 km and the number of projected yearly flight operations is greater than $500d^2$. Where the distance d is greater than 16 km, the hazard will be considered if the number of projected yearly flight operations is greater than $1000d^2$. For military installations or air space usage such as practice bombing or firing ranges, which might pose a hazard to the site, the hazard will be considered if there are such installations within 30 km of the proposed site.

e) SDV for explosions and sources for hazardous clouds shall be 10 Km.

f) SDV for fire hazard is 2 Km.

g) A second screening criterion is based on the probability of occurrence. The limiting value of the annual probability of occurrence of events with potential radiological consequences is called the screening probability level (SPL). The SPL value for the probability of 10^{-7} per year shall be used in the design of NPP as one acceptable limit on the probability value for interacting events having serious radiological consequences. While SPL value for the probability of 10^{-6} per year shall be used for each type of events.

h) If the site is not outside the SDV for the initiating event under consideration, the probability of occurrence of such an event should be determined and compared with the specified SPL. If the probability of occurrence of the event under consideration is smaller than the SPL, no further analysis should be made.

i) Initiating events with a probability of occurrence lower than this screening probability level should not be given further consideration, regardless of their consequences. If, the probability is higher than SPL, the NPP must be protected. The events which have a defined probability of not being exceeded 10^{-6} per year will be selected for the design basis.

j) If the probability of occurrence of the initiating event under consideration is greater than the specified SPL value, a detailed evaluation should be made. This implies that the associated interacting events should be determined as well as their corresponding probabilities of occurrence. More details are described in IAEA code of practice; Safety Series No. NS-G-3.1 issued in 2002 and entitled "External Human Induced Events in Site Evaluation for Nuclear Power".

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquake in the Design of Nuclear Power Plant, Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in the Site Evaluation for Nuclear Power Plant. Safety Standards Series No. NS- G-3.1, IAEA, Vienna (2002).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Survey for Nuclear Power Plant, Safety Standards Series No.50-SG-S9, IAEA, Vienna (1983).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review of Operational Nuclear Power Plants, Safety Series No. 50-SG-O12, IAEA, Vienna (1994).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

SAFETY CONSIDERATIONS IN THE SELECTION OF NUCLEAR POWER PLANT CANDIDATE SITES IN JOHOR STATE, MALAYSIA

A.T. RAMLI, N. A. BASRI, N. Z. H. ABU HANIFAH
Department of Physics, Faculty of Science
Universiti Teknologi Malaysia
Johor, Malaysia
Email: termiziramli@gmail.com

Abstract

Nuclear power is considered as one of the best options for future energy development in Malaysia. Since Malaysia has no experience in nuclear energy generation / production, commissioning the first nuclear power plant needs tremendous effort in various aspects. The most obvious challenges are to ensure the nation's safety and to handle security issues that may arise from a nuclear power plant site. This paper aims to propose a site for nuclear power plant in Johor State, Malaysia as well as listing the possible safety challenges in the process. The site selection uses the Malaysian Atomic Energy Licensing Board (AELB) guideline document as the main reference, supported by documents from International Atomic Energy Agency (IAEA) and from various countries. Only five site characteristics are chosen as study parameters – geological features and seismic data, air dispersion analysis using meteorological data, population distribution, safety zones and emergency supports. This paper concluded that site number 2 (CS2) at Tanjung Tenggaroh, Mersing is the most suitable area for nuclear power plant in Johor state. It has the least possible risks, safety and security issues.

1. INTRODUCTION

Malaysia is in the process of deciding to use nuclear as an alternative energy source to support its future power generation. Presently, Malaysia relies on fossil sources and hydro power to generate electricity. To secure future power supply and generate clean energy, nuclear power is seen as the best solution because it generates large amount of power with minimum of carbon release to the atmosphere.

Since nuclear energy is new in Malaysia, various challenges are inevitable in the commissioning process. The most obvious challenges are issues related to nuclear installation safety. Public sentiments in Malaysia are not yet supportive towards nuclear energy due to recent global events such as the Fukushima incident in Japan and other incidents related to nuclear reactors. Other reasons that cause negative reaction towards nuclear energy are basically fear and prejudice towards radioactive material safety issues, and limited information on nuclear related activities and its development in Malaysia.

Negative sentiments toward nuclear development could possibly be changed with transparent and detailed information on the preparations to embark on the nuclear era. This paper tries to find a candidate area for NPP construction in accordance with safety requirements and without ignoring the public's wariness towards nuclear power development in Malaysia. Since public acceptance is very important, the selection procedure must minimize possible issues that may cause negative reaction from the public.

Site selection and evaluation was conducted to satisfy the safety requirements stated by the IAEA. This study refers to various documents provided by the IAEA. This study is also based on the site selection guideline published by Malaysian Atomic Energy Licensing Board (AELB) [1].

2. OBJECTIVE

This study aims to identify a nuclear power plant (NPP) candidate site in Johor state and determine the possible challenges in safety, security and safeguard issues in the selected site.

3. METHODOLOGY

AELB lists eleven (11) parameters as regulatory considerations in the selection of suitable sites for NPP (AELB, 2011). This paper considers only five (5) characteristics as the most important parameters to determine possible candidate sites. The selected parameters are:

(1) Geological and seismological characteristics.
(2) Population considerations.
(3) Atmospheric dispersion analysis using meteorological data.
(4) Safety zones allotment.
(5) Emergency supports.

Mandatory criteria and rejection criteria were listed and the areas are marked using MapInfo Professional software. Mandatory criteria for NPP in Peninsular Malaysia were listed in a study by Tenaga Nasional Berhad (TNB), stating that the NPP site must be located along coastal area, and next to large water body to meet the NPP cooling requirements in Ref. [2]. Rejected areas involve critical safety issues such as unstable surface and densely populated area. These areas are deemed unsuitable for NPP site as discussed in Ref. [3].

Areas other than rejection areas were analyzed accordingly based on the above chosen parameters. The parameters were ranked by their relative importance based on safety requirements. Table 1 shows the proposed ranks for each parameter.

For each selected candidate sites, marks will be given based on its safety supports potential and possible radiological risks. Higher mark will be given if the site has lower risk based on the evaluation for each parameter. The proposed marks are shown in Table 2.

TABLE 1. LIST OF PROPOSED PARAMETERS AND THEIR RANKS IN WEIGHTING PERCENTAGE

No.	Parameters	Sub Parameters	Sub Rank Percentage	Total Rank percentage
1.	Geology and seismicity characteristics	Geological stability Surface faulting Seismic data	10% 10% 10%	30 %
2.	Atmospheric dispersion analysis	Wind data Atmospheric dispersion simulation	10% 15%	25%
3.	Population consideration	Distance to population centre Population distribution	12% 8%	20%
4.	Safety zones allotment	Exclusion zone Low population zone	5% 10%	15%
5.	Emergency supports	Evacuation route Emergency support facilities	5% 5%	10%

TABLE 2. PROPOSED MARKS

Marks	Suitability criteria
0	Rejected
1	Avoided due to high risks
2	Avoided but with lower risks
3	Acceptable, but need safety support
4	Slightly suitable, with minimal risks
5	Suitable

The final mark for each candidate site was calculated using following formula:

Total Mark = Suitability mark (sub parameter) x Sub rank Weighting Percentage

Sites with the highest total mark were considered as the best candidate based on the 5 safety parameters / characteristics as suggested by AELB.

4. STUDY AREA

As stated in Ref. [4], Johor State is located in the South of Peninsular Malaysia. Johor is the fifth largest (18,986 km^2) in term of area and the second most populous state (3.35 million) in Malaysia. Out of 10 districts in Johor, 4 districts are identified as having potential areas for site selection – Mersing, Muar, Batu Pahat, and northern part of Kota Tinggi. Muar and Batu Pahat are located in the western region of Johor while Kota Tinggi and Mersing in the eastern side of Johor. The southern part in Kota Tinggi is to be avoided due to its closeness to Singapore.

All locations are close to coastal areas which have access to adequate amount of cooling water. Two other districts in Johor (Johor Bahru and Pontian) were also located along the coastal line, but both districts are too close to Singapore and Indonesia. It is difficult to fulfil the international requirements in terms of safety, security and safeguards.

In those four districts, areas within 10 km from coastal line are marked using MapInfo Professional software as the potential area for NPP sites. From the area, 5 candidate sites were selected and labelled (CS1 to CS5). The sites chosen were at a considerable distances from densely populated areas. Each district has at least 1 candidate site to be evaluated. Two (2) candidate sites (CS1 and CS2) were chosen in Mersing district. The potential candidate sites are shown in Table 3. The locations of the sites chosen are illustrated in Figure 1 (a) and (b).

TABLE 3. POTENTIAL CANDIDATE SITES

Region	District	Mukim	Label
East	Mersing	Jemaluang	CS1
	Mersing	Tenggaroh	CS2
	Kota Tinggi	Sedili Besar	CS3
West	Muar	Seri Menanti	CS4
	Batu Pahat	Lubok	CS5

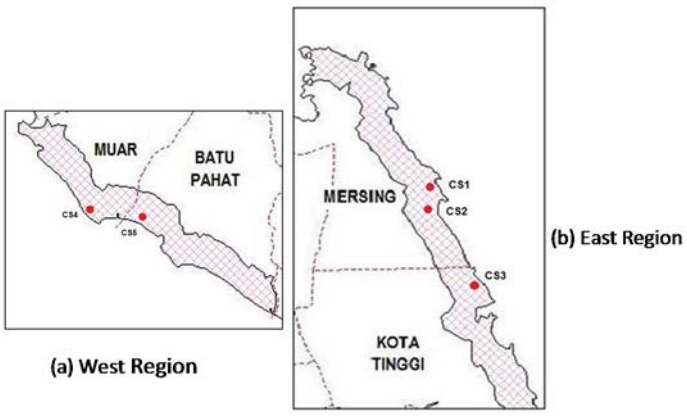

FIG. 1. Candidate Sites.

5. RESULTS

From the potential candidate sites, the evaluation process was done using ranking and marking methods as stated above. The results are shown in Table 4. From Table 4, the highest mark in suitability evaluation is given to site (CS2) located at *Mukim* Tenggaroh, Mersing while the lowest mark is the site in Seri Menanti, Muar (CS4).

6. DISCUSSION – SAFETY ANALYSIS IN SELECTION PROCESS

6.1. Geological Characteristics and Surface Stability

AELB suggested areas with competent bedrock, stable rock or dense sand area as suitable area for NPP foundation [2] to prevent events related to geological and seismological phenomena like earthquakes and surface faulting [3].

Geological map published by the Department of Geosciences and Mineral in reference [5] shows that the most stable areas are located in the centre of Johor, near the mountain ranges where granitic rocks are found. Relatively unstable areas consist of alluvial soils located near the estuaries, mangroves and beaches. There are also acceptable geological features such as clay and limestone areas in the eastern region.

There are also surface faulting areas in the inner land in the region as marked in Surface Stability Map published by the Department of Agriculture Malaysia in Ref. [6]. Geological instability and surface faulting areas in the potential candidate areas are marked as in Figure 2.

CS4 and CS5 are located in relatively unstable geological areas. The areas have Quaternary geological formation, covered by peat soils in the inner region and mangrove swamps at the coastal areas. Stable areas (granitic rocks) in the western region are too close to densely populated area, so they are considered as rejected.

CS1, CS2 and CS3 lie on more stable grounds than the sites in western region. Geological formation characteristic at CS1, CS2 and CS3 are Quaternary and Jurassic, while granitic rocks could be found in the inner land. Although the sites generally lie on stable ground, there are small relatively unstable areas in the undulating region that need to be avoided.

TABLE 4. CANDIDATE SITE EVALUATION ACCORDING TO SELECTED PARAMETERS

Parameters	Candidate Site Mark*				
	CS1	CS2	CS3	CS4	CS5
Geology and Seismicity Characteristics	1.40	1.40	1.50	1.10	1.10
Meteorological Data and Atmospheric Dispersion	0.80	0.80	0.80	0.70	0.70
Population Consideration	0.88	1.00	0.60	0.20	0.28
Safety Zones	0.55	0.65	0.45	0.35	0.25
Emergency Facilities	0.30	0.35	0.35	0.40	0.45
Total Marks	3.93	4.20	3.70	2.75	2.78

*Marks are multiplied with Sub Parameter Rank Weighting Percentage

Generally, Johor state is considered suitable for nuclear power plants in terms of geological and surface characteristics. However, certain areas are considered as relatively unstable by related agencies, due to the ground physical characteristics of the area. This weakness can be compensated using engineering and architectural designs of the nuclear power plant.

6.2. Seismological Records and Earthquake Possibilities

In a study discussed in reference [7], it stated that Peninsular Malaysia has a very low possibility of earthquake events since it did not lie on the Pacific Ring of Fire. However, Malaysia did feel the effect of high magnitude earthquake occurring in the neighbouring country, Indonesia. Malaysian Meteorological Department in reference [8] has recorded felt earthquake events and intensity in Johor. Recorded maximum earthquake intensity in Johor ranged from II to IV based on Mercalli Intensity Scale. Figure 3 shows the intensity of felt earthquake recorded from 2007 until 2009.

According to seismic records provided by the Meteorological Department, all candidate sites (CS1 to CC5) have low peak ground acceleration for felt earthquake events occurring from 2007 until 2009. This record depicts that risks from earthquake and surface faulting events are very small. However, the data must be updated regularly to ensure all possible risks from such events stay low and manageable throughout the NPP operation.

6.3. Population distribution Analysis

Density limit for NPP site selection suggested by AELB is not more than 250 people per km^2, and far from major population centres [2]. As mentioned in the study in Ref. [1], it stated that an area with more than 25,000 persons is considered highly populated, hence rejected as candidate area. A site is also rejected if the location is within 10 km distance from a major population centre.

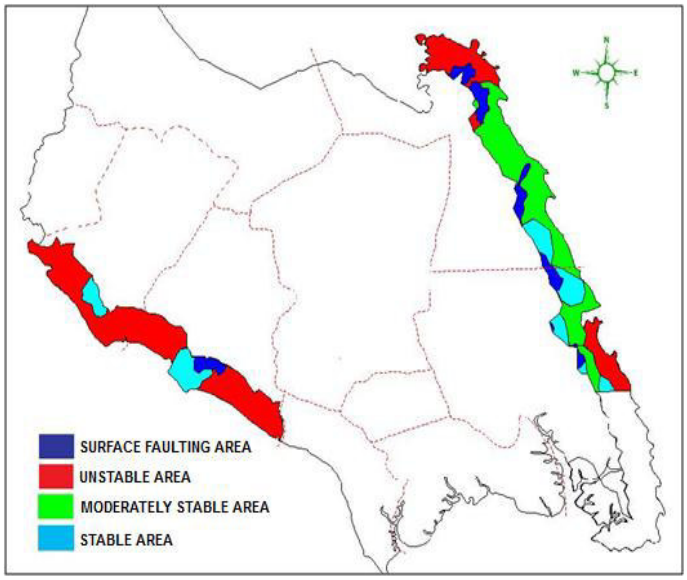

FIG. 2. Map of Geological Instability and Surface Faulting in Potential Candidate Area.

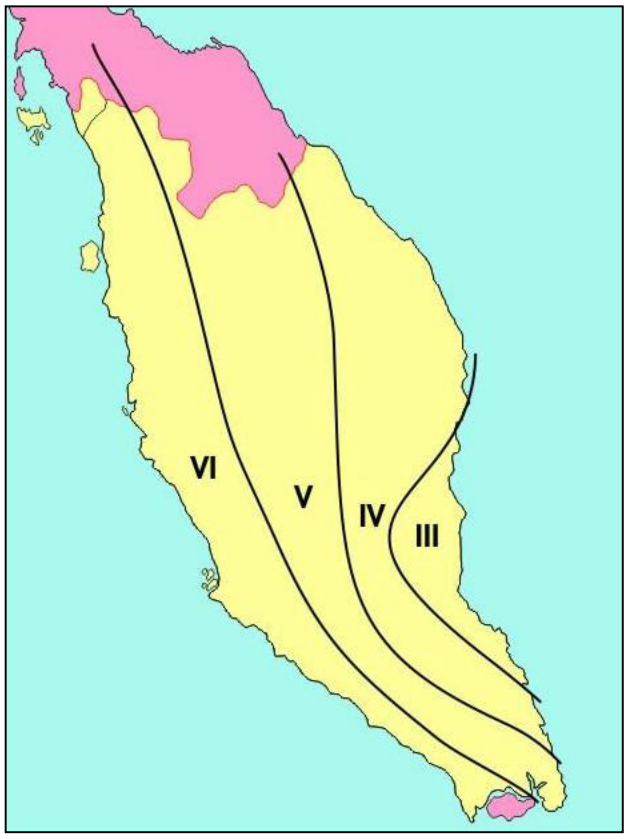

FIG. 3. Intensity of felt earthquake from 2007 to 2009.

Areas with population density of more than 250 persons per km square are marked as rejected areas. Since population distribution maps for recent census (Census Report 2010) are not yet published, the areas were marked using the Malaysia Population Density Map published in 2000. The density and distribution may changes in these 12 years, but the difference is assumed to be not too big in the potential candidate areas. The higher populated areas are shown in Figure 4.

Both sites in the western region are also located near densely populated areas. The population in CS4 and CS5 are about 11,000 and 6,660 people respectively. CS4 is located 6.7 km away from Batu Pahat town, while CS5 is located 9.7 km away from Muar town. Both towns are densely populated areas where the population density is more than 250 people per kilometre square. Meanwhile, CS1, CS2 and CS3 have much lower population distribution. The total population in the area did not exceed 25,000 people and the population density is not higher than 250 persons per kilometre square. The most dense population centre is Mersing town that has population of more than 25,000 persons.

Population data may offer both advantages and disadvantages to safety considerations in NPP site selection. Generally, better services and facilities such as transportation routes, communication and electricity grid, as well as emergency amenities such as hospital, military base and fire department can be found easily in highly populated areas, but denser population distribution may complicates safety measures and emergency planning for the area. Candidate sites with higher population density but fulfil sufficient safety criteria are more favourable than sites with low population density but not fulfilling safety criteria, as long as the population does not exceed 25,000 and the population centre distance is more than 10 km from the site as stated in Ref. [7].

6.4. Air Dispersion Analysis Using Meteorology Records

In a report stated in reference [9], climate zones in Johor are divided to two zones: Middle Eastern Zone and Western Coast Zone, according to dry and rainy season for both areas. Middle Eastern Zone covers Mersing, Kota Tinggi, Keluang and Segamat while Western coast zones cover Johor Bahru, Kulaijaya, Pontian, Muar, Batu Pahat and Ledang.

According to wind speed report for the year 2009 until mid-2011 by Malaysian Meteorological Department in reference [10], the average wind speed in the western region and eastern region is in the range from 0.3 to 1.5 m s^{-1} and 1.6 to 3.3 m s^{-1}, respectively. The maximum wind speed occurs during Northeast Monsoon from November until March in both regions. During monsoon, the wind speed will increase to the ranges from 1.6 to 3.3 m s^{-1} in the western region and 5.5 to 7.9 m s^{-1} in the eastern region.

Air dispersion analysis was conducted using simulation of radioactive dispersion utilizing meteorological records provided by the Meteorological Department. The purpose is to estimate the dose rate and dispersion distance of radioactive material through air in a case of a postulated radiological emergency in the candidate area.

The situation used in this simulation is general radioactive plume with radioactive dispersion similar to the Fukushima accident in March 2011. Radioactive material used in this simulation is caesium-137 with total activity of 10^{15} Bacquerel, which is the estimated activity of released caesium-137 during the Fukushima accident as reported in Reference [11]. Sampling time is 120 minutes, immediately after the plume was released to the atmosphere. Other variables needed in the calculation use the default values suggested in the software.

The results show that the amount of estimated Cs-137 deposition and dose rates are related to wind velocity. The deposition and dose rate is much higher at lower wind speed. This is because Cs-137 is in the form of particles and its dispersion depends on atmospheric behaviour.

Higher value of wind speed results in a wider dispersion distance and larger contaminated area. In the simulation, the contaminated area spans 80 km away from the plume's origin in less than 24 hours. At wind speed of 7.9 m s^{-1}, the dispersion arrived at 80 km distance in 3 hours. However, at this distance, the surface deposition and dose rates are smaller and did not exceed the dose limit specified by the IAEA.

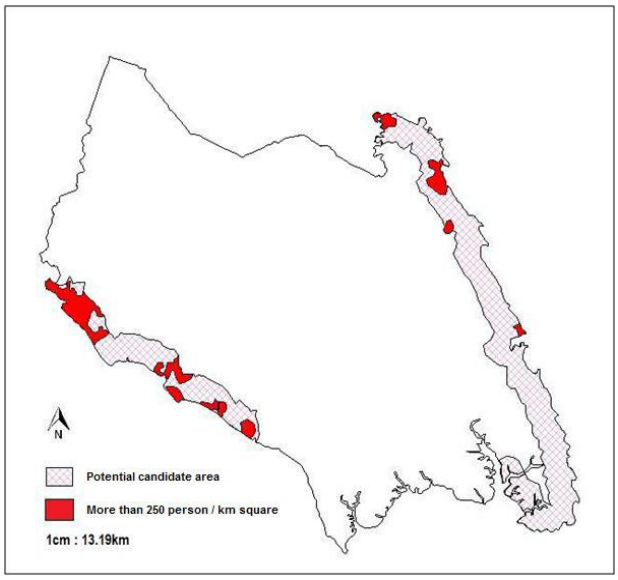

FIG. 4. Areas with more than 250 persons per km^2.

Western region has lower average wind speed and the estimated ground deposition distance for radioactive dispersion is lower so it may not reach the population centre (Muar and Batu Pahat town). However, due to the lower wind speed, the dose rate in the affected vicinity will be expected to be higher.

In eastern region, average wind speed is higher than the western region, so the deposition distance may extend further than 5 km away from the sites. The maximum wind speed in the eastern region is 3.3 m s^{-1} in non-monsoon season and 7.9 m s^{-1} in monsoon season. The estimated dose rate in a 120 minutes sampling time is lower due to the higher dilution process by the wind. Careful consideration must be taken due to wider area of estimated radiological impact at these locations.

6.5. Safety Zones Distribution and Emergency Planning Analysis

6.5.1. Exclusion Zone

AELB suggested exclusion zone and low population zone as the basic requirement for safety zoning in a candidate site. The zone size and boundary is not specifically regulated by AELB, but refers to the sizing guidance provided by United States Nuclear Regulatory Commission (USNRC).

The size of exclusion zone is determined by the simulation of radioactive air dispersion due to radioactive material release in an emergency situation similar to the Fukushima accident. The size is measured from the dispersion origin to the point where the estimated effective dose is less than 0.25 Sv in 2 hours sampling time. The distance is calculated based on AELB description of exclusion zone in Ref. [2], which is an area of such size that an individual located at any point outside this zone within two hours immediately following the onset of the postulated fission product release shall not receive a total radiation dose to the whole body in excess of 250 mSv or total radiation dose in excess of 3 Sv to the thyroid from iodine exposure.

The result of simulation for the exclusion zone size in all candidate sites gave the range between 0.7 to 1.0 km, depending on the non-monsoon and monsoon average wind speed in the area.

6.5.2. Low Population Zone

The low population zone (LPZ) is the area immediately beyond the exclusion zone as stated in Ref. [2]. In the guideline, AELB stated that simple determination of LPZ size is by fulfilling the requirement where distance to the boundary of the nearest densely populated centre shall be one and one-third times the distance from the NPP to outer boundary of the low population zone.

The LPZ size is determined by measuring the sites' distance to the nearest population centre. Using the calculated exclusion zone and the requirement by the guideline, the LPZ size for each candidate site can be determined. Figure 5 below shows the dimension of LPZ according to the requirement.

The LPZ calculation considers the nearest town to the selected site. The nearest town to CS1 and CS2 is Mersing town while the nearest town to CS3 is Sedili town. From the calculation, the LPZ distance for CS1, CS2 and CS3 are 13.5 km, 19.63 km and 6.5 km respectively. Hence, the distance to the population centre from the outer boundary of LPZ is 4.25 km for CS1, 6.27 km for CS2 and 1.9 km for CS3. From the results, CS2 has the biggest size of LPZ and it has farthest distance to the population centre from the LPZ outer boundary.

In Western region, the LPZ sizes are 7.48 km and 5.23 km for CS4 and CS5 respectively. If the distance to the population centre from the LPZ boundary were calculated, its size is too small to set up an emergency zone (CS 4 – 2.22 km and CS5 – 1.47 km).

Safety zoning also considers the population number in the region. In the eastern region, the potential area has 3,000 to 5,000 persons in each *mukim*, except Mersing town. This number gives huge advantage in setting up LPZ; hence candidate sites in the area might be selected as suitable site according to the limit proposed by AELB. In the western region, the population number is considerably higher in each *mukim* (5,000 to 25,000). The main town has more than 100,000 persons with population density of more than 250 persons per km^2. It is expected that emergency planning will have to consider more than 25,000 people in a postulated emergency, so the LPZ and safety zones in western region are harder to be alienated and possible candidate sites will be very limited.

6.5.3. Safety Support for Emergency Planning

In the site evaluation stage, suggestion for emergency planning must be made to fulfil the safety requirements by IAEA. Safety support plays important roles to overcome or reduce risks for selected sites. Hence, it is best located in or near the emergency planning zone as suggested in Ref. [12].

Hospital and fire brigade stations are examples of essential emergency support during radiological emergency to provide emergency aid to the NPP. Efficient medical support is important during radiological events, especially in treating high dose patients or acute radioactive symptoms. However, hospitals are also considered as avoidance entity in safety planning for NPP. During radiological accidents, patients in nearby hospitals must be evacuated to prevent unnecessary dose. Having a hospital near to NPP is risky, but is needed in emergency planning. Hence, it is suggested that the best location for a hospital is in the low population zone that is close to its outer boundary.

Military bases are also important to be included in emergency planning. During radiological events, military support can hasten evacuation; hence reduce fatalities and exposure to the public [7]. Other than that, military presence ensures security to the NPP facilities from events that may threaten nation's safety and security related to nuclear power plant. However, like the need of medical support from hospitals, the military base must be located within a reasonable distance from the NPP. Since military bases usually have weapons and explosives, it is too risky to be placed nearby NPP to prevent catastrophic events such as explosions or sabotage to the NPP.

The western region currently has better facilities for emergency support than the eastern region. Since the candidate sites are located near highly populated and developed areas, emergency support and evacuation processes could be very efficient in emergency situations. The transportation route and communication access is very good with reasonable number of hospitals and fire brigade stations in the region. For evacuation plans, military support is available from Kem Bakri at Muar, 21 km from CS4 and 27 km from CS5.

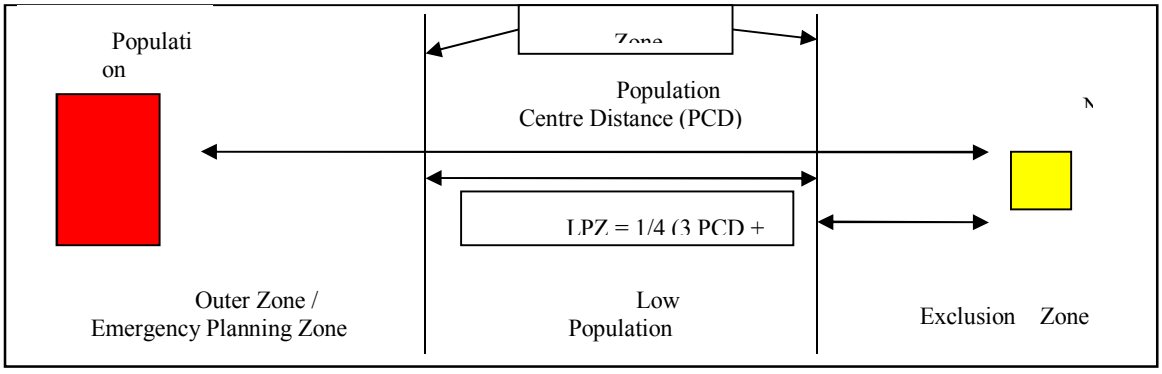

FIG. 5. An impression of safety zones dimension and lpz calculation.

The emergency and safety support evaluation for the eastern region is not as good as in the western region. Major hospitals and fire brigade stations were located at the nearest town centre; Mersing, Sedili and Kota Tinggi. The location is fairly far from the candidate sites, but at acceptable distance for emergency planning purposes. The transportation network is not as extensive as in the western region either. Alternative route may need to be constructed if the available routes are deemed to be insufficient.

7. CONCLUSIONS

It is concluded that Johor state has high potential to be candidate site for the first NPP in Malaysia. Based on AELB guidelines and IAEA requirement documents, selected candidate sites in the state are proven to be a potential site for NPP.

The candidate sites' characteristics fulfil most of basic safety requirements. Most of the identified weaknesses at the candidate sites can be overcome by engineering and architectural designs, as well as safety supports that can help reduce risks and efficiently manage the emergency situation.

In this study, site number 2 (CS2) was chosen as the most suitable site for NPP in Johor based on evaluation on the five parameters required by AELB; geological, meteorological, population distribution, safety zones and emergency planning. Further evaluation must be done referring to other parameters to ensure all requirements of AELB guidelines are fulfilled.

ACKNOWLEDGEMENT

The authors would like to thank the Ministry of Higher Education (MOHE) and Universiti Teknologi Malaysia for providing a research grant (GUP - **Q.J.130000.2526.00H70**) for this research and the International Atomic Energy Agency, IAEA for providing the conference grant for this paper.

REFERENCES

[1] AHMAD, M.N., et al., Nuclear Power Plant Siting Guideline for Peninsular Malaysia, Proceeding of the 2nd International Conference on Advances in Nuclear Science and Engineering, November 3 – 4 2009, USA, American Institute of Physics, (2010) 311 – 316.

[2] ATOMIC ENERGY LICENSING BOARD, Guideline for Site Selection for Nuclear Power Plant, Dengkil, AELB Guideline LEM/TEK/63, (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations. IAEA Safety Standards, Safety Requirements No. NS-R-3, IAEA, Vienna (2003).

[4] DEPARTMENT OF STATISTICS MALAYSIA, Laporan Banci Penduduk 2010, Kuala Lumpur, Jabatan Perangkaan Malaysia, (2010).

[5] DEPARTMENT OF GEOSCIENCES AND MINERAL, Geological Map of Peninsular Malaysia 2000, Kuala Lumpur: Jabatan Geosains dan Mineral, (2000).

[6] DEPARTMENT OF AGRICULTURE MALAYSIA, Peta Tinjauan Tanah-Tanih, Putrajaya: Jabatan Pertanian Malaysia, (2008).

[7] DEPARTMENT OF AGRICULTURE MALAYSIA, Peta Tinjauan Tanah-Tanih, Putrajaya: Jabatan Pertanian Malaysia, (2008).

[8] BASRI, N.A. AND RAMLI, A.T., Selection of Possible Candidate Area for Nuclear Power Plant in Johor - Malaysia, Journal of Nuclear and Related Technologies, V 9(1), June (2012), 56-63.

[9] MALAYSIAN METEOROLOGICAL DEPARTMENT, Seismic and Earthquake Data (Johor), Putrajaya, Malaysia: Jabatan Meteorologi Malaysia, (2011).

[10] DEPARTMENT OF FORESTRY JOHOR, Summary of the State of Johor Forest Management Plan for the Period between 2006 – 2015, Johor: Jabatan Perhutanan Malaysia, (2010).

[11] MALAYSIAN METEOROLOGICAL DEPARTMENT, Meteorological Data (Johor) 2009 – 2011, Putrajaya, Malaysia: Jabatan Meteorologi Malaysia Data, (2011).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Fukushima Daiichi Status Report 28, June 2012, IAEA, Vienna (2012).

[13] SOURAV. A., et al., Monograph on Siting of Nuclear Power Plants, India: Atomic Energy Regulatory Board, (2005).

DEFINING A LIST OF ACCIDENTS TO BE CONSIDERED AS A FIRST STEP OF FORGING EFFECTIVE LEVEL 4 OF DEFENSE-IN DEPTH

M. LANKIN
Scientific and Engineering Center for Nuclear and Radiation Safety,
Moscow, Russian Federation
Email: lankin@secnrs.ru

Abstract

Russian national regulatory documents require consideration of beyond design basis accidents (BDBAs) while organizing defence-in-depth for nuclear power plants. Consideration of BDBAs in plant design analysis forms the basis for development accident prevention and mitigation strategies. Since sheer quantity of possible beyond design basis accidents is limitless, we face a necessity of working out selection criteria for choosing scenarios of such accidents to be taken into consideration while assessing adequacy of Level 4 of Defence-in-Depth for NPPs. This paper presents possible algorithm for defining a list of beyond design basis accidents that are to be taken into account for NPPs. Developing such a list is to include examination of the following criteria: a) Representativity of set of scenarios covered by the list (representativity to be assessed from the point of view of organizing emergency response actions); b) Cumulative occurrence probability of the scenarios not covered by the list (this probability should be low); and c) Necessity to cover scenarios recommended by current international state-of the art practices.

1. INTRODUCTION

In accordance with the Fundamental Safety Principles [1] to ensure that NPP is operated so as to achieve the highest standards of safety that can reasonably be achieved, the following measures are to be taken:

a) Restriction of the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation (in order words, minimization of probability than an accident may occur).

b) Mitigation of the consequences of such events if they were to occur.

Traditionally, NPP safety was assessed for postulated initiating events in order to prevent them from progressing to severe accidents or to mitigate their consequences, as appropriate. Later on, as defence-in-depth concept was being introduced and developed, requirements for beyond design basis accidents analysis and implementation in an NPP design of technical and organizational measures of controlling such accidents were being formulated.

Current operating Russian General Regulations on Ensuring Safety of Nuclear Power Plants OPB-88/97 [2] state that tentative list of beyond design basis accidents (BDBA) including initiating events, sequence paths and consequences shall be specified in regulatory documents for each type of reactor. They shall include representative scenarios with severe consequences for planning emergency response. The final lists of BDBAs, their realistic (not conservative) analysis containing assessment of probabilities of BDBA accident sequence paths including severe accidents, consequences of BDBA, functioning of safety systems shall be presented in the NPP Safety Analysis Report.

If the analysis of BDBA consequences do not confirm that “estimated probability rate of limiting emergency release did not exceed 10^{-7} per year criterion is met”, it would be necessary to provide in the design additional technical measures for accident management for the purpose of mitigating their consequences.

Thus, Russian regulatory approach to account for a BDBA in an NPP design consists of the following:

a) Representativity (from the point of view of the planned emergency actions) of the

accidents to be included in the provisional and final list of BDBA for the NPP must be ensured.

b) Probability of beyond design basis accidents should be evaluated, including those leading to large radioactive releases and additional technical measures of accident management provided for in case probability of exceeding of Large Release Frequency target regulatory value.

Following these requirements will ensure compliance with the abovementioned Fundamental Safety Principles [1].

2. STEPS OF THE SELECTION ALGORITHM

How, according to the abovementioned requirements, should beyond design basis accidents be selected for taking into account in an NPP design?

Regulatory documents used to give no instructions in this respect. This paper describes Methods (see [3]) presenting selection algorithm for beyond design basis accidents scenarios.

First of all, Methods [3] introduced a term "beyond design condition" (by analogy with "design extension condition", mentioned in requirement 20 of SSR-2/1 standard [4]) as a wider one, compared to the term "beyond design basis accidents" used in the national regulatory documents. Beyond design conditions are defined as breach of NPP normal operation (both developing and those not developing into an accident) caused by the initiating events, not accounted for by the design accidents or breach of NPP operation accompanied by additional equipment failures compared to the design accidents, as well as by implementation of erroneous personnel decisions.

Selection algorithm, proposed in [3], is presented as a scheme in Figure 1.

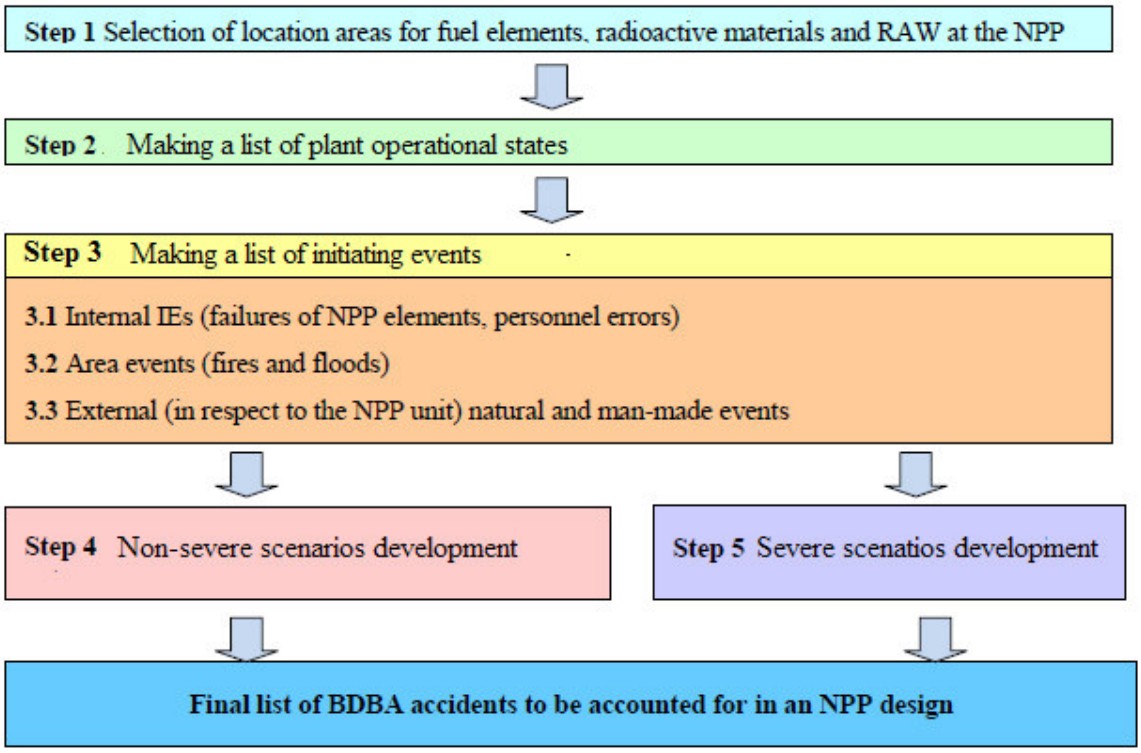

FIG.1. Series of steps in making a list of "beyond design conditions".

According to the algorithm, several consecutive stages (steps) are being carried out. First of all, in step 1, those NPP locations where an accident, including a beyond design basis one, might occur, are being individuated. Then, in step 2, NPP operational states are being differentiated on the basis of possible sets of BDBAs. Next in step 3 possibly the most comprehensive list of initiating events - breaches in normal operation that could develop into an accident is drawn. At this stage internal initiating events triggered by failure of NPP components or personnel errors are being analyzed: step 3.1, area initiating events - fires and floods - step 3.2, external hazards of natural and man-made origin - step 3.3. The next steps of making a list of BDBAs are different for accidents (conditions) not developing into the stage of severe beyond design basis accidents on the one hand, and severe BDBAs, on the other.

In step 4 safety functions and their NPP systems, necessary for each of the initiating events (groups of events) are identified, frequencies of accident sequences are calculated and non-severe accident sequences (combinations of initiating events, events of safety function success or failure, as well as other events) to be included to the list of beyond design basis accidents are being specified. In step 5 a separate analysis is carried out in order to identify severe accidents to be included in the BDBA list.

3. STEP 1 - SELECTION OF LOCATION AREAS FOR FUEL ELEMENTS AND RADIOACTIVE MATERIALS

It is necessary to mark all the NPP locations, where fuel elements can be operated, stored and transported, as well as locations for radioactive materials and radwaste. Possible locations are: reactor cores, fresh and spent fuel storage facilities, transportation casks and containers, nuclear material installations, Solid and Liquid Radwaste storages, nuclear waste handling facilities. For each of the abovementioned locations it is examined whether events, classifiable as “accidents” might occur in them. NPP location areas for fuel elements, radioactive materials and RAW with such characteristics are included into the list of BDBAs to be analyzed. This process is represented as a scheme in Figure 2 below.

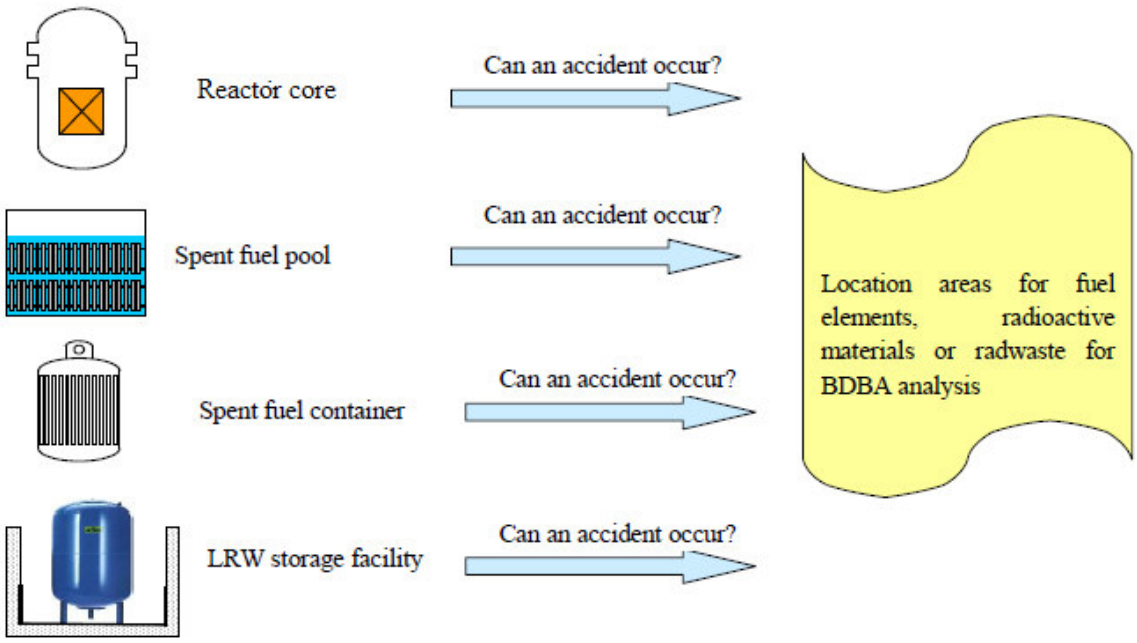

FIG. 2. Selection of location areas for fuel elements and radioactive materials.

4. STEP 2 - MAKING A LIST OF PLANT OPERATIONAL STATES

Accident sequence can be characterized by a combination of events: plant operational state, initiating event (NPP equipment failure, personnel errors or external hazard, which caused initial plant operation failure), events of successful or unsuccessful completion of safety functions (successful operation or failures of plant systems and components, errors or erroneous decisions of personnel and, generally, other events, for example, environmental parameters).

It is necessary to make a list of different possible plant operation states for each of the location areas of fuel elements, radioactive materials and RAW, identified in the previous step. Thus, for a reactor facility, such states may include operation at full and low power levels, with total and partial amount of operating primary loops, different states with a subcritical reactor ("hot shutdown", "cold shutdown", "maintenance shutdown", "refueling outage", reactor facility heat up and cooldown states).

Plant operational states differ both in sets of possible initiating events that cause breaches from normal operation (accidents) and in availability of plant safety systems. Divergences in IE nomenclatures and in availability of safety systems result in the fact that for different operational states, included in the abovementioned list, different sets of beyond design conditions (beyond design basis accidents) are possible. Figure 3 below illustrates the process of defining operational states on the example of a reactor facility.

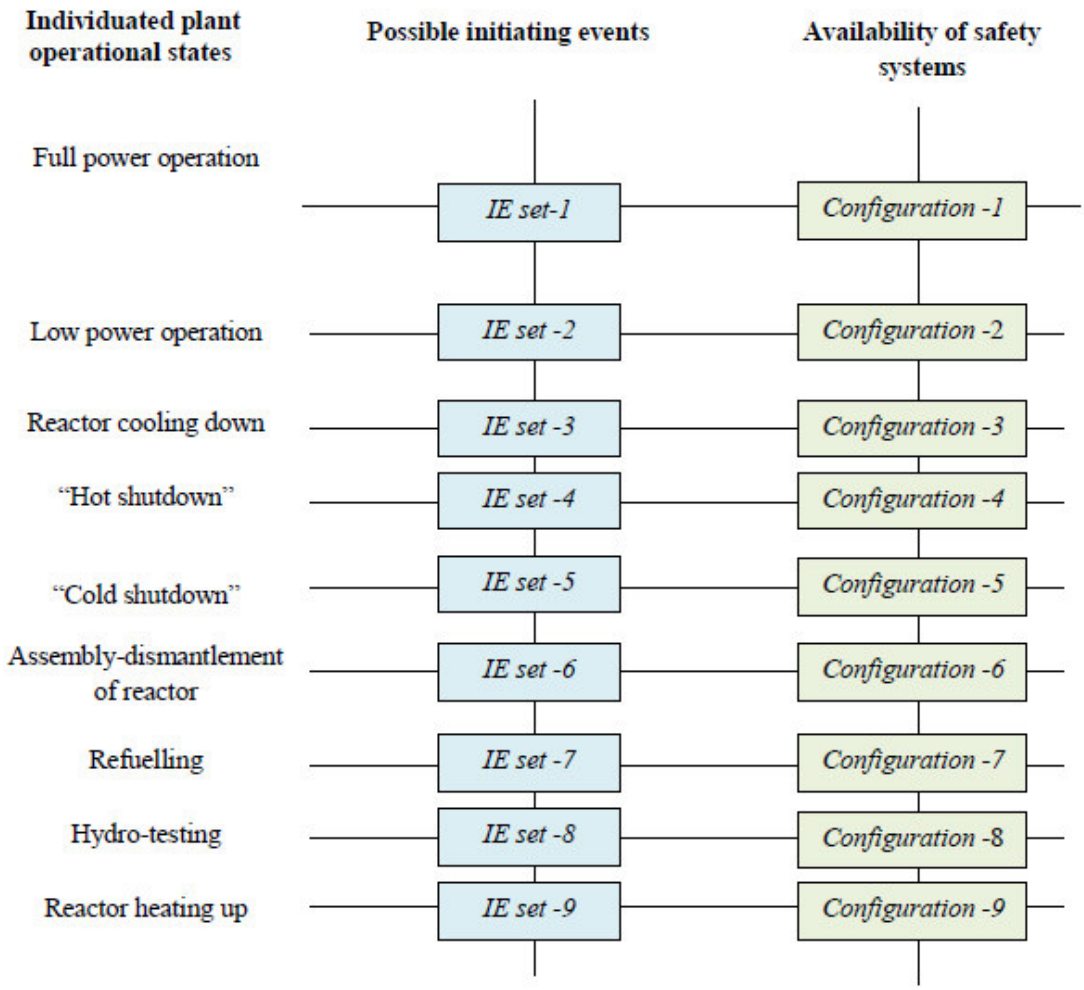

FIG. 3. Selection of plant operational states (on the example of a reactor facility).

5. STEP 3 - MAKING A LIST OF INITIATING EVENTS

Any accident, including a beyond design basis one, has an initiating event as a mandatory attribute. As a result, a guarantee that a list of beyond design basis accidents (conditions), included in the final BDBA list would be complete and representative consists of drawing the most comprehensive list possible of initiating events. A separate list of initiating events is made for each of the location areas of fuel elements, radioactive materials and RAW, defined in step 1 and another separate list for each of the plant operational states, defined in step 2.

For the event to be included in the list of initiating events, it must absolutely comply with two conditions:

- the event interrupts normal plant operation; and
- the event requires plant system and/or personnel intervention in order to prevent it from developing into an accident, or event directly leading to an accident.

The following types of initiating events are to be accounted for: internal initiating events (plant elements failures, personnel errors), area initiating events (area fires and floods), and external events of natural and man-made origin.

When making a list of internal initiating events, the following elements must be implemented: analysis of failure modes and their consequences for the plant components and systems, in the course of which influence on plant operation of failures of different types, is analyzed system by system; deductive analysis (by means of Master Logic Diagram or other methods), taking into consideration IE lists from the previously accomplished safety analyses, including probabilistic safety analyses, as well as summarized IE lists from authoritative national and international sources; operational experience of the analyzed or similar plants.

When defining fires and floods to be taken into account, fire (flood) consequences for each of the plant designated fire (flood) areas are being analyzed. Besides, probability of fires and floods occurring in several areas simultaneously is being evaluated on the basis of operational experience.

When selecting external hazards of natural and man-made character, the course of actions is as follows:

- each of the factors of natural and man-made character, enumerated in the regulatory nomenclature (e.g. in [5]) is analyzed from the point of view of whether a possibility exists that hazard sources, presented in the plant area could afflict it to the extent that normal plant operation would be interrupted and that plant systems and/or operator interference might be required in order to prevent this external hazard from developing into an accident. All the hazards, dependant on the analyzed one are also taken into consideration;
- a possibility of simultaneous adverse impact of several factors is analyzed in order to identify those cases, when such simultaneous impact results in more severe consequences than impact of each of the factors, taken separately. For this scope a matrix of joint impact of external factors developed on the basis of [6] could be applied; and
- if for the same natural (man-made) factor plant reaction (degree of impact and extent of reactions on the part of the plant systems and personnel) differs depending on the intensity of the said factor, then external hazards, corresponding to the same factor but with different intensity and leading to field trouble of different magnitude and requiring different plant system and personnel reactions are included into the IE list as independent events (for example, seismic forces of different magnitude may be included in the list as independent initiating events).

6. STEP 4 - DEFINING REQUIRED SAFETY FUNCTIONS AND WAYS OF THEIR IMPLEMENTATION FOR NON-SEVERE BEYOND DESIGN BASIS CONDITIONS

For each of the events (sets of events) individuated in the previous steps, a list of safety functions is defined, be implemented in order to avoid a developing BDBA into a severe accident stage. Accidents which cannot be prevented from developing into a severe stage, as well as other beyond design basis accidents after they have developed into a severe stage are analyzed for being included into the final BDBA list separately (step 5 below).

The following actions should be implemented:

a) all the failures, triggered by the initiating event are individuated and then examined jointly with the initiating event itself;
b) for each initiating event a set of safety functions and ways of their implementation, allowing to avoid an accident developing into a severe stage is defined. An example of safety functions and ways of their implementation for a VVER-type reactor facility is presented below in Table 1;
c) initiating events for which it has been established that they require implementation of the same set of safety functions performed by the same systems with the same requirements, the same personnel actions, performed in similar conditions and for which the same availability of systems, performing safety functions, is established, are grouped together and examined as a single set of initiating events;
d) for each group of initiating events (or initiating event, not making part of any group) combinations are made: “initiating event” + "way K failure for safety function N". Combinations are made for each safety function if its necessity for the analyzed IE group has been established at the previous step (see b). Only one safety function is included into each combination;
e) in presence of Level 1 PSA model, realization frequencies of the abovementioned (d) combinations of events are being evaluated. Additional combinations are being made by adding to the already existing combination failure events of other safety functions or failure events of other ways of performing the same safety function, failure of which already makes part of the analyzed combination. If realization frequency of the newly formed combinations exceeds threshold limit value (e.g. ~10^{-6} 1/year and above), such combinations are left for further examination, meanwhile combinations with lower frequencies are screened out. If any of the newly-formed combinations still have significant rate of occurrence, the process of adding new failure events of safety functions (or failure events of ways of performing SF) to the combinations should be continued[1];
f) it is necessary to make sure that for each of the combinations of events, formed according to d) and e), a possibility is not excluded that there might be such an algorithm of plant systems operation and personnel course of actions, that would prevent the accident from developing into a severe stage or, at least, would considerably postpone such development. Combinations, not meeting these requirements, are excluded from examination and analyzed separately in step 5 (see below);

[1] This part can be omitted in absence of Level 1 PSA model or in a situation when initiating events are not covered by the available PSA model. For example, if the PSA model examines only internal initiating events and does not cover fires and floods, this part will not be performed for beyond design accidents (conditions), connected with fires and floods corresponds to the regulatory target probabilistic criterion and to decide whether a plant disposes of enough technical and organizational means of managing a BDBA.

g) it is necessary to make sure that combinations of events, formed according to d) and e), include accidents, not classified as severe, but recommended to be accounted for in BDBA by Russian regulatory documents and international standards, reflecting up-to-date concepts in the matter (ATWS accidents, plant blackout, etc.); and
h) all combinations of events, created according to d) and e) (including specifications, introduced according to f) and g), are to be included into the final list of plant beyond design basis accidents (beyond design conditions).

Thus, the approach, described above, ensures that for beyond design plant conditions, not making part of severe accidents, the only scenarios, not covered by the list of design and beyond design accidents, are those with extremely low probability.

7. STEP 5 - ACCOUNT OF SEVERE ACCIDENTS

Severe accidents are to be examined separately in order to decide whether they should be included into the final BDBA list. For the purpose of developing suitable technical and organizational measures of managing accidents and mitigating their consequences and in order to guarantee regulatory requirement of representativity of a set of severe accidents, included in the final BDBA list, it is necessary to make sure that the aforementioned list includes all plant states, distinguished from each other by the implemented accident management strategy. At this it is not important which emergency sequence caused the plant to enter such state.

For this scope the following actions can be implemented:

a) making a list of safety functions, physical barriers and means of their protection, whose state influences action strategy of managing accidents and mitigating their consequences;
b) for each of safety functions, physical barriers and means of their protection, individuated in accordance with paragraph a), a gradation of states is worked out - from total effectiveness of safety function (barrier, means of barrier protection) to total ineffectiveness, in such a way that different gradations of the said states would require different strategies of managing beyond design basis accidents;
c) nomenclature of safety functions, physical barriers, means of protection of physical barriers as well as nomenclature of gradations of states of the said objects is represented as a matrix (example of such a matrix for WWER-type reactor unit is given in Table 2 below);
d) all possible combinations are made of states (and their combinations) of safety functions, physical barriers and means of protection of physical barrier, included into the matrix, created in accordance with paragraph b). From the resulting multitude of combinations are excluded those, containing incompatible gradations of states (for example, a combination of events “reactor vessel damage” and “possible pressure increase in the primary circuit to the critical value” would be incompatible).
e) it must be controlled that among the analyzed combinations there are plant states, connected with severe accidents and recommended by the national regulatory documents (e.g. in [7]). If need may be, a combination set is completed accordingly;
f) if the total number of the analyzed combinations, received in accordance with paragraph d) (and specified in accordance with paragraph e) is too big, it is possible to group some combinations together with attributing to this resulting group a “paramount” plant state;
g) final BDBA list must include all combinations of gradations of safety functions, physical barriers and means of protection of safety barriers, identified as a result of paragraphs d), e) and f) being implemented jointly.

Thus, the final BDBA list would include all severe accidents scenarios, severe plant states, or those that require different strategies (actions) of accident management, by this way the requirement of representatively of the BDBA list is being fulfilled.

8. CONCLUSIONS

The presented Methods [3] include a formal algorithm of making a BDBA list, which comprises both severe accidents and those not developing into a severe stage. A list, drawn according to the proposed Methods, covers accidents, caused by all possible types of initiating events: personnel errors, failures of systems and equipment, fires and floods, external hazards of natural and man-made character. Making a final list of BDBA following the presented algorithm is possible both in presence of a full-scale PSA for the analyzed NPP and when there is only partial PSA available. Making a list of beyond design basis accidents in compliance with the presented Methods meets the requirements for representativity of the accounted scenarios for planning emergency actions of the national regulatory documents and is in line with the modern international view on accounting for accidents in a NPP design. This forms solid basis for construction Level 4 of NPP Defence-in-Depth.

TABLE 1. EXAMPLE NOMENCLATURE OF SAFETY FUNCTIONS AND WAYS OF THEIR IMPLEMENTATION (FOR A WWER-TYPE REACTOR) [3]

Safety function	Way #	Method of safety function implementation
Reactor subcriticality	1	Mechanical Control and Safety System (automatic)
	2	Mechanical Control and Safety System (operator)
	3	Extra borating system (operator)
	4	Chemical and volume control system + borated water system (operator)
Maintaining water inventory in the primary circuit	5	Core flooding system (passive)
	6	Emergency cooling system for high-pressure zone (automatic)
	7	Emergency cooling system for high-pressure zone (automatic)
	8	Chemical and volume control system (operator)
Primary circuit heat transport via steam generators	9	Main (or emergency) feedwater system + main condensate system + BRU-A (automatic)
	10	Main (or emergency) feedwater system + main condensate system + BRU-A, SG SV (automatic) + demineralized water supply (operator)
...	11	...
...	12	...

TABLE 2. EXAMPLE NOMENCLATURE OF STATES OF SAFETY FUNCTIONS, PHYSICAL BARRIERS AND MEANS OF PROTECTION OF SAFETY BARRIERS FOR THE PURPOSE OF MAKING A REPRESENTATIVE LIST OF SEVERE BDBAS FOR A WWER REACTOR FACILITY [3].

#	Safety function, physical barrier or means of protection of physical barrier	Gradation of states of safety function or physical barrier (means of protection of physical barrier)			
		A	B	C	D
1	Core subcriticality	Safe	Possible exit out of subcritical state. Means and procedures, compensating input of positive reactivity, are available.	Possible exit out of subcritical state. Means and procedures, compensating input of positive reactivity, are not available.	-
2	Core cooling	Cooled geometry of reactor core is intact	Cooled geometry of reactor core is damaged - formation of corium	-	-
3	Integrity of primary circuit	Primary circuit is intact	Primary circuit is damaged, break does not exceed a small break size	Primary circuit is damaged, break does not exceed a medium break size	Primary circuit is damaged, break coincides with or exceeds large break size
4	State of containment isolation valves	Isolation valves are intact or closed	Isolation valves are in open and uncontrollable states	Isolation valves are damaged	-
5	…	…	…		

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[2] General Regulations on Ensuring Safety of Nuclear Power Plants. OPB-88/97. Moscow (1997).

[3] Methods of Developing a List of Beyond Design Basis Accidents to Be Considered in an NPP Design. SEC NRS Report. Moscow (2011).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

[5] Nomenclature of External Hazards of Natural and Man-made Origin and Their Impact on Nuclear Energy facilities, NP-064-05, Moscow (2005).

[6] Michael Knochenhauer Pekka Louko. Guidance for External Events Analysis, SKI Report 02:27, Stockholm (2003).

[7] Requirements for Content of Safety Analysis Report for NPPs with WWER-type reactor, NP-006-98, Moscow (1998).

ADVANCES AND CHALLENGES IN THE IMPLEMENTATION OF DID IN SITING, DESIGN, AND CONSTRUCTION OF NUCLEAR INSTALLATIONS IN VIETNAM

H.A. NGUYEN
Vietnam Agency for Radiation and Nuclear Safety,
Hanoi, Vietnam
Email: nhanh@varans.vn

Abstract

Vietnam is embarking on a development of a nuclear power program. The main focus is now on the initial 1000 MWe x 2 units of the nuclear power plant in Ninh Thuan province. Now, the nuclear projects of Vietnam are in the phase of siting approval and investment projects approval. The design assessment will be performed in 2013-2014; the construction and installation will be performed from now until the operating licensing is obtained in 2020-2021. With state of development of a nuclear power program in Vietnam, this paper only focuses on advances and challenges in the implementation of Defence in Depth (DID) in siting, design, and construction of nuclear installations in Vietnam.

1. INTRODUCTION TO STATE OF VIETNAM

1.1. Ninh Thuan first nuclear power plant

The first Nuclear power plant (nuclear power) proposed to be built in Vietnam [1] is a light water reactor with the technology from Russia (probably VVER-1000/AES-91 or VVER-1000/AES-92, model 2006, etc.). This type of reactor has different characteristics from the European or American technology prevailing in the world with 4 horizontal steam generators, which are designed according to the safety standards of Russia (OPB-88/97, PBY 74 -04, SP-AES-79) associated with additional standards of EU and some other safety standards.

In terms of technology, this nuclear power generation III has been improved by the Russia State Atomic Energy Corporation (ROSATOM). The improvements are based on nearly 20 years of experience in operating nuclear power generation II, design evaluation results, and summary of safety measures of the international safety agencies during more than 10 years after the Chernobyl accident. In addition to the improvements of ROSATOM, more advanced techniques such as control systems (I & C of SIEMENS), hydrogen recombiners (AREVA), core catcher, boron emergency pumping system, residual heat removal system, water storage systems complement, passive and active safety systems, particularly European-American safety culture has been deployed in the design of nuclear power VVER-1000/AES-91, VVER-1000/AES-92 and AES2006.

For safety, this type of nuclear power reactor has mostly met the safety standards of developed countries in Europe and America. Probabilistic safety assessment (PSA) has been applied in all phases of the design process, based on two test programs "Project 1.4 of the TACIS-91 Programme" and "NOVISA Project". However, it is necessary to note disadvantages of the current design, such as: i) In the process of design and construction, quality assurance is not European-American standards, ii) Lack of verified operating procedures in the case of incidents.

After the Chernobyl disaster (1986), the nuclear safety agencies in the world such as United States Nuclear Regulatory Commission (USNRC), the Institute of Radiation Protection and Nuclear Safety in France (IRSN), the regulatory body of German (GRS), the regulatory body of Russia (Rostechnadzor), International Atomic Energy Agency (IAEA) has coordinated together in order to evaluate the design of Russian nuclear power technology under their standards of nuclear safety, and proposed some improvements on design to ensure safety.

In 2006, the design of VVER-1000 has been certified by EU. However, due to the VVER-1000 reactor technology having been commercialized in many countries, including some countries in the European Union (EU), the evaluation of the design characteristics and requirements about the safety of this reactor has been conducted by a number of organizations in Europe in order to meet the requirements of safety and reliability.

For technology selection for the first NPP in Vietnam, we have to consider all these factors and the new changes which ROSATOM has applied through the evaluation of the safety analysis report (SAR) submitted by the utility to the licensing approval authorities.

1.2. Ninh Thuan second nuclear power plant

On 31/10/2010, Prime Minister Nguyen Tan Dung has declared Japan will be partner of Vietnam in building the second NPP. Japan is one of the leading countries in research and development in the nuclear energy field. In recent years, Japan has cooperated and supported Vietnam in various fields related to research, development, training and use of nuclear energy for peaceful purposes, especially to support Vietnam in preparing for nuclear power development program. Up to now, it is not clear which technology will be imported from Japan; however, the choice of technology will be more specific as soon as the recommendation report from Japan is completed.

Currently, Japan possesses advanced nuclear technology for both pressurized water reactors (PWR) and boiling water reactors (BWR). Japanese nuclear technology has achieved a high degree of reliability and proven through 45 years of experience in operating PWRs and BWRs. Japanese technology ensures safety through the application of many modern and proven technologies, such as assessment and design technology in earthquake-resistance, technology in preventing, minimizing pipeline rupture , steam generator technology, optimized design factory's premises, etc.. However, after the serious accident that occurred at the Fukushima (a second generation reactor) due to earthquake and tsunami in Japan, the design safety issues must be paid special attention to for the nuclear power project in Ninh Thuan in Vietnam (Although, Ninh Thuan nuclear power technology would be more advanced than Fukushima nuclear power technology).

Figure 1 shows the site of the first and the second NPP of Vietnam.

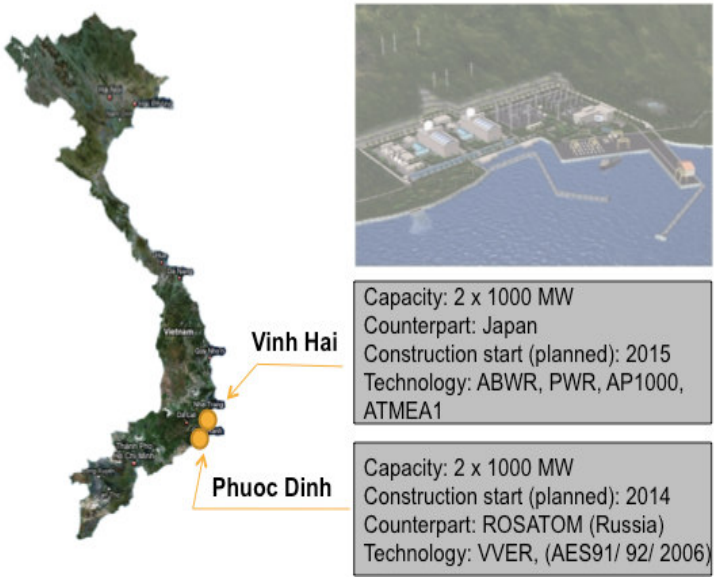

FIG. 1. Site of the first and the second NPPs.

2. ADVANTAGES

2.1. Legal framework

Vietnam is establishing the Safety Infrastructure for a Nuclear Power Program including governmental, legal and regulatory framework. Concerning the legal framework, some legal documents such as Decree, Circular and Standards has just been issued for site approval, FS approval and construction permit phases. These legal documents were mostly based on IAEA requirements and guides. In general, the needs for effective Defence in Depth (DID) implementation such as: number of measures, including robust physical barriers, redundant and diverse safety systems, strong physical security, and emergency response readiness are mentioned [2, 3]. The list of regulatory documents that have been issued for Site, FS and Construction approval phase is outlined below [4-11].

2.1.1. For Pre-FS and Site Approval

- Decree No. 70/2010/ND-CP dated by The Government on detailing and guiding a number of articles of the Law on Atomic Energy regarding nuclear power plants.
- Circular No. 13/2009/TT-BKHCN dated 20th May, 2009 by Minister of Science and Technology guiding on preliminary nuclear safety assessment for site selection for nuclear power plants in the investment decision stage (Pre-FS stage).
- Circular No. 28/2011/TT-BKHCN dated 28th November, 2012 on nuclear requirements for nuclear power plants site.
- Circular No. 29/2012/QĐ-BKHCN dated 28th December, 2012 on format and content of SAR for NPP site approval.
- Nuclear Safety Standards 6941: 2013 – External Human Induced Events in Site Evaluation for Nuclear Power Plants (based on NS-G-3.1).
- Nuclear Safety Standards 6942: 2013 - Dispersion of Radioactive Material in Air and Water and Consideration of Population Distribution in Site Evaluation Nuclear Safety (based on NS-G-3.2).
- Nuclear Safety Standards 6943: 2013 – Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Power Plants Nuclear Safety (NS-G-3.4).
- Nuclear Safety Standards 6944: 2013 – Seismic hazards in site evaluation for nuclear installations (based on SSG -9).
- Nuclear Safety Standards 6945: 2013 – Geotechnical aspects of site evaluation and foundations for nuclear power plants (based on NS-G-3.6).

2.1.2. For FS Approval and Construction Permit phases [4, 12, 13]

- Decree No. 70/2010/ND-CP dated by The Government on detailing and guiding a number of articles of the Law on Atomic Energy regarding nuclear power plants;
- Circular No. 30/2012/QD-BKHCN on requirements on nuclear safety of design of NPPs;
- Circular on the format and content of SAR for FS approval and Construction Permit phases to be issued in 2013.

2.2. International consultants

Vietnam Electricity Group, the owner of the nuclear power plant in Ninh Thuan 1 and Ninh Thuan 2 Vietnam Electricity Group will submit to the Government for siting approval and investment projects approval. The Ministry of Science and Technology will conduct nuclear safety evaluation of the submitted documents.

Safety assessment for site approval and approval of investment projects is a complex task and completely new in Vietnam. This task requires high demand for qualified staffs that Vietnam cannot fulfil alone.

Besides, for the legal framework of the first nuclear power plant, Vietnam cannot produce all the necessary documents to meet the requirements for nuclear power program in this phase. Therefore, we must apply the appropriate guidelines and technical standards of countries that export nuclear technology. The full understanding and application of a large amount of guidelines, standard and criteria for the evaluation of safety is not a simple task to accomplish.

According to the IAEA expert's recommendations and the experiences of countries that possess nuclear power plants, Vietnam Government decided to hire international consultants to support the majority of work related to safety assessment activities of the first nuclear power plants.

In terms of policy, Vietnam will establish a joint bid invited international consultants to assess the Feasibility Study report (FS) of Ninh Thuan nuclear power plant (basically, although site approval and FS approval is two separate stages, according to Vietnam's rules, in general, the profiles of FS phase will include the profile of site approval. Additionally, for each nuclear power plant, EVN will submit to MOST / VARANS both sets of reports. Therefore we only referred to a unified bid evaluation reports for both phases (FS approval and siting approval).

It is expected that there are 4 packages of content: (1) selecting technology (for both Japanese and Russian technology), (2) safety analysis report (including content related to site investigation), (3) report the environmental impact assessment, and (4) economic issues and other problems.

The hiring of international consultants is one of the advantages for the implementation of an effective DID during the site selection, design review and construction. With experience and knowledge of experts, the elements needed for the implementation of DID will be made to ensure a full and accurate assessment. In additional, by learning from international experts, Vietnam's staff competence will gradually improve and step by step increase the rate of self-assessment for the next nuclear power plant.

2.3. Human resources

During the past 30 years, a generation of nuclear experts had conducted meticulous and persistence preparation to initially build the foundation of nuclear technology in Vietnam. From 1975 to 1990, Vietnam had a team of 500 scientists in nuclear technology trained domestically and abroad. But after the Chernobyl accident, all research and training plans of our country have been halted. With delays longer than 20 years, the number of actively working experts became limited with lack of experts in the younger generation; therefore, the training of human resources for nuclear energy field became very important.

In that situation, May 8/2010 Government of Vietnam declared 10 years of training project in human resource in the field of nuclear energy along with students training plan in advanced countries such as Russia, Japan, France, Hungary and the United States. Particularly

in the last 3 years we have sent 200 students to Russia and other countries to study both short-term and long-term in nuclear energy and nuclear power.

More recently, in early 12/2012, the Ministry of Education and Training has published the Draft Decision of the Prime Minister stipulated preferential and support policies for the training for students in the field of atomic energy and nuclear engineering.

3. CHALLENGES

3.1. Legal framework

The authorities have issued some legal documents related to the implementation of DID. However, for these document mentioned in general, the authorities have yet to develop and issue uniform, adequate and detailed standards and guidelines for survey, design, fabrication, construction, and commissioning of nuclear power plants. In particular, acceptance criteria and internal guides for safety assessment are lacking.

The lack of uniform rules, standards and guidance will lead to certain problems during project implementation.

3.2. Human resources

Human resource development is one of the key issues in preparing infrastructure for nuclear power projects in Vietnam. It will become much more essential for a developing country like Vietnam. According to the approved scheme of training and human resource development of nuclear power, the first nuclear power plant will start to operate in 2020. Vietnam needs at least 2,200 engineers of nuclear power. However, until now, it seems that the training of human resources for the nuclear power program is facing several problems explained below:

- Lack of flexible mechanism for recruitment (no more new recruitment for a long time).
- Lack of policy to attract good students: currently, Vietnam has 7 universities responsible for education and training for the needs of human resources in the field of atomic energy. However, actual enrolment in the program is not adequate and quality of students is below expectation.
- Lack of policy to attract experts, especially Vietnamese experts who worked overseas for years.
- Brain-drain within the nuclear energy sector of Vietnam.

3.3. Other challenges

Vietnam is going to build two types of NPPs from 2 different countries at the first phase of the long-term nuclear power program. The introduction of two different technologies caused many difficulties for Vietnam in preparing legal documents infrastructures for nuclear power projects. This is caused by the two countries having applied different standards and norms for their technologies, so understanding the system requirements and standards of the two countries is also a major problem for Vietnam.

The specific technology has not been decided yet: WWER AES91/92/2006 (Russia) and ABWR, MPWR+, AP1000, ATMEA1 (Japan).

4. IMPROVEMENTS

4.1. Legal framework

One of the actions to take in order to overcome the difficulties mentioned above is that Vietnam should issue a systematic and comprehensive legal documents in details for standards, guidelines for the implementation of the survey work, design, fabrication, construction and operation of nuclear power plants, construction, inspection, testing, licensing, and maintenance.

However, with no experience in building technical standards for nuclear power, Vietnam should revise statements premier technical regulations applied in other countries such as Russia and Japan. After that, experience will be learned from implementation process. Based on these experiences, technical regulations will be established in accordance with Vietnam to meet the needs of nuclear power development.

4.2. Human resources development

Vietnam's government should strengthen without delay its human, financial resources, and technical capability to meet immediate needs for regulating both existing activities and, in particular, for the introduction of nuclear power.

Vietnam should have remuneration policy to attract a lot of human resources. However, besides attracting large amount of human resources, quality assurance is highly important. Besides, we can utilize the resources from Vietnamese experts who are working in overseas, especially those devoted to the development of the country.

5. CONCLUSIONS

Effective Defence in Depth (DID) implementation is one of the most important issues for countries pursuing nuclear power including Vietnam. We have already initially prepared for implementation of DID: infrastructure, legal development and human development. Safety assessment is complicated and unfamiliar in Vietnam and needs to be performed by high quality experts. For the first two NPPs in Vietnam, using international consultants for supporting safety assessment is unavoidable. Although the achievement gained recently is significant, more needs to be done in the future.

REFERENCES

[1] Vietnam National Assembly, Resolution No. 41/2009/NQ-QH12 on approval of investment reports on the first NPP in Ninh Thuan, Hanoi (2009).

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Requirements No. NS-R-1, IAEA, Vienna (2000).

[4] Vietnam Government, Decree No. 70/2010/ND-CP on detailing and guiding a number of articles of the Law on Atomic Energy regarding nuclear power plants, Hanoi (2010).

[5] Minister of Science and Technology, Circular No. 13/2009/TT-BKHCN by guiding on preliminary nuclear safety assessment for site selection for nuclear power plants in the investment decision stage (Pre-FS stage), Hanoi (20-May, 2009).

[6] Minister of Science and Technology, Circular No. 28/2011/TT-BKHCN on nuclear requirements for nuclear power plants site, Hanoi (2012).

[7] Minister of Science and Technology, Circular No. 29/2012/QĐ-BKHCN on format and content of SAR for NPP site approval, Hanoi (2012).

[8] Minister of Science and Technology, Nuclear Safety Standards 6941: External Human Induced Events in Site Evaluation for Nuclear Power Plants, Hanoi (2013).

[9] Minister of Science and Technology, Nuclear Safety Standards 6942: Dispersion of Radioactive Material in Air and Water and Consideration of Population Distribution in Site Evaluation Nuclear Safety, Hanoi (2013).

[10] Minister of Science and Technology, Nuclear Safety Standards 6943: Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Power Plants Nuclear Safety, Hanoi (2013).

[11] Minister of Science and Technology, Nuclear Safety Standards 6944: Seismic hazards in site evaluation for nuclear installations, Hanoi (2013).

[12] Minister of Science and Technology, Nuclear Safety Standards 6945: Geotechnical aspects of site evaluation and foundations for nuclear power plants, Hanoi (2013).

[13] Minister of Science and Technology, Circular No. 30/2012/QD-BKHCN on requirements on nuclear safety of design of NPPs, Hanoi (2012).

APPLICATION OF PSA IN DESIGNING NEW THIRD-GENERATION NPPs EQUIPPED WITH VVER REACTORS

A.YU. KUCHUMOV, V.B. MOROZOV
JSC Atomenergoproekt, Moscow, Russian federation
Email: morozov-sloboda@mail.ru

Abstract

The projects of new third-generation NPPs shall meet more stringent safety requirements. A proper balance between a high level of safety and modern requirements for power unit availability indicators cannot be achieved without applying a probabilistic approach in the course of designing, central to which is probabilistic safety assessment (PSA). The report presents the main results from application of PSA in working out new projects of NPPs equipped with VVER reactors, as well as the obtained quantitative results reflecting the entire spectrum of operational states and initiating events. It is shown that by using an efficient combination of active and passive safety systems it is possible to achieve a safety level in the projects complying with the latest requirements, including those following from the lessons learnt from the Fukushima accident.

1. A REVIEW OF THE MAIN SOLUTIONS IMPLEMENTED IN THE PROJECTS OF NEW NPPS EQUIPPED WITH VVER REACTORS

1.1. Main engineering solutions adopted for the new VVER plants

The new evolutionary designs of NPPs equipped with VVER reactors developed in JSC "Atomenergoproekt" are presented by NVNPP-2 and VVER-TOI projects.

The objective of developing the NVNPP-2 project was to construct the pilot NPP unit based on the AES-2006 design (third-generation of NPPs with light-water reactors), which shall possess, as compared with the reference power units at NPPs equipped with VVER-1000 reactors, an increased power capacity, better technical-economic and performance indicators, and enhanced safety level.

The VVER-TOI project as a further development of the AES-2006 was elaborated with a view to work out a standard (basic) project of a large-capacity NPP able to compete in the market with the products offered by rapidly developing and recognized leaders in the field of nuclear power engineering.

A comprehensive information model of an NPP has been developed as a result of the performed works. Suitability for serial production and a shorter construction period have been achieved as compared with the AES-2006 project. The main characteristics of the two projects are given below in Table 1. The general view of a two-unit VVER-TOI project is shown in Figure 1.

TABLE I. MAIN CHARACTERISTICS OF THE TWO VVER PREOJECTS

Key indicators	AES-2006	VVER-TOI
Power unit electrical capacity	1 198 MWe	1 255 MWe
Power unit (RP) service life	50 years	60 years
Power unit gross efficiency for annual average conditions	37.4%	37.9%
Availability factor (with a 18-month fuel cycle)	91%	93%
Autonomy time in case of BDBA	24 h	72 h
SSE	7 points	8 (9) points
Aircraft crash (a design-basis initiating event)	5.7 t	20 t
Heavy aircraft crash (a beyond design-basis event)	-	400 t
Time of construction	54 months	48/40 months

FIG. 1. Two-unit VVER-TOI project.

1.2. Safety system design

The safety assurance concept (see Table 2) adopted in the VVER-TOI project is based, as in the AES-2006 project on applying active and passive safety systems (SSs) having different principles of their operation. Active SSs have a two-train structure, and each train has a 100% capacity. This structure meets single failure criterion for any postulated IE. In order to achieve a longer time of independent survival under the conditions of BDBAs involving failure of active systems, the projects incorporate supplementary hydro accumulators, which guarantee, jointly with operation of the PHRS, maintaining controlled state of the shutdown reactor for no less than 24h (for AES 2006) and 72 h (for VVER-TOI) without any intervention of the personnel at any complex sequence, whose frequency cannot be neglected. Storage batteries for long-term operation are also included in the project.

In accordance with the PSA recommendations, the project incorporates redundancy of active elements in the trains of support systems except with the diesel-generators (DGs).

The project incorporates means intended to protect safety systems from onsite effects (fires, floods, steaming, steam-water jets, missiles, and whipping of pipelines in the NPP premises). Protection from such effects is ensured by implementing the principle of physical separation, i.e., by placing the equipment of individual safety trains in separate rooms segregated from each other by distance or protective barriers, and also by reliably fastening the equipment.

The main technical solutions on safety systems in the VVER-TOI project are also reflected in Figure 2.

1.3. Supplementary measures aimed at control of BDBA

In case of accidents evolving under the conditions of multiple failures of elements in active SSs (e.g., common-cause failures of inner nature) the time interval equal to 72 h from the accident onset moment is sufficient for taking corrective measures on restoring equipment, as a result of which the NPP is transferred from controlled state into safe state.

TABLE 2. STRUCTURE OF SAFETY SYSTEMS ADOPTED IN THE NEW VVER PROJECTS

Name of safety system	System structure
High-pressure ECCS	An active two-train system equipped with fully-variable combined pumps (2x100% trains)
Emergency and planned coodown system (EPCS)	An active two-train system (2x100% trains)
Emergency boron injection system JND	An active two-train system (2x100% trains)
SG emergency cooldown system (ECS)	A closed-loop active two-train system (2x100% trains)
ECCS passive part (HA1-)	A four-train passive system (4x33% trains)
Supplementary passive core flooding system (HA-2)	A four-train passive system (4x33% trains)
Passive heat removal system (PHRS)	A four-train passive system (4x33% trains) fitted with air-cooled heat exchangers
Passive annulus filtration system (PAFS)	A four-train passive system (4x33% trains)

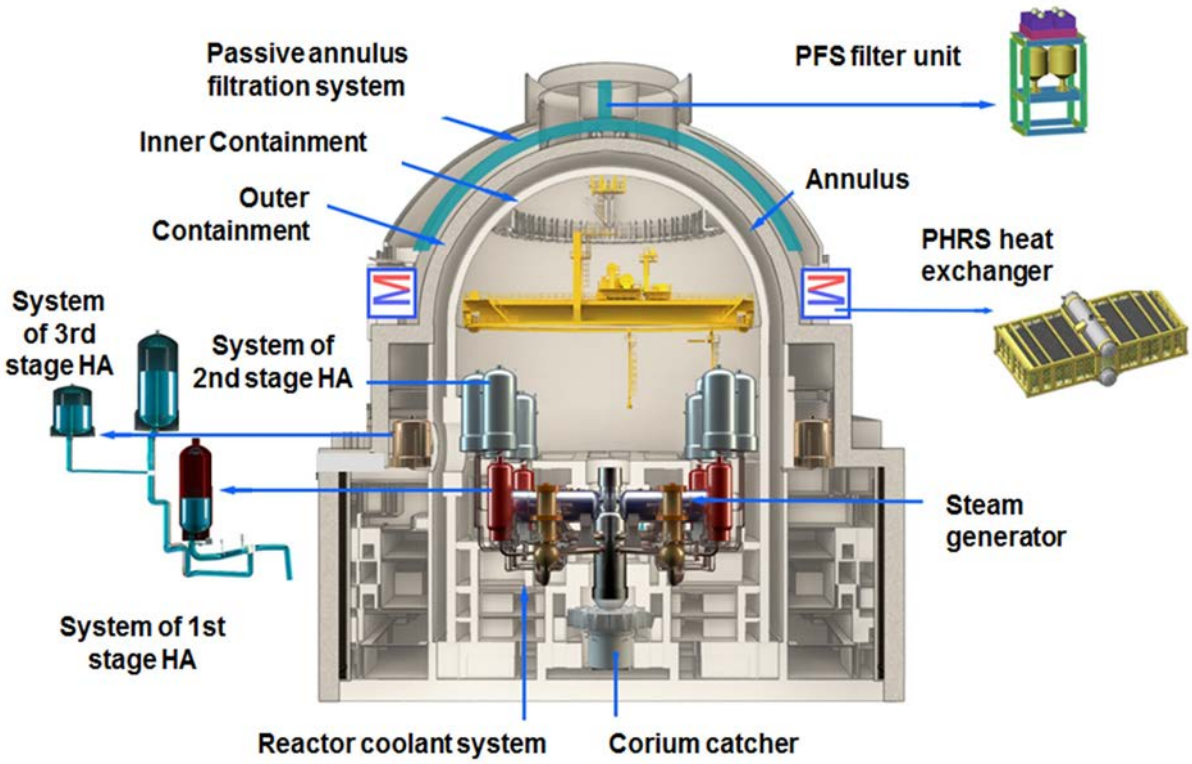

FIG. 2. VVER-TOI safety systems.

However, in the light of events that occurred at the Fukushima NPP, during which extreme (off-design) natural events led to multiple failures and eventually to a severe event, the VVER-TOI project incorporates supplementary systems ensuring safety in the following extreme situations:

- SBO (total loss of all AC sources including emergency ones);
- loss of all ultimate water heat sinks; and
- a combination of the above-mentioned events.

In the above-mentioned cases, after exhausting water inventories in the hydro accumulators, if attempts to restore normal or emergency power supply were not successful, makeup of the reactor and fuel pool is organized using pump sets powered from a mobile air-cooled diesel generator (water may be inaccessible as DG cooling medium), as well as heat removal by means of a dry mobile cooling tower. The operating principle of these systems is presented below in Figure 3.

Similar supplementary systems were introduced in the NVNPP-2 project based on the results of performed tests.

The VVER-TOI project incorporates more enhanced - as compared with the NVNPP-2 project - protection from accidents caused by aircraft crashes. At present, such accidents, along with extreme natural phenomena, are regarded as one of the main risk factors in the subsequent decades. The VVER-TOI project takes into account recommendations formulated in the new revision of the EUR document and in the WENRA documents.

The characteristics of the considered events with regard of the design aircraft and a large commercial aircraft are given in Figure 4.

To comply with the above-mentioned requirements, the external protective structures of the UJA building are separated by a construction joint and annulus from the internal structures of the building to exclude direct transfer of dynamic impacts on the internal structures and equipment of the building.

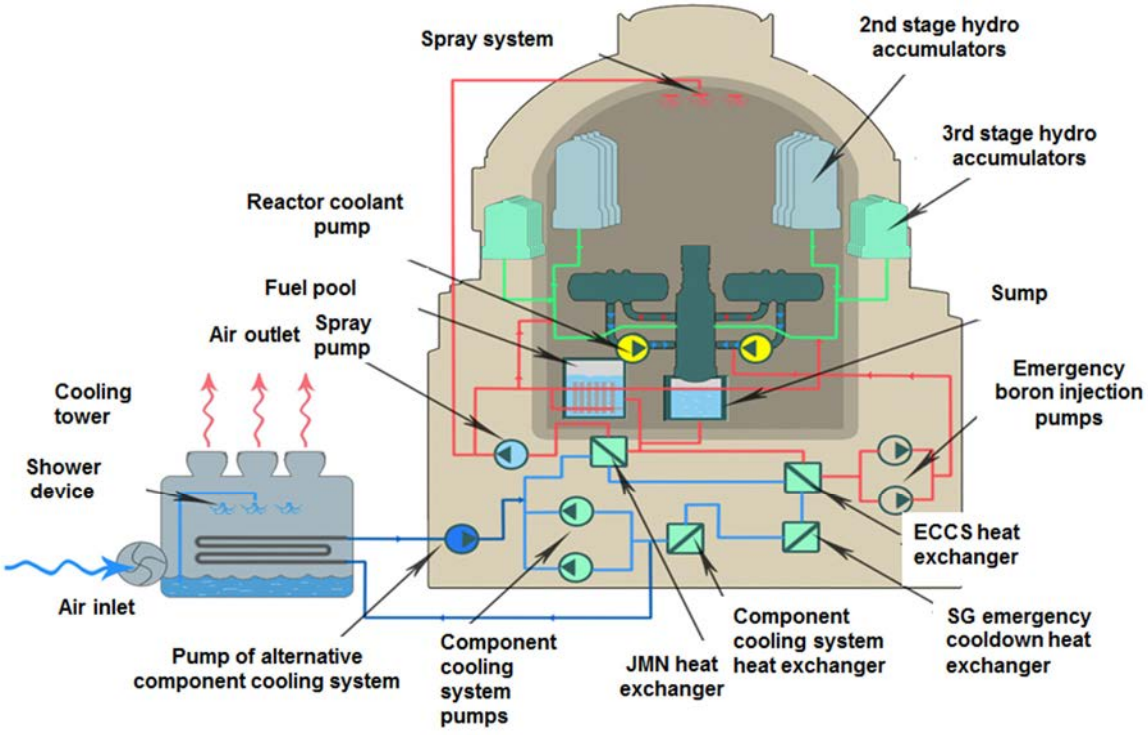

FIG. 3. Supplementary safety systems.

Mass, t	Velocity , m/s	Impact spot, m^2	
LearJet 23 (considered in the NVNPP-2 project)			
5.7	100	12	
Phantom RF-4E – a design-basis initiating event			
20	215	7	
Boeing 747-400 – a beyond design-basis initiating event			
400	150	50+50	

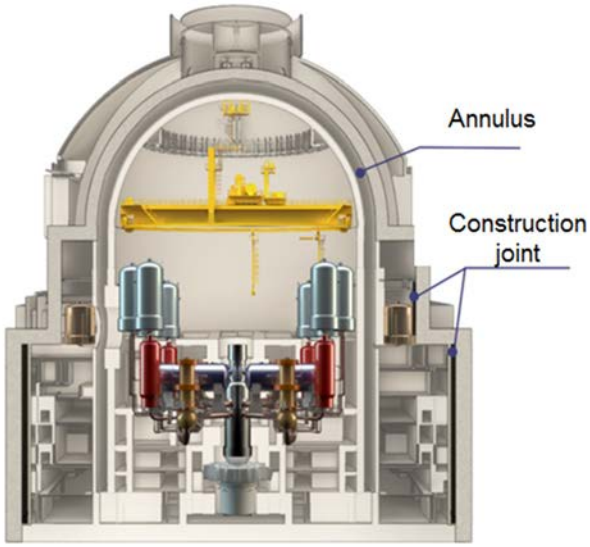

FIG. 4. Aircraft crash protection.

2. VERIFICATION OF THE PROJECT WITH RESPECT TO PROBABILISTIC SAFETY CRITERIA

2.1. Probabilistic Safety Criteria for the NVNPP-2 Project

According to the requirements set forth in OPB 88/97 [1], which is the RF basic regulatory document in the field of safety, the NVNPP-2 project shall comply with the following probabilistic safety criteria. Efforts should be taken to ensure that the overall probability of a severe beyond design-basis accident estimated using PSA methods would not exceed 10^{-5} per reactor a year.

The probability (occurrence rate) of NPP states in case of which relocating the population to beyond the zone of planning protective measures may be required shall not exceed 10^{-7} per reactor a year.

The technical assignment for both projects specifies a more stringent requirement with regard to the second criterion, according to which the overall probability of severe damage to nuclear fuel shall not exceed 10^{-6} per reactor a year. In the followed chapter the results of design verification against this target are presented.

2.2. The Scope of Level 1 PSA for the NVNPP-2 Project

The fulfilment of the above-mentioned criterion is demonstrated in the project based on the results of performing full-scale Level 1 PSA. The results of Level 1 PSA must be submitted and approved by the Russian regulator (Rostekhnadzor) to grant a license for NPP construction.

Therefore, in developing Level 1 PSA all kinds of IEs, including internal events, internal risks, and natural and man-made risks typical for the NPP site were considered for all operational states: operation at nominal and low power levels, shutdown states for refuelling and planned maintenance, and shutdown state for unscheduled repair of failed equipment.

2.3. Main results and conclusions

2.3.1. The Results of Level 1 PSA for Internal IEs

The list of operational states (OSs) of the NVNPP-2 power unit is given below in Table 3. Twenty states were considered, including two states of power operation and 18 states with the shutdown reactor.

The shutdown OSs 01a, 03a, and 04в are connected with repairs of failed equipment and occur at random moments of time. The other OSs are characterized by planned outage periods.

For the OS 00a the PSA model was developed assuming that the unit operates at the nominal level of power. For this state, a list of IE groups was drawn, which included 23 events belonging to groups 2, 3, 4 of postulated events, as well as IEs of BDBAs that are not considered in the project. The results of Level 1 PSA for internal IEs at power operation (specified with IEs that contributes more than 3% to the CDF) are given in Table 4.

TABLE 3. LIST OF OPERATIONAL STATES OF THE NVNPP-2 UNIT

Designation and name of OS	Designation and name of OS
OS 00a - The reactor is in critical state and operates in power-generating modes	OS 05 – Refuelling with partial unloading of fuel
OS 00в - The reactor is in critical state and operates at low power with the TG disconnected	OS 05a – Refuelling with partial unloading of fuel
OS 01 – “Hot” state, the RP is cooled down through the secondary coolant circuit till disconnection of the ECCS passive part	OS 05в – Inspection of the RP equipment after full unloading of fuel
OS 01a – “Hot” state for shutdown without draining and cooling down	OS 06 – Filling the primary and secondary coolant circuits and testing the sealed enclosure
OS 02 – RP cooling down through the secondary coolant circuit from disconnection of the ECCS passive part to connection of the EPCS	OS 07 – Heating to the temperature of hydraulic tests
OS 03 – Cooling down through the reactor coolant system (RCS) and degassing of the RCS	OS 08 – Hydraulic tests of the RCS
OS 03 a – Cooling down through the RCS, "cold" state, and repair of equipment for shutdown without draining but with cooling down	OS 09 – Hydraulic tests of the secondary coolant circuit
OS 04 – Disassembling the reactor, assembling the reactor during refueling outage with partial unloading of fuel	OS 10 – Heating to connection of the ECCS passive part
OS 04a – Disassembling the reactor, assembling the reactor during refueling outage with full unloading of fuel	OS 10 a – Heating to connection of the ECCS passive part for shutdown without draining and with cooling down
OS 04в – Repair of RCPL loops (during outage for repairing the RCPL equipment)	OS 11 – Heating to the “hot” state, “hot” state

TABLE 4. LEVEL 1 PSA RESULTS

Description of IEs	IE code	IE frequency, 1/year	CD frequency, 1/year	Contribution, %
Large-LOCA	LL	2.09E-05	5.19E-09	3.3
Medium-LOCA	ML	4.33E-05	5.38E-09	3.4
Small-LOCA	SL	9.10E-04	3.63E-08	23.0
LOCA compensated by the volume control system	LCC	1.00E-01	7.86E-09	5.0
LOCA outside the containment	LCI	2.50E-03	2.55E-10	0.2
Primary-to-secondary LOCAs	-	2.13E-03	7.12E-09	4.5
All primary leaks	-	1.05E-01	6.21E-08	39.3
Loss of offsite power	-	6.40E-02	2.43E-08	15.4
General transients	GT0	6.00E-01	5.27E-09	3.3
Loss of normal heat removal	LNHR	2.70E-01	9.67E-09	6.1
Leak of steam lines in the non-isolated part	SLN	2.20E-02	7.19E-09	4.6
Small-break secondary leak, administrative shutdown	SSLN	7.20E-02	1.04E-08	6.6
Loss of service cooling water	SWS	5.10E-03	7.80E-09	4.9
IEs with administrative shutdown	AS	5.08E-01	5.38E-09	3.4
All Transients	-	1.84E+00	5.81E-08	36.8
IEs of beyond design basis accidents	BDA	1.37E-08	1.37E-08	8.7
All initiating events	-	2.01E+00	1.58E-07	100.0

Small LOCA (23% and 39.3% due to all leaks) and LOOP (15.4%) are the major contributors to the CDF. The group of transients accounts for 36.8% of CDF, but actually this group encompasses a multitude of IEs the contribution from each of which does not exceed 7%. Among the dominant sequences, the greatest contribution in CDF is due to accident sequences initiated by small and compensated primary leaks. The next events in the above-mentioned accident sequences include a common cause failure to open the JNA (ECCS) gate valves in the lines supplying water from the sump. It should be noted that 6.33% of the overall CFS is due to BDBAs involving RPV rupture.

The contributions in the CDF from internal IEs from different OSs during power unit operation at low power levels and for the shutdown reactor are given in Table 5. It should be pointed out that for each OS we determined an individual list of IEs and developed event trees. In all, 118 event trees were developed.

TABLE 5. RESULTS FROM ESTIMATING THE CDF

OS	CDF, 1/year	Contribution, %	OS	CDF, 1/year	Contribution, %
OS 00в	1.95E-09	0.8	OS 05	6.06E-08	23.5
OS 01	7.40E-09	2.9	OS 05A	8.30E-09	3.2
OS 01A	2.64E-08	10.2	OS 06	6.01E-10	0.2
OS 02	7.72E-10	0.3	OS 07	5.71E-09	2.2
OS 03	3.75E-09	1.5	OS 08	4.87E-09	1.9
OS 03A	1.55E-08	6.0	OS 09	2.72E-09	1.1
OS 04	1.03E-07	39.9	OS 10	2.10E-09	0.8
OS 04A	6.96E-09	2.7	OS 10A	5.60E-10	0.2
OS 4B	1.63E-09	0.6	OS 11	4.96E-09	1.9
OS 05	6.06E-08	23.5	**Overall CDF**	**2.58E-07**	**100**

Among the IE groups, the greatest contribution in the CDF in these modes is due to IEs involving falling of heavy components in states with the depressurized reactor (BDBAs) – 39.5%, loss of offsite power – 15%, loss of normal heat removal and loss of service cooling water – around 7% for each IE. The most significant basic events in these modes are a common-cause failure of steam dump valve (SDV-A) to close, common-cause failure of the DG during operation, and independent failures of DGs. The overall CDF for all internal IEs and all power unit operational states is 4.16E-07.

2.3.2. The Results of Level 1 PSA for Internal Fires

All site-specific events of natural and man-made origin were analyzed taking into account commonly adopted selection criteria. Among the internal hazards fires in the premises of NPP buildings, which are a serious safety jeopardizing factor for the majority of NPPs were selected.

The cumulative value of CDF caused by fires is 9.04E-09 per reactor a year, which is less than 6% from the CDF during power unit operation in the power-generating mode.

In all, six fire zones with a contribution in the CDF more than 0.1% each were revealed. The overall fraction of these premises in the total CDF is 99.4%. The greatest contribution in CDF is from the scenario with a very small primary leak, which can take place in case of fire in the sealed containment building (UJA). For the NVNPP-2 project the possibility of false change of equipment state in case of fire in these premises is ruled out almost completely, except with spurious opening of pilot-operated safety valves, which is possible in a limited number of rooms; all these scenarios are characterized by low probability and, taking into account physical and spatial separation of safety system trains, are insignificant.

The relatively low significance of the turbine building is attributed to the use of measures aimed at both reducing the fire load in this building and enhancing protection of the reactor compartment from events in the turbine building.

An essentially smaller significance of the MCR and remote shutdown station (RSS) premises (these premises were not among the dominant contributors) achieved in the project

as compared with the operating NPPs is due to a number of special measures, such as use of dedicated remote control arrangements ensuring protection from generation of false commands, separation and protection of cables in SS trains in the MCR (RSS) cable floor, organizing reliable escape routes for the personnel from the MCR in case of fire in this control room, and complete independence of these control rooms from each other.

2.3.3. Results of Level 1 PSA for External hazards

In accordance with the commonly adopted approach [3, 4], the PSA for external risks includes the stages of preliminary selection of events, the boundary and detailed analyses.

The first stage involves selection of external events that can be significant for contribution into the CDF. The screening criteria were used to exclude insignificant events from the subsequent analysis (see Tables 6 and 7).

The following effects were selected based on an analysis of external hazards for carrying out a boundary analysis:

- a direct effect of strong wind loads (including missiles),
- a direct effect of tornado (including missiles), and
- a direct effect of snow loads.

A detailed analysis was performed for the seismic impact in accordance with [4, 5]. Models of sources and models of seismic effect attenuation laws with distance were developed during the probabilistic analysis of seismic hazard (Figures 5 and 6).

TABLE 6. QUALITATIVE CRITERIA

Code of criterion	Description of criteria
A	An IE able to affect the NPP power unit cannot occur sufficiently close to the NPP site
B	An IE is included in the definition or bounded by another considered event
C	An IE features a slow development, and a large time margin is available for the plant personnel to prevent its development to a critical size of the impact or to take adequate measures on limiting its effect

TABLE 7. QUANTITATIVE CRITERIA

Code of criterion	Description of criteria
D	An IE either itself has a very low average occurrence rate ($<10^{-7}$/year) or its average occurrence rate is significantly lower than the other considered events, which are characterized by similar uncertainty and no less severe consequences from the viewpoint of risk of severe core damage
E	(a) An IE is characterized by a similar or smaller destructive potential than the event the NPP immunity for which is ensured by the design; (b) The occurrence rate of a destructive event leading to core damage is less than 10^{-7} 1/year. Note: The use of this criterion implies analyzing the NPP project to determine if the NPP structures and systems are adequately protected from a particular IE.

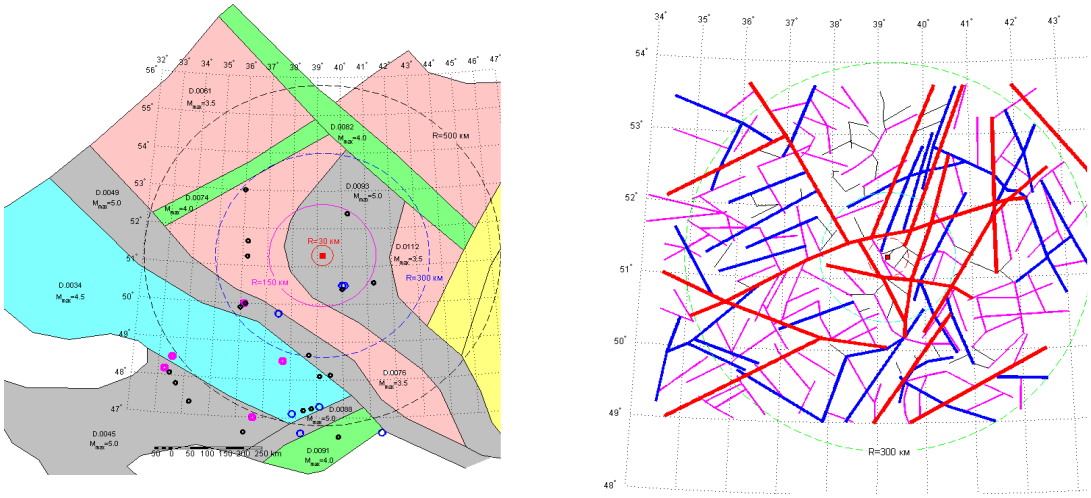

FIG. 5. Models of seismic effect sources for the NVNPP-2.

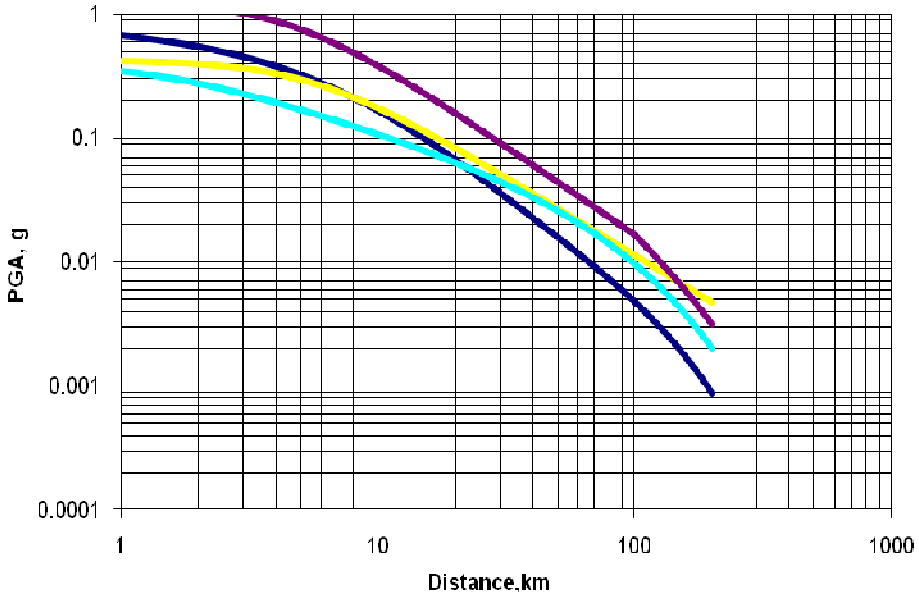

FIG. 6. Models of attenuation laws for the NVNPP-2 model.

A probabilistic logic tree was developed for taking into account uncertainty in the selection of source models, attenuation laws, estimates of impact magnitudes, and other possible inaccuracies.

Seismic hazard curves were obtained as a result of calculations for different levels of confidence probability that take into account various uncertainties (Fig. 7).

The PSA model for seismic events is constructed on the basis of the PSA model for internal IEs. The estimated frequencies of the external effects selected for analysis, as well as possible direct consequences (internal IEs and failures caused by them), are given below in Tables 8 and 9.

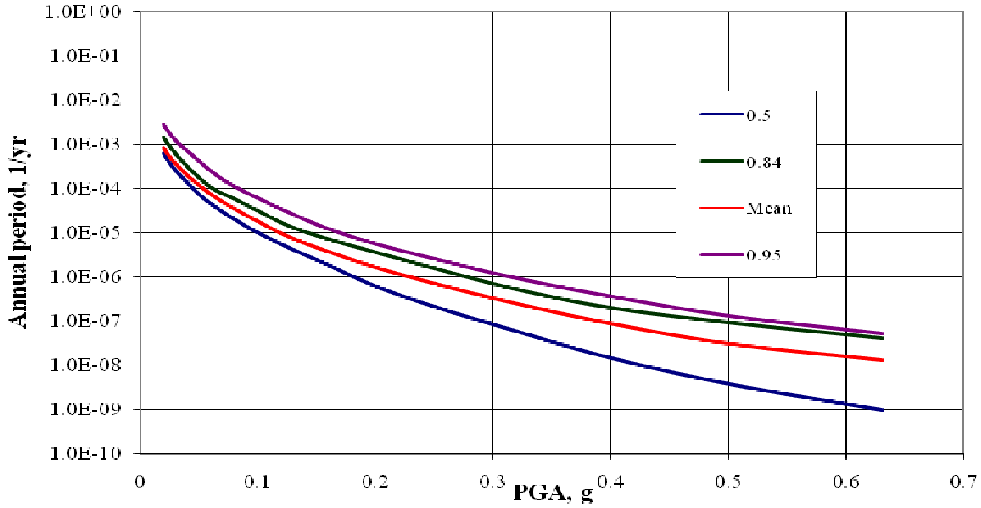

FIG. 7. Seismic hazard curves.

TABLE 8. ESTIMATED FREQUENCIES AND CONSEQUENCES CAUSED BY EXTERNAL NATURAL AND MAN-MADE EFFECTS FOR A MARGINAL ANALYSIS

External effect	Initiating event in the PSA model	Frequency, 1/year
Direct effect of wind loads (including missiles)	Long-term loss of offsite power*	$3.28 \cdot 10^{-4}$
	Long-term loss of offsite power* + damage to turbine building (10UMA)	$1.9 \cdot 10\text{-}^{5}$
Direct effect of tornado (including missiles)	Long-term loss of offsite power + failure to supply cooling service water to essential loads	$1.85 \cdot 10^{-5}$
	Long-term loss of offsite power + failure to supply cooling service water to essential loads + damage to turbine building (10UMA)	$1.3 \cdot 10^{-6}$
Direct effect of snow loads	Short-term loss of offsite power + damage to turbine building (10UMA)	$4.8 \cdot 10^{-4}$

** Considered jointly with failure to supply cooling service water to essential loads after 48 h since the commencement of power unit shutdown operations.*

TABLE 9. FREQUENCIES OF SEISMIC IES FOR DIFFERENT EFFECT LEVELS, 1/YEAR

Initiating event	0.04g	0.06g	0.08g	0.13g	0.20g	0.25g
Damage to buildings of seismic category II with LOOP	$3.31 \cdot 10^{-7}$	$1.52 \cdot 10^{-6}$	$1.97 \cdot 10^{-6}$	$1.17 \bullet 10^{-6}$	$2.39 \cdot 10^{-7}$	$7.89 \cdot 10^{-8}$
Rupture of the LBA, JNB pipeline system in the part non-isolated from the SG in the steam chamber with LOOP	$1.62 \cdot 10^{-9}$	$3.84 \cdot 10^{-8}$	$1.10 \cdot 10^{-7}$	$2.81 \cdot 10^{-7}$	$1.59 \cdot 10^{-7}$	$6.79 \cdot 10^{-8}$
Combination of the events: damage to buildings of seismic category II, pipeline ruptures in the part non-isolated from the SG in the steam chamber with LOOP	$3.33 \cdot 10^{-7}$	$1.55 \cdot 10^{-6}$	$2.06 \cdot 10^{-6}$	$1.29 \cdot 10^{-6}$	$2.53 \cdot 10^{-7}$	$8.07 \cdot 10^{-8}$

The total contribution of external events in the CDF per NVNPP-2 power unit was estimated to be $3.89 \cdot 10^{-8}$ 1/year or approximately 24% of the CDF due to internal IEs. The maximal contribution of events connected with extreme snowfalls is attributed to the initial relatively high frequency ($4.8 \cdot 10^{-4}$ 1/year) of direct consequences of such events connected with possible damage to the turbine building, which may lead to dependent failures of the secondary coolant system equipment. It should also be pointed out that a noticeable growth of snow cover has recently been observed in the European part of Russia, which is consistent with the obtained results.

A conclusion can be drawn from the Level 1 PSAs that have been accomplished that the overall estimated CDF obtained taking into account all of the considered internal and external hazards is $4.8 \cdot 10^{-8}$ 1/year, which is equivalent to approximately 30% of the CDF during power operation or 10% of the total accumulated CDF from all modes, which is equal to $4{,}8 \cdot 10^{-7}$ 1/year per power unit.

It also follows from the presented analysis that the use of a passive heat removal system (PHRS) to the ultimate heat sink, as well as physical and spatial separation of the safety system trains show efficient performance under the conditions of external effects. The results obtained confirm that the target safety criteria are met.

2.4. Results of Level 1 PSA for the VVER-TOI Project

The Level 1 PSA (PSA-1) for the basic VVER-TOI project has presently been carried out within the scope of internal IEs, because it is advisable to analyze external hazards for specific NPP sites subject to receiving a positive conclusion of Rostekhnadzor (the Russian Regulatory Authority) on the basic PSA for internal IEs.

In all, 48 different types of initiating events for 20 operational states (OSs) were considered, including the following ones:

- 41 IEs for OSs with the power unit operating in the power-generating mode, including its operation at the MCL with the turbine shut down; and
- from 3 to 33 IEs for different OSs with the reactor shut down (11 groups of OSs, in all, 19 states).

In estimating the probabilistic safety indicators we also considered events of beyond-design basis accidents involving a catastrophic rupture of the RPV, the SG shell and header, and also an accident involving overdraining of the RCS, and accidents caused by falling of heavy components into the reactor in shutdown modes.

The models of accident sequences were developed taking into account the need to reach safe states. The minimal period of time considered in the PSA corresponding to regular (design) operation of safety systems is taken equal to 24 h. Restoration of failed equipment in this period of time is not considered. The maximal period of time considered in the PSA is defined for particular sequences of BDBAs and is no less than 72 h.

In all, 135 event trees (ETs) have been developed in the PSA-1 model, including 76 IEs for the reactor core in power-generating modes, 44 ETs for the reactor core in shutdown modes, and 15 ETs for the fuel pool in different modes.

The point assessment of the overall (totalled over all groups of IEs for all power unit modes) CDF is 2.6E-07 (see Table 10) per reactor a year, which is a factor of 16 lower than required according to the technical assignment.

The largest contributions in the overall CDF value are from the power operation modes (OS 00, 1.0E-07 1/year, 45%) and shutdown modes with disassembling and assembling the

reactor during its shutdown with partial refuelling (OS 04, 7.9E-08 1/year, 27%) or with full refuelling (OS 04a, 3.8E-08 1/year, 13%).

Among the IEs, a considerable contribution (43%, see Figure 8) is due to IEs that are not considered in the project (IES of BDBAs), for which we postulate fuel damage in the core as a consequence of the IE itself. A high contribution from BDBAs is attributed primarily to conservatism in assessing the frequencies of such events (detailed probabilistic-strength analyses for such initiating events have not been completed).

A conclusion can be drawn from the obtained results that a high level of safety has been achieved for the VVER-TOI project, which is confirmed by comparison with other evolutionary projects, especially taking into account the conservatism in assessments of frequencies for IEs of BDBAs. This result has been achieved through applying the following solutions:

– efficient combination of active and passive systems ensuring functional redundancy, long-term independent survival of the power unit during accidents (no less than 72 h), protection from common-cause failures, and decreased influence of the human factor; and

– application of additional measures in the above-mentioned extended period of independent survival for restoring the critical safety functions, including connection of a mobile DG station to the loads (in case of SBO) and use of an independent heat exchanger connected to the heat exchangers of safety systems (for accidents involving total loss of service cooling water or loss of the component cooling system).

TABLE 10. CDF VALUES ESTIMATED FOR OF INITIATING EVENTS IN DIFFERENT MODES OF POWER UNIT OPERATION (95%)

Description of IEs	Code of calculation	IE frequency, 1/year	CDF, 1/year	Contribution, %
OS 0; RPV rupture	00-IE-RVR	6.7E-08	6.7E-08	23.2
OS 4a; Falling of heavy components (a BDBA)	04AIE-DROP	2.6E-08	2.6E-08	8.9
OS 4; Falling of heavy components (a BDBA)	04-IE-DROP	2.6E-08	2.6E-08	8.9
OS 0; Small-break leak (20<Dnom≤40 mm)	00-IE-LCS20	3.02E-03	2.5E-08	8.7
OS 4; Loss of offsite power	04-IE-LOOP	9.70E-04	1.7E-08	5.8
OS 4; Boron dilution	04-IE-BOR	2.33E-05	1.5E-08	5.0
OS 0; Very small primary-to-secondary leak	00-IE-SGSL	1.04E-01	1.3E-08	4.3
OS 4; Loss of heat removal from the core due to EPCS failures	04-IE-LHR	2.71E-04	1.2E-08	4.0
OS 4a; Loss of heat removal from the core due to EPCS failures	04AIE-LHR	2.94E-04	1.1E-08	3.6
OS 4; Loss of component cooling system of service cooling water for essential loads	04-IE-SWS	6.51E-06	9.7E-09	3.3
OS 3a; Rupture of the planned cooldown line inside the containment	03AIE-LCPCI	3.64E-06	9.3E-09	3.2
All IEs in all modes	-	-	2.6E-07	100

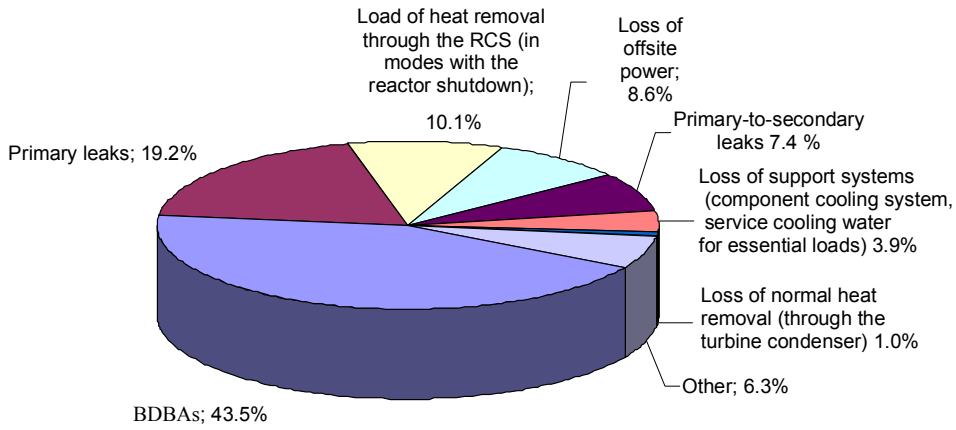

FIG. 8. CDF Contribution from internal events.

3. OTHER PSA APPLICATION FIELDS IN DESIGNING NPPs

3.1. Substantiating the Fulfilment of Deterministic Criteria

The safety analysis report contains a representative list of events postulated in the design (PIEs) in performing a safety analysis. Each of the main safety functions is characterized, depending on a particular PIE, by certain configuration of safety systems required for performing this function.

In accordance with i. 2.1.8 of document [2], PIEs must be classified according to their occurrence rates (frequencies). The Technical Assignment for the NVNPP-2 project stipulates three categories of PIEs with respect to frequency bands:

- Category 2 of PIEs (from 10^{-2} to 1 1/year frequency).
- Category 3 of PIEs (PIEs of DBAs from 10^{-4} to 10^{-2} 1/year frequency).
- Category 4 of PIEs (PIEs of DBAs t from 10^{-6} to 10^{-4} 1/year frequency).

The most stringent requirements have been established for the most frequent events relating to PIEs of category 2; in case of such events, the operational limits specified for the state of nuclear fuel and release of radioactive substances shall not be exceeded.

Categories 3 and 4 of PIEs correspond to design-basis accidents for which the design must define the final states and limits that shall not be violated provided that the safety systems perform their intended functions taking into account the single failure criterion.

In order to show that the above-mentioned requirements of the document [2] and Technical Assignment for the NVNPP-2 project are fulfilled, a report has been developed, in which PIEs were categorized according to their probabilities (frequencies) based on field experience and application of probabilistic methods of fracture mechanics. A number of results obtained from estimates of IE frequencies generated the need to reconsider operating modes toward shifting them into the category of PIEs with more stringent requirements.

According to [1], PIEs for which the project shall contain substantiation of its compliance to the deterministic criteria mentioned above include single events, i.e., events occurring as a consequence of single failures of NPP components, human errors, or single events external with respect to the NPP. The results obtained in the Level 1 PSA were used

for checking if this requirement is fulfilled by analyzing systems structure and the minimal cut sets obtained in different operational states. To this end, the IEs of BDBAs for which no protection is provided in the design, but which are characterized by extremely low probability (e.g., the RPV rupture) to be excluded from the consideration, as well as those which themselves or the subsequent IEs are in fact common-cause failures (complex sequences) or erroneous operator decisions. For the other sequences, the check of whether the criterion is fulfilled consisted of checking the number of events. An analysis has shown that the PSA model for the NVNPP-2 and VVER-TOI does not contain sequences comprising only one independent event apart from the IE. A conclusion can also be drawn that both projects are stable with respect to multiple common-cause failures (there is a limited number of events containing single CCF). An example of this is a CCF involving a group of valves in the suction lines from the sump (failure to open mode).

The obtained results demonstrate the effectiveness of design solutions aimed at ensuring protection from common cause failures that are constructed based on the diversity principle.

3.2. Substantiation of Technical Specifications

For the NVNPP-2, the AOT for taking SS trains for unscheduled repair during power operation is 72 h, and that adopted for taking redundant parts of SS train for unscheduled repair is 240 h. For substantiating AOT for which a safety train can be taken for repair, the influence of this time on CDF value was analyzed. To this end, a number of calculations were carried out, namely:

- determination of CDF taking into account inoperable state of one safety train due to repair during power operation for 72 h (and for 240 h in case of redundant safety train components);
- determination of CDF without taking into account inoperable state of SS elements due to repair during power operation (assuming that the SS have their full configuration); and
- determination of CDF taking into account inoperable state of SS elements due to forced repair during power operation for the mean time of restoration for each item of equipment but without exceeding the limitations established in the regulations.

The CDF value estimated taking into account inoperable state of the train for the AOT of taking SS train components for unscheduled repair during power operation equal to 72 h and the AOT of taking redundant parts of safety train for unscheduled repair for 240 h is 1.59E-07 1/year. In case of SS train equipment failure, the entire train is not taken out from operation; only the failed equipment is repaired. The permissible time of taking SS equipment for repair was substantiated proceeding from the following criteria:

- a comparative assessment of an increase in the CDF in postulating the repair time intervals equal to their permissible scheduled values (72 and 240 h, respectively) as compared with the version involving full configuration of the SS (the difference is less than 10%);
- a comparative assessment of an increase in the CDF in postulating the repair time intervals equal to their permissible scheduled values as compared with the basic calculated PSA version (the difference is less than 1%); and
- the absolute CDF value in the version with the postulated time (this value is well below the TA requirements).

In view of the obtained results, a conclusion can be drawn that adoption of the permissible restoration time equal to 72 h and the permissible time of unscheduled repairing redundant parts of a safety train for 240 h has almost no effect on the CDF value (toward increasing) for internal events with the power unit operating in the power-generating mode.

REFERENCES

[1] General Provisions for Ensuring Safety of Nuclear Power Plants, OPB-88/97, Moscow (2001).

[2] Nuclear Safety Regulations for Nuclear Power Plant Reactor Installations, NP-082-07, Moscow (2007).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Nuclear Plant Design Options to Cope with External Events, IAEA-TECDOC-1487, IAEA, Vienna (2006).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards, Specific Safety Guide No. SSG-3, IAEA, Vienna (2010).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety assessment for Seismic Events, IAEA-TECDOC-724, IAEA, Vienna (1993).

DEFENCE IN DEPTH AND AGEING MANAGEMENT

S. FABBRI, G. VEGA, A. DILUCH, R. VERSACI
Comisión Nacional de Energía Atómica
Buenos Aires, Argentina
Email: versaci@cnea.gov.ar

Abstract

Accident prevention is the first safety priority of both designers and operators. It is achieved through the use of reliable structures, components, systems and procedures in a plant operated by personnel who are committed to a strong safety culture. For future nuclear power plants, consideration of multiple failures and severe accidents will be achieved in a more systematic and complete way from the design stage. Defence in depth (DID) consists of a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant. The primary way of preventing accidents is to achieve a high quality in design, construction and operation of the plant, and thereby to ensure that deviations from normal operation are infrequent. The best way to meet these premises of effectiveness of the barriers and the Systems, Structures and Components (SSCs) is to develop an ageing management programme to prevent potential failures and accidents. In this work we will refer to the ageing management programme for Atucha I and Atucha II power plants and to the Atucha I spent fuel storage.

1. INTRODUCTION

The principle of defence in depth is to compensate for potential human and mechanical failures; a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective [1]. Defence in depth helps to establish that the three basic safety functions (controlling the power, cooling the fuel and confining the radioactive material) are preserved, and that radioactive materials do not reach people or the environment.

All the levels of defence are available at all times that a plant is at normal power. Appropriate levels are available at other times. Severe accidents in the past have been the result of multiple failures, both human and equipment failures, due to deficiencies in several components of defence in depth that should not have been permitted.

The first means of DID preventing accidents is to strive for such high quality in design, construction and operation of the plant that deviations from normal operational states are infrequent. Safety systems are used as a backup to feedback in process control to prevent such deviations from developing into accidents. Safety systems make use of redundancy and diversity of design and the physical separation of parallel components, where appropriate, to reduce the likelihood of the loss of a vital safety function. SSCs should be inspected and tested regularly to reveal any degradation which might lead to abnormal operating conditions or inadequate safety system performance. Abnormal conditions possibly affecting nuclear safety are promptly detected by monitoring systems that give alarms and in many cases initiate corrective actions automatically.

Thus the prevention of accidents depends on conservatively designed equipment and good operational practices to prevent failure, quality assurance to verify the achievement of the design intent, surveillance to detect degradation or incipient failure during operation, and steps to ensure that a small perturbation or incipient failure would not develop into a more serious situation.

After the Fukushima accident the application of the defence in depth concept should be improved to clarify how to focus safety measures on both the prevention of accidents and the

mitigation of accident consequences. In particular, the mitigation measures to ensure containment integrity should be strengthened [2].

In the application of the DID concept, the main efforts are concentrated on prevention of significant reactor core damage. This objective should continue, but in addition, more effort should be directed at the mitigation of radiological consequences in the event that prevention fails. In this case, special emphasis should be given to preserving the containment function. One objective of the DID concept is to control accidents within the design basis to prevent their evolution to severe reactor core or spent fuel damage. Experience has shown that events may take place that were not specifically addressed in the original design of currently operating plants and that were not protected against with specific safety systems. Such events are often called BDBAs, and the current requirements generally imply that also the conceivable BDBAs are addressed in the design of new facilities and in emergency measures.

In the updated IAEA safety standards on nuclear power plant design [3], BDBA events are called design extension conditions (DECs), as a step toward improved inclusion of BDBAs in the design requirements for nuclear power plants. At nuclear facilities currently in operation, the BDBAs have to be considered in connection with the safety reassessment or periodic safety evaluation. Consequently, 'compensatory measures' such as new back-fitted systems or the provision of transportable equipment may be found to be necessary. The result is a balanced safety concept that prevents any accident from evolving into a severe accident. For prevention of severe accidents, it is important to emphasize the high reliability of reactivity control and decay heat removal from the reactor core and the spent fuel. For the mitigation of accidents, the protection of containment integrity is most important. However, after severe core damage, reactivity control and decay heat removal are also needed in order to maintain containment integrity. In practice, it is necessary to separately consider all physical phenomena that could endanger the containment integrity, and to plan adequate protection against each of them.

It is important that systems for the prevention of accidents and for the mitigation of accidents be separate and fully independent. Without such separation, it is probable that a single incident would cause the loss of several levels of DID. Independence and separation also need to be emphasized between redundant subsystems within each DID level and between diverse systems within each DID level.

2. AGEING MANAGEMENT PROGRAMME

To meet the requirements of the DID, physical barriers and the safety related SSCs must be operative. To maintain plant safety it is very important to detect ageing effects of SSCs, to address associated reductions in safety margins and to take corrective actions before loss of integrity or functional capability occurs.

Managing ageing for nuclear power plants means ensuring the availability of required safety functions throughout the service life of the plant, with account taken of changes that occur with time and use. This requires addressing both physical ageing of SSCs, resulting in degradation of their performance characteristics, and obsolescence of SSCs, i.e. their becoming out of date in comparison with current knowledge, standards and regulations, and technology. A foundation for effective ageing management is that ageing is properly taken into account at each stage of a plant's lifetime, i.e. in design, construction, commissioning, operation (including long term operation1 and extended shutdown) and decommissioning. Effective management of ageing of SSCs is a key element of the safe and reliable operation of nuclear power plants.

Physical ageing, referred to in a related IAEA Safety Guide as Ageing [4], of SSCs may increase the probability of common cause failures, i.e. the simultaneous degradation of physical barriers and redundant components, which could result in the impairment of one or more levels of protection provided by the defence in depth concept.

Effective ageing management is in practice accomplished by coordinating existing programmes, including maintenance, in-service inspection and surveillance, as well as operations, technical support programmes (including analysis of any ageing mechanisms) and external programmes such as research and development. Effective ageing management throughout the service life of the SSCs requires the use of a systematic approach to managing ageing that provides a framework for coordinating all programmes and activities relating to the understanding, control, monitoring and mitigation of ageing effects of the plant component or structure.

Understanding the ageing of Systems, Structures and Components, as illustrated in Figure 1, is the key to its effective ageing management. This understanding is derived from knowledge of: the design basis (including applicable codes and codes and cycle to the ageing management of the SSCs. The design basis (including applicable codes and standards); safety functions; the design and fabrication (including the material, material properties, specific service conditions, manufacturing inspection/examination and testing); equipment qualification (where applicable); operation and maintenance history (including commissioning, repair, modification and surveillance); generic and plant specific operating experience; relevant research results; data and data trends from condition monitoring, inspection and maintenance.

The PLAN activity in Fig. 1 means coordinating, integrating and modifying existing programmes and activities that relate to managing the ageing of a structure or component and developing new programmes, if necessary.

The DO activity in Fig. 1 means minimizing expected degradation of a structure or component through its ‘careful’ operation or use in accordance with operating procedures and technical specifications.

The CHECK activity in Fig. 1 means the timely detection and characterization of significant degradation through inspection and monitoring of a structure or component, and the assessment of observed degradation to determine the type and timing of any corrective actions required.

The ACT activity in Fig. 1 means the timely mitigation and correction of component degradation through appropriate maintenance and design modifications, including component repair and replacement of a structure or component. The closed loop of Fig. 1 indicates the continuous improvement of the ageing management programme for a particular structure or component, on the basis of feedback of relevant operating experience and results from research and development, and results of self-assessment and peer reviews, to help ensure that emerging ageing issues will be addressed.

Nuclear power plant safety can be impaired if obsolescence of SSCs is not identified in advance and corrective actions are not taken before associated declines occur in the reliability or availability of SSCs. Management of obsolescence is a part of the general approach for enhancing nuclear power plant safety through ongoing improvements of both performance of SSCs and safety management.

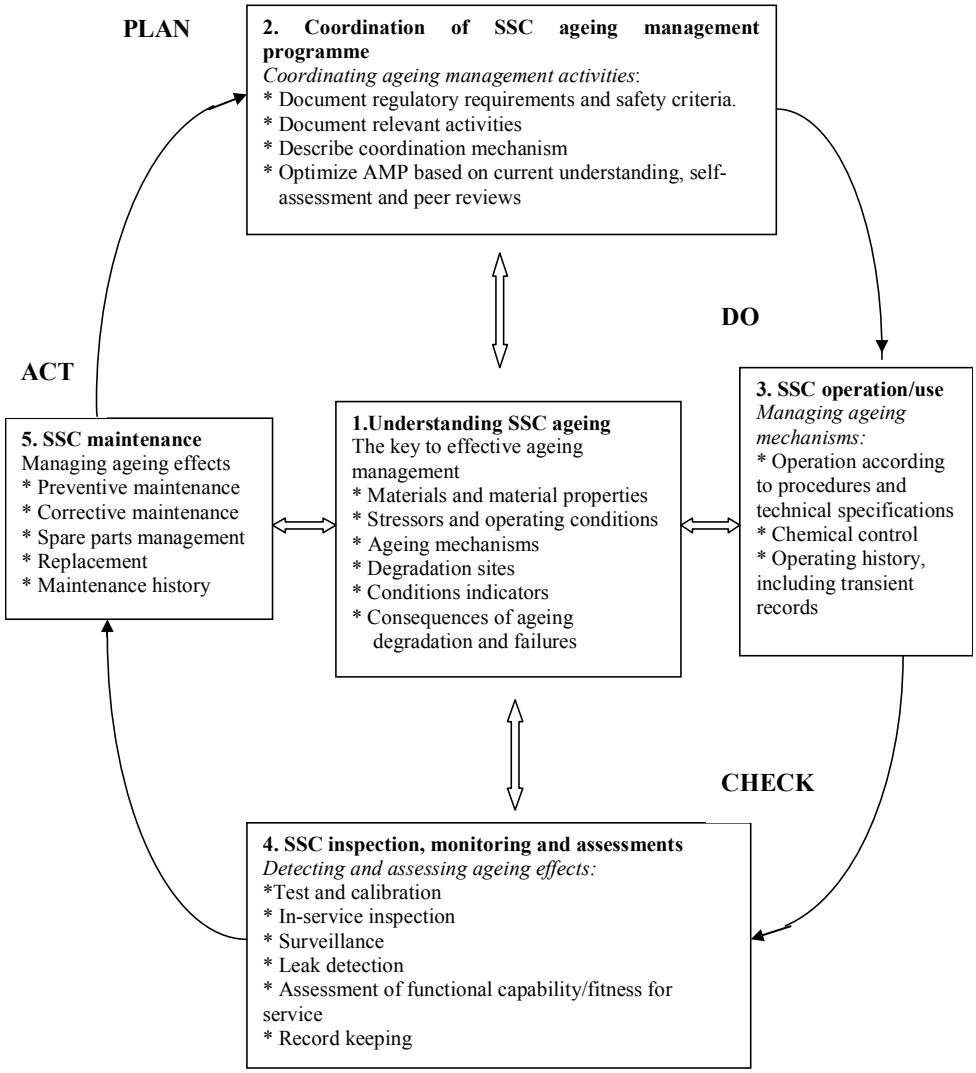

FIG.1. Understanding the ageing of Systems, Structure and Components.

3. ATUCHA TYPE NUCLEAR POWER PLANTS

Atucha I and Atucha II (see Table 1) Nuclear Power Plants (NPPs) are unique in design all around the world and have particular features that hinder the execution of accurate predictions on ageing of Systems, Structures, and Components (SSCs) due to the lack of international experience available to refer.

3.1. Atucha I Nuclear Power Plant

Atucha I has been in operation since 1974 and is close to reach its design life. The design of an integrated Plant Life Management Program for this NPP has recently started. In accordance with the national priorities the Atomic Energy Commission (Comision Nacional de Energia Atomica – CNEA) is developing the Life Management and Life Extension Programs of Argentinean Nuclear Power Plants. At the moment CNEA is working on the design of a single approach for Aging Management of both Atucha I and Atucha II Nuclear Power Plants, considering the peculiar characteristics of the plants.

TABLE 1. ATUCHA I AND ATUCHA II NUCLEA POWER PLANTS

	Atucha I	**Atucha II**
Designer	Siemens AG	Siemens AG
Status	Commercial activity since 1974	Under construcion
Gross power	370 MWe	740 MWe
Reactor type	Pressurized heavy water reactor (PHWR)	Pressurized heavy water reactor (PHWR)
Fuel channels	252 vertical	NA
Fuel	natural Uranium (UO2), low enriched uranium (0.85 % 235U) in-service reloading	natural Uranium (UO2), in-service reloading
Moderator & coolant	Heavy water (D_2O)	Heavy water (D_2O)

The technology to be used consists of the methodologies specifically developed for the assessment of ageing issues within the nuclear industry. These methodologies allow for the correct selection of the SSCs to be included within the scope of the PLIM program and provide guidance on how to design proper Ageing Management Programs to ensure high standards of safety and reliability [4, 5].

3.2. Atucha II Nuclear Power Plant

Atucha II NPP construction was completely stopped in 1995 after many delays. In 2006 the assembly of the Atucha II Nuclear Power Plant was restarted with the in service operation scheduled for 2014. The implementation of the Plant Life Management Program for the plant was also delayed; along with the plant construction. The situation of Atucha NPPs makes it extremely important to have in place a single PLIM approach for both plants in order to have:

a) The best information of Atucha I available to be used as both the experience base for Atucha II PLIM and the business case of a possible Long Term Operation (LTO) of Atucha I NPP [6] [7] [8].
b) The effects of the construction delay on the condition of Atucha II SSCs assessed; and ensure the availability of the necessary information to make up the base line for the future analysis of SSCs degradation.

By way of example below we list a set of security-related systems that were included in the ageing management programme.

- Safety Actuation Systems: boron injection systems, moderator system, safety injection systems, cooling system of moderator cooler, volume control system and secured service cooling water system.
- Protection Systems: electrical I&C systems, local panel of emergency control station, in-core instrumentation, ex-core instrumentation, reactor protection system and radioactivity monitoring system.
- Safety related items: pressurizing and cooling system for refuelling machine, primary cooling system, feed water system, starts up and shut down system, fuel

assembly monitoring system, boric acid dosing system, coolant and moderator purification system. Pool cooling fuel system and fuel pool purification system.

3.3. Atucha I Spend Fuel Storage

Fuel elements characteristics:

- Fuel type: Natural uranium dioxide
- Number of fuel elements: 252
- Number of fuel rods: 36
- Fuel weight: 152.5 kg U/ assembly
- Total weight: 210 kg
- Fuel rod length: 5650 mm
- Active length: 5295 mm
- Total length: 6180 mm
- Cross-section diameter: 108 mm
- Cladding material: Zircaly-4
- Structural components (head and foot): Austenitic steel
- Spacer: Inconel

From August 2001, all the fuel of Atucha I is uranium dioxide, with slightly (0.85%) enriched U. The burn up increase from 5900 MWd/Tu to 11300 MWd/Tu and the numbers of fuel elements used per year decreased from 430.3 to 230.

Used fuels elements are stored in the places where the reactors are situated. Atucha I has two pools houses where about 11.800 spent fuels is accumulated so far. Pool House 1 has three individual pools, one is for operations, the other two are decay and storage pools. Pool House 2 has five pools, one for operation and four for decay and storage. The supporting structures of the pools are made of concrete with stainless steel liners.

Purification and cooling water system of the pools was designed to maintain the temperature of the storage pool below the 32 °C, under normal conditions of operation and to maintain the purity and cleaning of the water to allow observation during the handling operations of the used fuel under the water. To provide an appropriate capacity of extraction of radioactive material in suspension and dissolved in water to allow access to the work areas and to maintain a level of water minimum in the pools to assure appropriate shielding during all the phases of the handling procedures and storage of used fuel.

The fundamental point here is to keep in mind that the effects of ageing produce changes in the characteristics of a System, Structure or Component (SSC); for that reason formal processes of Figure 1 are used to systematically identify and evaluate the Critical Systems, Structures and Components (CSSCs) in the facility [9].

4. CONCLUSIONS

The best way to meet these premises of effectiveness of the barriers is to develop an ageing management programme to prevent potential failures and accidents. Therefore, the fundamental point here is to keep in mind that it is the effects of ageing due to time and use that cause net changes in the characteristics of a System, Structure and Component (SSC) was

used a formal processes to systematically identify and evaluate the Critical Systems, Structures and Components (CSSCs) in the facilities. Afterwards, a plan was applied to ensure the facilities surveillance, operation, and maintenance programs, monitoring and control of the component degradation within the original design specifications, essential for the facilities life attainment. Purification and cooling water system doesn't present degradation signs.

For all the structures in either pools we carried out visual inspection; it showed that fissures, ruptures or shelling are not present. The pools liners do not show signs of corrosion. The metal structure does not show signs of corrosion and the storage racks do not show degradation signs.

The facility can be operated safely for long term with the normal inspections, surveillance, maintenance and replacements. All this information must be retained for the entire life of the storage facility.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1, INSAG-12, IAEA, Vienna (1999).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, International Experts Meeting organized in connection with the implementation of the IAEA Action Plan on Nuclear Safety, Vienna (2012).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2012).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management for Nuclear Power Plants, IAEA Safety Standards, Safety Guide No. NS-G-2.12, IAEA, Vienna (2009).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safe Long Term Operation of Nuclear Power Plants, Safety Reports Series No. 57, IAEA, Vienna (2008).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Proactive Management of Ageing for Nuclear Power Plants", Safety Reports Series No. 62, IAEA, Vienna (2010).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Integrity of Reactor Pressure Vessels in Nuclear Power Plants: Assessment of Irradiation Embrittlement Effects in Reactor Pressure Vessel Steel, Nuclear Energy Series No. NP-T-3.11, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment and Management of Ageing of Major Nuclear Power Plant Components Important to Safety: PWR Pressure Vessels, IAEA-TECDOC-1556, IAEA, Vienna (2007).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Understanding and Managing Ageing of Materials in Spent Fuel Storage Facilities, Technical Report Series No. 443, IAEA, Vienna (2006).

COMMISSIONING AND OPERATIONAL EXPERIENCE IN POWER REACTOR FUEL REPROCESSING PLANT

S. PRADHAN
Tarapur Based Reprocessing Plant,
Bhabha Atomic Research Centre,
Tarapur, India
Email: spradhan@barctara.gov.in

Abstract

After completing design, construction, commissioning, operation and maintenance experience of the reprocessing plants at Tarapur, Mumbai and Kalpakkam a new reprocessing plant is commissioned and put into operation at BARC, Tarapur since 2011. Subsequent to construction clearance, commissioning of the plant is taken in many steps with simultaneous review by design and safety committees. In spite of vast experience, all the staff was retrained in various aspects of process and utility operations and in operation of innovative changes incorporated in the design. Operating personnel are licensed through an elaborate procedure consisting of various check lists followed by personnel interview. Commissioning systems were divided in sub-systems. Sub-systems were commissioned independently and later integrated testing was carried out. For commissioning, extreme operating conditions were identified in consultation with designers and detailed commissioning procedures were made accordingly. Commissioning was done in different conditions to ensure safety, smooth operation and maintainability. Few modifications were carried out based on commissioning experience. Technical specifications for operation of the plant are made in consultation with designers and reviewed by safety committees. Operation of the plant was carried out after successful commissioning trials with Deep Depleted Uranium (DDU). Emergency operating procedures for each design basis accident were made. Performance of various systems, sub-systems are quite satisfactory and the plant has given very good capacity factor.

1. INTRODUCTION

India's long term energy security is based on its closed fuel cycle policy and the three-stage nuclear program to utilize its large reserves of thorium as reactor fuel. The strategy is to use natural uranium in heavy-water reactors followed by plutonium-fuelled fast neutron reactors that would breed the thorium to U-233 required for an ultimate energy security. Low reserves of uranium and high reserves of thorium mandated India to adopt reprocessing and recycle of uranium and plutonium as feed stock for future nuclear reactors. Thus, for India the spent fuel is the vital resource material and not waste to be disposed of. The recycling and optimal utilization of Uranium is essential to meet the country's current and future energy security needs. The key to all this is advanced capabilities in reprocessing of spent nuclear fuels to separate TRU wastes from materials that will be fuels for other reactors. India has come a long way in fuel reprocessing of spent fuel since its first reprocessing in 1964 at Trombay. The experience gained in construction, commissioning and operation of this first reprocessing plant has given confidence towards aiming the growth of spent fuel reprocessing capability. The reprocessing facilities at Tarapur and Kalpakkam have demonstrated India's ultimate capability in spent fuel reprocessing and its energy security. For the purpose of boosting India's reprocessing capacity a new reprocessing plant (100 T capacity zircalloy clad oxide spent fuel using chop-leach technique for the head end) has been commissioned and put into operation at BARC, Tarapur since 2011. A view of the reprocessing plant is given in Fig.1.

FIG.1. Tarapur reprocessing plant.

2. FEATURES OF NEW REPROCESSING PLANT

2.1. Automated Charging Facility (ACF)

Indigenously developed ACF is used for charging of spent fuel bundles from charging cask to spent fuel chopper inside dissolver cell. The system operates on a PLC controlled environment, which has a servo pusher, mechanical couplers for push rods and indexing system for alignment of push rods. ACF helps in i) reduction in time cycle of charging and thereby, (ii) increase in Efficiency of the Head End System, (iii) reducing contact operations & manpower requirement, and (iv) reduction in radiation exposure of operating personnel.

2.2. Spent Fuel Chopper (SFC) Based on Gang Chopping Concept

Indigenously developed hydraulic machine (SFC) first time installed in new reprocessing plant is based on gang chopping concept, i.e., cutting of a spent fuel into multiple segments in single stroke. This helps in (i) reducing time for chopping of spent fuel, (ii) produces non-pinched perfect cut ends of chopped pieces aiding for complete dissolution, and (iii) reduced clad fines. The hull after dissolution is shown in Fig.2.

2.3. Modified Feed Clarification System

For filtration of dissolved contents, vacuum assisted fine filtration system is introduced. This system provides quick and efficient filtration.

2.4. Installation of high through put columns for solvent extraction

Higher diameter extraction columns designed for continuous organic phase with internal nozzle plates for higher efficiency of extraction are introduced.

FIG. 2. Chopped spent fuel.

2.5. High efficiency Thermosyphon evaporators (TSE)

Higher boil-up rate thermosyphon evaporators are designed and introduced. An additional safety feature of expansion bellow is provided to heat exchanger to avoid equipment failure.

2.6. Inter-cycle hold up capacity

Sufficient hold up tanks have been provided in between the cycles such that each cycle is independent of previous cycle operations. This provides uninterrupted cycle operations and sufficient time for maintenance thereby reduced down-time.

2.7. Redundant Evaporators

Stand-by evaporators have been introduced for each cycle of operation.

2.8. Multiple and flexible transfer routes

Separate transfer routes for product and off-grade product were provided to avoid downtime of operations. Different types of transfer modes like ejector, air-lift, vacuum, gravity and pump modes were provided. Minimum two types of transfer modes along with redundant modes were provided for each transfer operation.

2.9. Use of Indigenously Developed Remote Head metering Pumps

For the safety of the working personnel and pumping of metered radioactive solution remote head concept is used. A remote head is a diaphragm pump kept in a shielded enclosure away from the plunger system and connected hydraulically by a pipe.

2.10. Extended pump cubicles for remote maintenance of metering pumps

Indigenously developed maintenance vehicle is a shielded motorized moving enclosure used for remote maintenance of pump cubicles. Use of maintenance vehicle reduces man-Rem consumption.

2.11. Advanced solvent cleaning system

Advanced solvent cleaning system for cleaning of solvent to remove degraded products after certain batches of operation was introduced and this system reduces organic waste generation.

2.12. Seismically qualified interim waste storage tanks

High capacity seismically qualified interim waste storage tanks were introduced for storing HLLW, ILLW solutions.

2.13. Advanced Instrumentation and control system

First time in Indian reprocessing plant, SCADA (Supervisory Control and Data Acquisition) system is introduced with standby server. With experience gained from previous plants, alarm and interlock systems are introduced using PLC system with standby and passive safety features. Electronic transmitters are used to transmit signals from field to Control Room which reduces loss of signal. To shutdown plant in the event of damage to main plant control room due to earth quake, an Emergency Control room with important parameters and controls is established in seismically qualified process building.

2.14. Physical Protection system

Protection system such as CCTV in vital areas, turnstile gates with control access requiring RF Identification Cards with biometric identification, electric fencing, road blockers, tyre-killers, active bollards, etc. are installed to avoid unauthorized access to plant areas.

3. DEFENCE-IN-DEPTH MECHANISM

Defence-in Depth mechanism is adopted for the important systems in the new reprocessing plant.

a) *Control of runaway reaction:* Dissolvers are provided with emergency cooling provision in case of runaway reaction during dissolution. Primary cooling system is designed to take care of the heat generated during runaway reaction. In case of black out condition once through cooling system is provided which cools the dissolver content till the temperature reduces to room temperature there by controls the rate of dissolution.
b) *Control of Criticality*: All plutonium purification cycle tanks are designed to annular tanks as per criticality considerations. In addition to this concentration control is maintained for each plutonium storage tank. Interlocks are provided for all transfers to avoid mal-operation conditions.
c) *Control of Red Oil Explosion*: The aqueous feed solution to evaporators is passed through diluents washer column to remove entrained organic present. In addition to this the temperature of the evaporation is maintained below 135^{o}C by limiting the steam pressure to less than 1.8 kg/cm^2 using two parallel pressure regulating valves(PRVs). Also, steam safety valve set at 2.0 kg/cm^2 is provided in the circuit to vent steam in case of failure of PRVs.

4. REGULATORY CLEARANCES

Regulatory clearance for installation of new reprocessing plant was obtained for

a) Site clearance.
b) Environmental clearance.
c) Civil structure clearance.
d) Construction clearance for equipment installation and piping.
e) Stage wise clearance for commission – cold, DDU and hot.
f) Regular operational clearance.

5. CONSTRUCTION

Design of new reprocessing plant was done through rigorous evolution of safety subsystems at every stage of the plant operation. All possible design basis accidents are addressed while designing the plant. Meticulous design review was carried out by Design Safety Review Committee (DSRC) and all recommendations of DSRC were incorporated during design and construction phases. All the construction activities were completed before scheduled target with stringent Quality Assurance Program.

6. TRAINING, COMMISSIONING & OPERATION

After completion of all construction activities, Commissioning of entire plant systems was carried out by adopting Systematic Quality Plan Program (SQPP). The SQPP includes categorization of commissioning activities of plant systems into Cold Commissioning and Hot Commissioning. Before cold commissioning all major systems are divided into sub-systems and each sub-system is checked for the following:

- Compliance of construction with design intent.
- Compliance of all piping and relevant equipment and components as per approved drawings.
- System integrity checking.
- Preparation of commissioning procedures (CP) and commissioning reports (CR).
- Approval of all sub-systems by DSRC based on the physical verification and objective evidence of QA documents.

6.1. Training

Since the plant is equipped with new superior instrumentation and control systems like process SCADA, PLC alarms, RMS-SCADA, PA system and improved physical protection systems like CCTV coverage in vital areas and control access requiring RF identification cards with biometric identification etc., all working groups are provided with sufficient training to manage and maintain the systems always in healthy condition. License to operators to operate systems was given after rigorous training and qualification.

6.2. Cold Commissioning

All systems and components are subjected for worst design operating conditions and ensured their maintainability and reliable operation. For easy operability of equipment modification were carried out in some of the systems like head-end and auxiliary service systems. Technical Specifications for the plant were prepared in consultation with designers

and reviewed in safety committees. During cold commissioning each subsystem is subjected to the following:

- Ensured functioning of remote maintenance systems for head-end equipment and Pump cubicles.
- Checking of connectivity & negative slope of piping. Rectification of minor deficiencies such as inadequate slope of gravity transfer mode systems.
- Flushing of all lines and equipment.
- Calibration of all process tanks and instrument parameters.
- Functional checking of all transfer modes and equipment with DMW.
- Ensured all functioning of all interlocks
- Establishment of flow rates, evaporation rates, pulsing parameters, efficiency of filter clean-up systems, indications, controllers and safety interlocks, and calibration of radiological monitoring systems,

6.3. Hot Commissioning

After obtaining clearance for processing of Deep Depleted Uranium (DDU), all operations such as chopping, dissolution, filtration, first, second and third solvent extraction cycles were carried out and established all the process parameters. Subsequently hot fuel was chopped and processing continued.

- Initial solvent extraction operations carried out with DDU feed and Tri-Butyl Phosphate (TBP) as extractant.
- Established flow rates with required loading in TBP.
- Performance of individual columns with respect to losses and decontamination factor was satisfactory.
- Standardization of the all operating parameters has been achieved.
- Optimization of process parameters for improved performance, attaining the nameplate capacity with sustained operations.

6.4. Regular Operation

Performance of various systems, sub-systems are quite satisfactory and plant has given very good capacity factor with good quality product. Plant has operated with good safety record with respect to low environmental releases, less waste generation and low per-mSv exposure.

7. CONCLUSIONS

The successful commissioning and operation of the new Power Reactor Fuel Reprocessing plant is based on the vast experience gained in design, construction and operation of earlier reprocessing plants. Demonstrated and regular performances of indigenously developed reprocessing plant's equipment, components and systems have enhanced India's spent fuel reprocessing capability. The safety standards maintained in new Power Reactor Fuel Reprocessing plant is at par with the international safety standards. Now the debut to the second stage nuclear power program of India has been substantiated by the successful operation of new spent fuel reprocessing plant with its intended through put capacity.

THE ROLE OF COUNTERMEASURES IN MITIGATING THE RADIOLOGICAL CONSEQUENCES OF NUCLEAR POWER PLANT ACCIDENTS

F. S. TAWFIK, M.M. ABDEL-AAL
Siting & Environmental Department,
Nuclear and Radiological Regulatory Authority,
Cairo, Egypt
Email: basant572000@yahoo.com

Abstract

During the Fukushima accident the mitigation actions played an important role to decrease the consequences of the accident. The countermeasures are the actions that should be taken after the occurrence of a nuclear accident to protect the public against the associated risk. The actions may be represented by sheltering, evacuation, distribution of stable iodine tablets and/or relocation. This study represents a comprehensive probabilistic study to investigate the role of the adoption of the countermeasures in case of a hypothetical accident of type LOCA for a nuclear power plant of PWR (1000 Mw) type. This work was achieved through running of the **PC COSYMA**[1] code. The effective doses in different organs, short and long term health effects, and the associated risks were calculated with and without countermeasures. In addition, the overall costs of the accident and the costs of countermeasures are estimated which represent our first trials to know how much the postulated accident costs. The source term of a hypothetical accident is determined by knowing the activity of the core inventory. The meteorological conditions around the site in addition to the population distribution were utilized as input parameters. The stability conditions and the height of atmospheric boundary layers ABL of the concerned site were determined by developing a computer program utilizing Pasquill-Gifford atmospheric stability conditions. The results showed that, the area around the site requires early and late countermeasures actions after the accident especially in the downwind sectors. For late countermeasures, the duration of relocation ranged from about two to 10 years. The adoption of the countermeasures increases the costs of emergency planning by 40% but reduces the risk associated with the accident.

1. INTRODUCTION

PC COSYMA [1] is a probabilistic and/or deterministic code for accident consequence assessment used in calculating the risk posed by postulated nuclear accidents involving release to the atmosphere, taking into account the range of conditions, which may prevail at the time of the accident. The code was used under license agreement with the EC through NRPP, UK, 2001. The code was used to assess the off-site radiological and economic consequences of accidental atmospheric releases of radioactive materials with and without countermeasures. For deterministic assessment, it gives detailed results for a single set of atmospheric conditions, while for probabilistic assessment gives results taking into account the full range of atmospheric conditions.

In the present study, the probabilistic assessment used to carry out the calculations in locations with population. The endpoints of the system can be considered in two groups; referring to conditions at particular points or summed over the population. The first group includes endpoints such as air concentration, individual dose and individual risk. Information on these quantities for probabilistic runs can be presented in terms of the probability distributions at a specified point or at specified distances from the site. The second group includes endpoints such as the number of health effects in the population and the economic costs of the accident. Information on these quantities for probabilistic runs can be presented in terms of the probability distributions of the quantity in the affected population.

To some extent, countermeasures can be considered in both groups. Information can be presented in terms of the probability of imposing countermeasures at particular points or distances, and in terms of the numbers of people or areas affected by the countermeasures.

2. INPUT DATA

2.1. Atmospheric Conditions

The atmospheric conditions are critical factors in determining the spatial and temporal distributions of dispersed radionuclides. The collected hourly data for the whole year of 2006 of the proposed site is used. There were 8760 weather sequences. Stratified sampling utilized to carry out the calculations.

The distribution of wind direction and speed are considered to estimate the prevailing downwind direction; the WRPLOT code [2] was utilized for this purpose. The results indicated that the north direction is the prevailing wind direction, thus the south is the prevailing downwind sector.

An hourly basis of atmospheric stability conditions utilizing Pasquill-Gifford [3] and height of ABL of the site was determined [4]. The results revealed that, the stable conditions dominate among other conditions all over the year. In spring and summer, the unstable conditions were relatively high compared with the other seasons due to the increase of daily hour's sunshine. In addition, the mean average of hours at which the values of ABL is higher than 1500 m increased in the summer than in the other seasons, where the percent values of unstable conditions are high as compared with the other seasons.

2.2. Source Term

There are two methods of specifying the nuclides included. The first method is for the user to specify which nuclides he/she wishes to consider; the second method is to use a provided program with the system to choose those nuclides, which makes the largest contribution to dose from a list of those released in the accident.

In this study, the second method is used. The information of the core inventory of the PWR[(5)] was utilized in which only 40 nuclides according to their half-life and their important contributions are selected. The program then calculated a quantity related to the dose from each nuclide specified for each of the pathways of exposure considered and the sum of these quantities.

2.3. Population Distribution

PC-COSYMA includes data files giving population and agricultural production distributions on latitude and longitude grids; the information on the region of interest could be obtained by using a provided grids program.

There are two methodss; the first is to provide data on latitude, longitude grid with finer spacing used as input to the grids program. The second is to provide information on the distribution in distance bands and sectors around the site at short distances and combine this with information obtained from the grids program using the standard libraries at longer distances.

In this study, the second method was used to provide information on population only. The calculations were carried out without agricultural production distribution due to insufficient information.

3. RESULTS AND DISCUSSION

3.1. Countermeasures

The actions of early countermeasures are sheltering and evacuation, while relocation is a late countermeasure. Evacuation and relocation are means of moving people from their homes to avoid exposure. Evacuation is assumed to be implemented within a few hours of the accident, and would avoid exposure over the period for which people are away from their homes. Relocation, however, is assumed to be implementing over a period of a few days. Iodine tablets are assumed to be distributed automatically or according to dose level.

Tables 1a and 1b show the number of actions that are taken for 16 sectors at different distances. From table 1a, it is noticed that the actions of sheltering and evacuation take place automatically along distances up to 2.5 km in all sectors, and it takes place at distances greater than 3.5 km in downwind sector (sectors eight and nine).

Table 1b represents the pattern of iodine distribution, this action takes place automatically along distances up to 2.5 km in all sectors, while the same action takes place at a distance greater than 3.5 km in downwind sector based on dose level equals 0.02 Sv. Table 2 shows that the periods following the accident when resettlement was considered (the duration time of relocation). The duration time of relocation, found to be 7 days in regions close to the facility in all sectors except in the downwind sector. On the other hand, this time equals 10 years and 2 years in the regions close to the facility at down wind sectors.

TABLE 1. THE NUMBER OF ACTION FOR 16 SECTORS AT DIFFERENT DISTANCES

	(a) Sheltering + Evacuation 1 → Sheltering +evacuation automatically					(b) Iodine distribution 1 → Stable iodine automatically 2 → Stable iodine based on dose = 0.02 Sv				
Sector	Distance (km)					Distance (km)				
	0.5	1.5	2.5	3.5	4.5	0.5	1.5	2.5	3.5	4.5
1	1	1	1	0	0	1	1	1	0	0
2	1	1	1	0	0	1	1	1	0	0
3	1	1	1	0	0	1	1	1	0	0
4	1	1	1	0	0	1	1	1	0	0
5	1	1	1	0	0	1	1	1	0	0
6	1	1	1	0	0	1	1	1	0	0
7	1	1	1	0	0	1	1	1	0	0
8	1	1	1	1	1	1	1	1	2	2
9	1	1	1	1	1	1	1	1	2	2
10	1	1	1	1	1	1	1	1	0	0
11	1	1	1	0	0	1	1	1	0	0
12	1	1	1	0	0	1	1	1	0	0
13	1	1	1	0	0	1	1	1	0	0
14	1	1	1	0	0	1	1	1	0	0
15	1	1	1	0	0	1	1	1	0	0
16	1	1	1	0	0	1	1	1	0	0

TABLE 2. THE DURATION TIME OF THE RELOCATION

	1→ 7 days & 2→ 30 days & 3→ 90 days & 6→ 2 years & 8→ 10 years				
Sector	Distance (km)				
	0.5	1.5	2.5	3.5	4.5
1	1	1	1	0	0
2	1	1	1	0	0
3	1	1	1	0	0
4	1	1	1	0	0
5	1	1	1	0	0
6	1	1	1	0	0
7	1	1	1	0	0
8	8	6	3	1	1
9	8	6	6	2	1
10	1	1	1	0	0
11	1	1	1	0	0
12	1	1	1	0	0
13	1	1	1	0	0
14	1	1	1	0	0
15	1	1	1	0	0
16	1	1	1	0	0

3.2. Short and long-term individual Doses

The importance of countermeasures arises from the calculations of short individual dose in two cases with and without countermeasures. Tables 3a and 3b show the mean short-term individual dose for different organs at different distances in the two cases. It is noticed that the values in the first case are higher than the values in the second case. In addition, the absorbed doses of skin and thyroid have the highest dose values than other organs.

3.3. Late health effects

The CCDFs for numbers of late health effects in the population in both incidence and mortality are shows in Figures 1and 2, respectively. The numbers are greatest in the absence of countermeasures for the same probabilistic values. Countermeasures therefore, reduce mortality number in the population.

3.4. Risk of health effects

The CCDFs for long-term individual risk at 0.5 km and 1.5 km are shows in Figure 3. It is noticed that the probability at 0.5 km is higher than at 1.5 km for the same value of individual risk, where 0.5 km is the first distance located inside the working area around the plant; this value can be taken for operators, while the 1.5 km for the public.

TABLE 3. THE MEAN SHORT-TERM INDIVIDUAL DOSE VERSES DISTANCES FOR DIFFERENT ORGANS

a) Without countermeasures

Distance (km)	Effective	Thyroid	Eye lens	Ovaries	Skin	Lung	B.marrow	GI-tract
0.5	6.141E+00	3.498E+01	1.462E+00	1.775E+00	1.602E+02	1.815E+01	1.911E+00	7.330E+00
1.5	1.515E+00	5.732E+00	3.571E-01	4.510E-01	2.774E+01	5.319E+00	4.883E-01	2.107E+00
2.5	6.948E-01	2.149E-00	1.577E-01	2.033E-01	8.790E+00	2.612E+00	2.213E-01	1.025E+00
3.5	8.192E-01	2.009E+00	2.071E-01	2.447E-01	5.959E+00	2.921E+00	2.685E-01	1.160E+00
4.5	2.429E-01	8.923E-01	9.188E-02	9.100E-02	1.800E+00	7.397E-01	1.002E-01	3.116E-01

b) With countermeasures

Distance (km)	Effective	Thyroid	Eye lens	Ovaries	Skin	Lung	B.marrow	GI-tract
0.5	4.912E-02	4.995E-01	2.260E-02	1.967E-02	3.717E+00	3.967E-02	2.095E-02	3.151E-02
1.5	8.590E-03	7.827-02	4.023E-03	3.528E-03	5.931E-01	8.675E-03	3.772E-03	6.792E-03
2.5	3.065E-03	2.408E-02	1.440E-03	1.278E-03	1.887E-01	3.892E-03	1.372E-03	3.007E-03
3.5	1.651E-03	1.087E-02	7.464E-04	6.755E-04	9.020E-02	2.615E-03	7.292E-04	1.993E-03
4.5	7.999E-04	5.135E-03	4.032E-04	3.578E-04	4.151E-02	1.188E-03	3.856E-04	9.133E-04

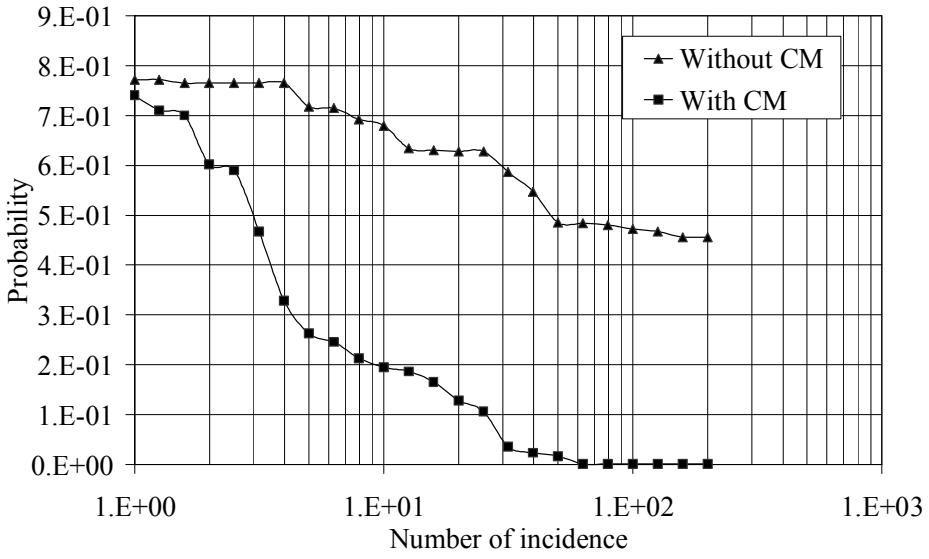

FIG. 1. The probability of number of late health effect (incidence).

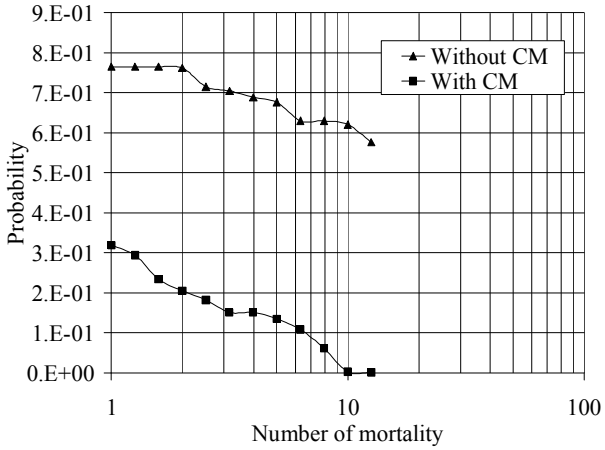

FIG. 2. The probability of number of late health effect (mortality).

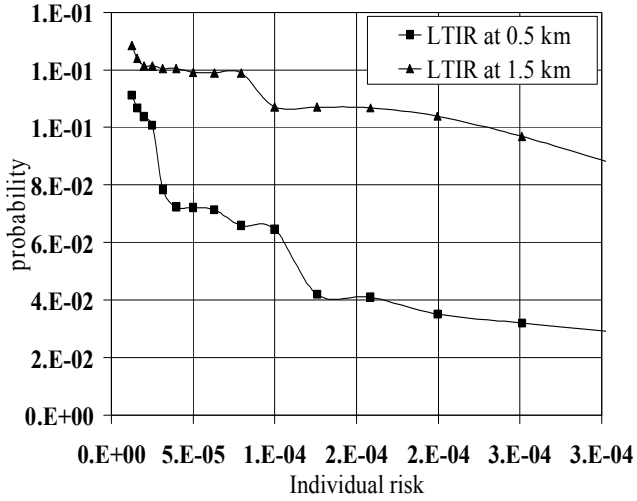

FIG. 3. CCDF's of long-term individual risk.

3.5. Economic costs

This is the first attempt to estimate the economic costs of a nuclear power plant accident. The overall costs and the costs of countermeasures for early and late health effects are shows in Figures 4 and 5. The cost in case of countermeasures is higher than the cost without countermeasures, but most of these costs arise for countermeasures. Without countermeasures, all costs are for late and early health effects. Therefore, countermeasures are increasing the costs but reduce the accident consequence.

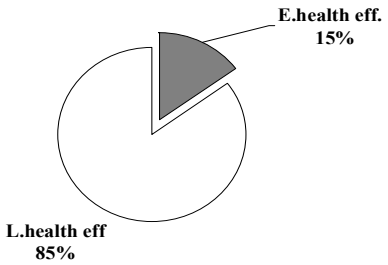

FIG. 4 Total cost = 7.248E+05 LE without countermeasures.

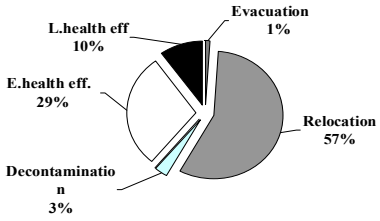

FIG. 5 Total cost = 1.375E+07 LE with countermeasures.

4. CONCLUSIONS

The actions of early and late countermeasures are very important, especially in the downwind sectors. The short individual dose values without countermeasures are higher than with countermeasures. For different organs, the skin and thyroid received the highest dose values than the other organs. Due to taking into consideration the countermeasures, the early health effects are very small and the late health effects are more important in case of mortality and incidence. The late individual risk was more important than the early risk near the plant and decreases with the distance. The economic cost is high with countermeasures but the countermeasures reduce the health and risk effects.

REFERENCES

[1] JONES, J.A., et al, PC Cosyma (Version 2): An Accident Consequence Assessment Package for Use on a PC, EUR 16239 EN, Luxembourg (1996).

[2] WRPLOT, NOAA, National Oceanic & Atmospheric Administrations, Environmental Research Laboratories, Idaho Falls, U.S.A. (1990).

[3] EVANS, J. S., MOELLER, D. W., and COOPER, D. W., Health Effects Models for Nuclear Power Plant Accident Consequence Analysis", NUREG/CR-4214, Rev 1, (1990).

[4] TAWFIK F. S., ABDELAAL M. M., Evaluation of Atmospheric Boundary Layer at Inshas Egypt, Isotope and Radiation Research, vol. 36, No. 4 (2004).

INSIGHTS FROM SEVERE ACCIDENT ANALYSES FOR VERIFICATION OF VVER SAMG

A. J. GAIKWAD, R. S. RAO, A. GUPTA, K. OBAIDURRAHAMAN
Nuclear Safety Analysis Division
Atomic Energy Regulatory Board, Mumbai, India
Email: avinashg@aerb.gov.in

Abstract

The severe accident analyses of simultaneous rupture of all four steam lines (case-a), simultaneous occurrence of LOCA with SBO (case-b) and Station blackout (case-c) were performed with the computer code ASTEC V2r2 for a typical VVER-1000. The results obtained will be used for verification of sever accident provisions and Severe Accident Management Guidelines (SAMG). Auxiliary feed water and emergency core cooling systems are modelled as boundary conditions. The ICARE module is used to simulate the reactor core, which is divided into five radial regions by grouping similarly powered fuel assemblies together. Initially, CESAR module computes thermal hydraulics in primary and secondary circuits. As soon as core uncovery begins, the ICARE module is actuated based on certain parameters, and after this, ICARE module computes the thermal hydraulics in the core, bypass, downcomer and the lower plenum. CESAR handles the remaining components in the primary and secondary loops. CPA module is used to simulate the containment and to predict the thermal-hydraulic and hydrogen behaviour in the containment. The accident sequences were selected in such a way that they cover low/high pressure and slow/fast core damage progression events. Events simulated included slow progression events with high pressure and fast accident progression with low primary pressure. Analysis was also carried out for the case of SBO with the opening of the PORVs when core exit temperature exceeds certain value as part of SAMG. Time step sensitivity study was carried out for LOCA with SBO. In general the trends and magnitude of the parameters are as expected. The key results of the above analyses are presented in this paper.

1. INTRODUCTION

VVER-1000 MWe is a light water cooled, light water moderated reactor. Reactor core consists of hexahedral fuel assemblies (FAs) and each FA comprises of number of fuel elements. The primary circuit consists of reactor core, downcomer, lower plenum, upper plenum and four loops. Each loop has a reactor coolant pump (RCP) set, hot leg and cold leg. Pressuriser is connected to hot leg of the 3rd loop and spray lines of the pressuriser are connected to the cold leg of the 4th loop. Three pulse safety devices (PSDs), one control and two safety PSDs are mounted on the pressuriser relief line.

The secondary circuit consists of four loops and each loop has a horizontal steam generator (SG) and four steamlines. Two pulse safety devices (PSDs), one main steam isolation valve (MSIV) and one electrical isolation valve are mounted on each steamline.

The reactor consists of reactor pressure vessel, core barrel, core baffle, in-core instrumentation detectors, protective tube units and other structures. The schematic of primary and various safety systems are shown in Fig. 1. The severe accident analysis for the following events was carried out using Accident Source Term Evaluation Code (ASTEC V2r2):

a) Simultaneous rupture of all four steamlines.
b) Simultaneous occurrence of LOCA and SBO.
c) Station blackout.

This paper deals with the in-vessel scenario analysis i.e., up to the vessel failure for the above cases. Furthermore, a detailed containment model was developed for a typical VVER-1000MWe. Containment thermal-hydraulic and hydrogen distribution analysis was carried out for the item (b) in addition to the above in-vessel scenario of severe accident analyses.

2. SEVERE ACCIDENT CODE - ASTEC

The computer code ASTEC [1] was jointly developed by IRSN and GRS for predicting the entire severe accident sequence from the initiating event to fission product release out of the containment. Source term determination studies, PSA Level 2 (PSA-2) studies, accident

management studies and detailed analyses of particular phenomena to improve the understanding of the phenomenology were main objectives of the development of the ASTEC code. The following ASTEC modules are used for the present analysis:

- CESAR for thermal hydraulics in the reactor coolant system.
- ICARE for core degradation up to vessel lower head failure.
- SOPHAEROS for fission product vapour and aerosol transport in the reactor coolant system.
- CPA for thermal hydraulics, aerosol and fission product behaviour inside the containment.
- SYSINT for management of engineered safety systems.

2.1. ASTEC Nodalisation

CESAR module of the ASTEC is used for simulating the thermal-hydraulics of the reactor vessel, primary coolant loops, steam generators and pressuriser. The ICARE module is used for simulation of the reactor core, which is divided into five radial regions by grouping similarly powered fuel assemblies together. Initially, CESAR module computes thermal hydraulics in primary and secondary circuits. As soon as the core uncovery begins, the ICARE module actuates based on certain parameters, and after this, ICARE module predicts the thermal hydraulics in the core, bypass, downcomer and the lower plenum. CESAR handles the remaining components in the primary and secondary sides. Fig. 1 shows the nodalisation diagram of the reactor vessel, primary piping, secondary circuit and pressuriser respectively.

The vessel model (Figure 1) represents all major components of the reactor vessel, including the downcomer, lower plenum, core, core bypass and upper plenum. The upper plenum is divided into two control volumes. The portion of the downcomer (DOWNCO1) is simulated as part of the primary structure. The remaining portion of the downcomer, lower plenum, parallel channels and core bypass are simulated using vessel degradation structure. The core is divided into five parallel channels, each consisting of fifteen sub-volumes. The structural components like baffle, barrel, spacer grids, fuel rods, control rods, guide tubes etc. were simulated using various components available in the vessel degradation structure. Heat structures/wall components are used to model the thermal behaviour of reactor vessel metal structures to simulate the heat losses. The flow paths between various control volumes are simulated using junction components.

Figure 1 also shows the nodalisation diagram of the first of the four primary coolant loops. This loop consists of one hot leg (simulated in two control volumes), hot collector, one steam generator (secondary side of SG is discussed subsequently), cold collector, pump suction leg (simulated into 3 control volumes), and cold leg. The primary side of the steam generator is represented by 3 parallel volumes with five cells in each volume. The pump is modelled as the pump component using SYSINT. The other three loops are clubbed into one loop and are similar to the first loop except pressurizer and ECCS connections. The pressuriser surge line is connected to the hot leg of the first loop. Heat structure/wall components are used to represent the thermal behaviour of the primary piping. The heat transfer between primary to secondary is simulated using wall components and CONNECTI structures. The connections involved between two modules e.g. upper plenum (UPPLE1) to various channels (CHAN1 to 5, CHANBYP) are connected through CONNECTI structures.

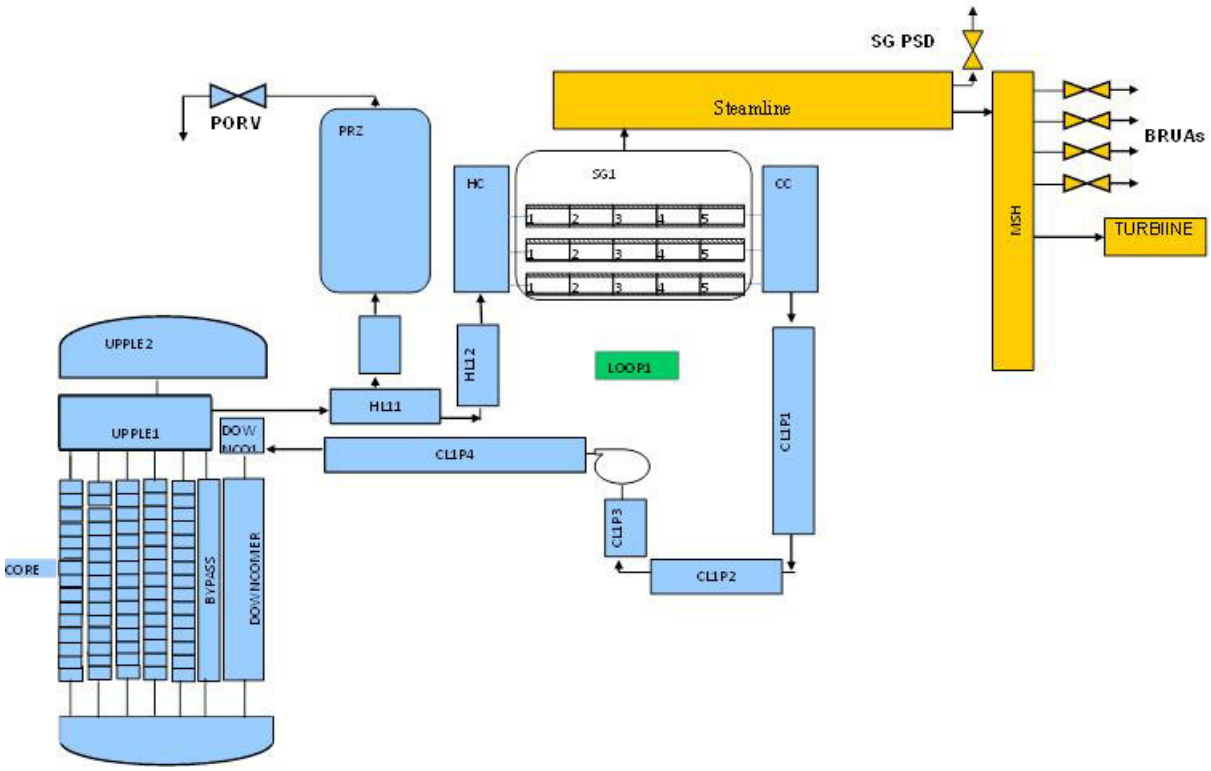

FIG. 1. VVER-1000 MWe nodalisation.

The reactor coolant pumps, accumulators, high pressure and low pressure injection systems, main feedwater, auxiliary feedwater are simulated using SYSTEMS structure and connected through CONNECTI. The high pressure and low pressure injection systems are simulated using boundary conditions. The pulse safety devices (PSDs) or relief valves mounted on the pressuriser and steam generator steamlines are simulated using SGVALVE type as these valves opening and closing times are different. Again these are connected through CONNECTIs. Atmospheric discharge valves (BRUAs) are also simulated using SGVALVE type.

Secondary side nodalisation is also shown in Figure 1. The secondary side of the SG is simulated using a single control volume. Steamline of the first loop is connected to SG. Similarly other three loops which are clubbed as one loop and are simulated using a single control volume. Both the steamlines i.e., single steamline and combined steamlines (3 loops) are connected to the main steam header (MSH) using junction structures.

The core is divided into five regions for this analysis by grouping similarly powered fuel assemblies together. Each Fuel Assembly (FA) consists of 311 fuel elements and each control rod and burnable absorber rod bundle consists of 18 elements.

To carry out hydrogen distribution detailed containment model has been developed using CPA module of ASTEC. Total containment volume is divided into 17 zones. Containment nodalization along mutually perpendicular sections AA and BB are shown in Figures 2a & 2b, respectively. Twenty six (26) connection structures are used to connect various zones. A total of 55 heat structures are used to simulate inner and external walls. Large break in primary is assumed to take place in C6 zone of containment. CONNECTI is used for interaction between primary circuit (CESAR) and containment (CPA). Various criteria used for modelling different phenomena in ICARE module are listed in Table 1. The criteria/models used for ICARE module activation, creep failure of clad, oxidation kinetics and vessel failure are shown in Table 1.

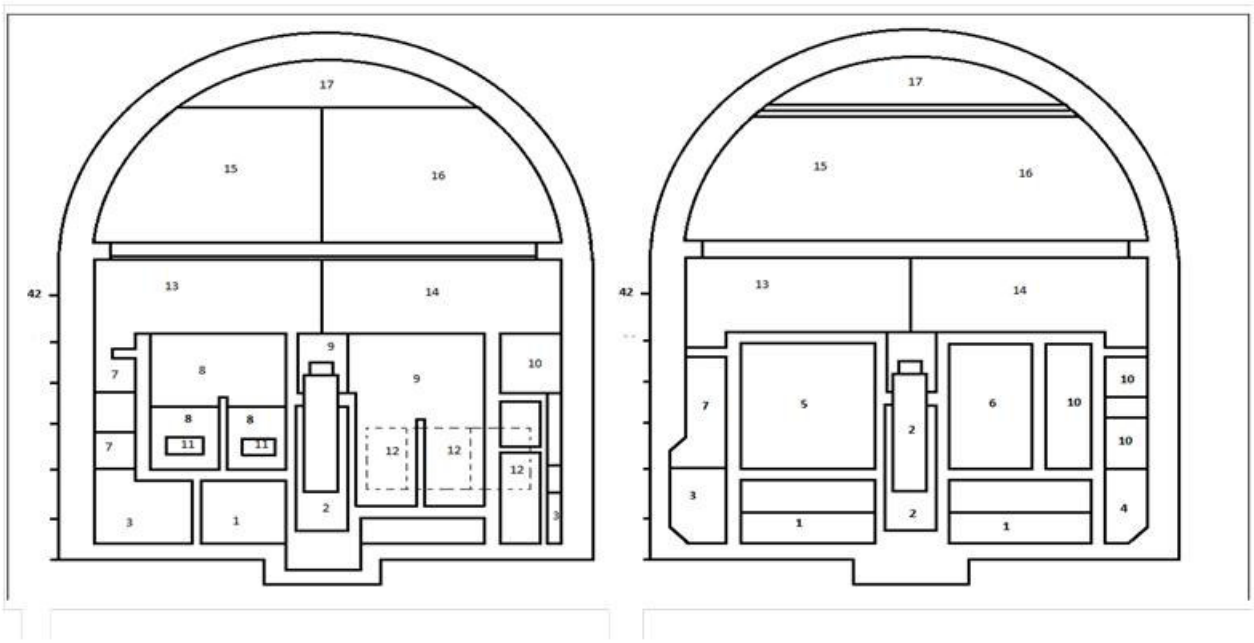

FIG.2a. Nodalization of containment (Section-AA).

FIG. 2b. Nodalization of containment (Section-BB).

TABLE 1. CRITERIA USED FOR VARIOUS PHENOMENA IN ICARE MODULE

Phenomena	Criteria/Correlations
Starting of ICARE module	Average void Fraction of Primary > 0.5 Void fraction of upper plenum and top of core > 0.925
Clad creep failure	Model developed by MIPhi for a typical VVER clad Criteria for creep failure, Hoop strain >δ_B (T) (Effective Burst strain) Where δ_B (T) is given below 293 < T <951 K, δ_B (T) = 2016.27-5.2948.T+0.00627. T^2-2.823*10^{-6}*T^3 951 < T <1190 K, δ_B (T) = 1.1614.10^6.exp(-0.0085753.T) 1190 < T <1493 K, δ_B (T) = 7.912. 103.exp(-0.004283.T)
Oxidation	**Zircaloy:** Best fit obtained from the CATHCART, URBANIC, PRATER and SOKOLOV **Steel:** Oxidation rate for different composition of steel Stainless steel 304 L (20% Cr, 12% Ni): J.F. White correlation Stainless steel N 1.4970 & 1.4914 (15% Cr, 15% Ni): Leistikov correlation
Vessel Failure	• User Defined Criteria o Maximum temperature > 1200 ^{0}C, Maximum molten fraction > 0.7 o Maximum mechanical stress >150 MPa • COMBESCURE rupture model o Instantaneous plastic rupture: Applied stress >$\sigma_{ultimate}$ o Creep rupture: Deformation rate >Rupture strain (Deformation velocity)

3. INITIAL CONDITIONS

Steady state 100% full power conditions were obtained using the above nodalization schemes. The initial conditions obtained from the steady state calculation are shown in Table 2 The key steady state parameters obtained are in agreement with nominal values for typical VVER-1000 MWe.

TABLE 2. INITIAL CONDITIONS

Parameter	Actual Value	Value (ASTEC)
Reactor thermal power, MW	3000.0	3000.0
Coolant temperature at reactor inlet, ^{o}C	291.0	289.71
Coolant temperature at reactor outlet, ^{o}C	321.0	319.77
Coolant pressure at the core outlet, MPa	15.7	15.7
Coolant flow rate through reactor, kg/s	86000 (m^3/h)	17622.4
Level in steam generator, m	2.4	2.38
Steam pressure at the SG outlet, MPa	6.27	6.27
Steam rate to turbine from each steam line kg/s	408	405

4. SIMULTANEOUS BREAK OF ALL MAIN STEAMLINES

4.1. Results and Discussion

The simultaneous double-ended rupture of all main steamlines is considered as an initiating event. The main steam isolation valves (MSIVs) are assumed to remain open during the accident progression. Scram occurs with a delay (both processing and instrument delay) of 1.5 seconds. The steam flows out through all the 4 steam lines following the breaks. Steam flow rate increases due to the large pressure difference across the break and attains critical flow. Sudden increase in flow through secondary side results in large heat removal from primary side, due to which pressure and temperature of primary decrease. The primary temperature reaches about 200^{o}C after steam line break from its steady state temperature of 322^{o}C as shown in Fig. 3. On the other hand as secondary pressure decreases turbine shut-off valves closes. Reactor coolant pumps (RCPs) trip on the secondary pressure less than 4.41MPa, saturation temperature difference between primary and secondary is greater than 75^{o}C and primary temperature is more than 150^{o}C with a delay of 1.5 seconds.

Steam generators dry out occurs due to loss of secondary inventory through steam line breaks. Due to combined effect of decay heat and loss of secondary inventory, primary pressure and temperature begin to rise as shown in Figures 3 and 4. Primary pressure is controlled by the opening (18.11 MPa) and closing (17.2 MPa) of PORV (pressurizer over pressure relief valve). ICARE module which deals with core degradation starts automatically based on void fraction in the primary at around 13212 s based of criteria discussed earlier. When the temperature of structural material reaches oxidation temperature metal water reaction starts. Rate of metal water reaction depends on availability of unreacted metal and its temperature and availability of steam/water. Cumulative H_2 produced due to metal water reaction is shown in Fig. 5. Due to combined heat generated from metal water reaction and decay heat, maximum surface temperature in the core increases as shown in Fig. 6. Melting of structural material starts as structural material temperature reaches their melting point. Melt pool formation is predicted to occur at around 16357 s. First slumping of the molten material to lower plenum occurs at around 24854 s. Loss of Primary inventory through PSD (PORV) ultimately leads to a total core uncovering at 24931 s. Corium mass accumulated in the lower plenum continues to heat the vessel and finally leads to lower head failure at around 44256 s based on temperature criteria.

Total mass of the corium in the lower plenum at the time of vessel failure is predicted to be about 18646 kg. Hydrogen produced during the accident scenario for the in-vessel phase is about 494 kg.

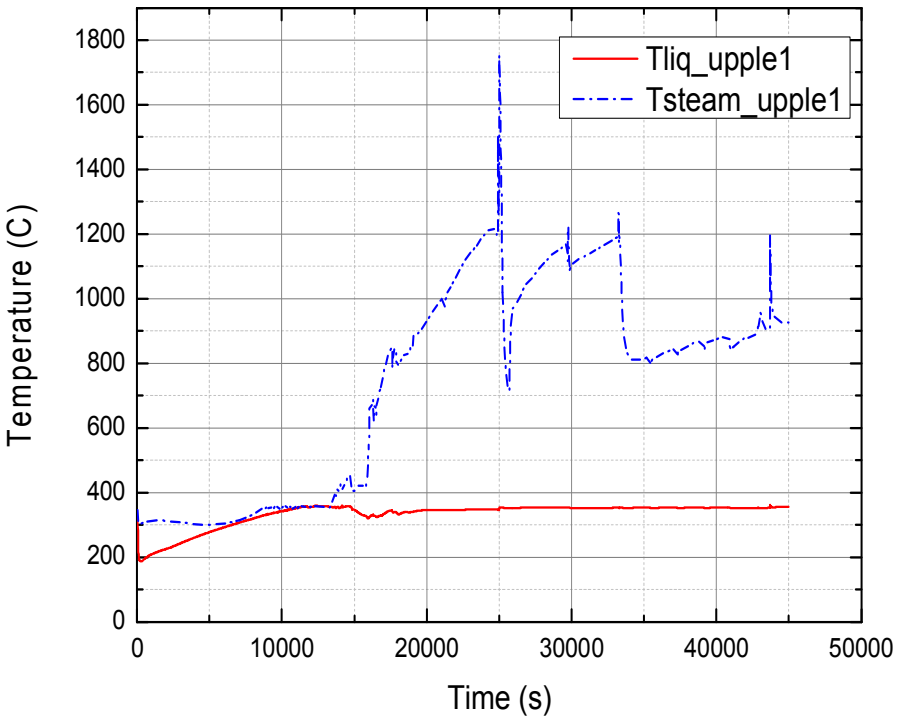

FIG. 3. Temperature of liquid and steam in upper plenum.

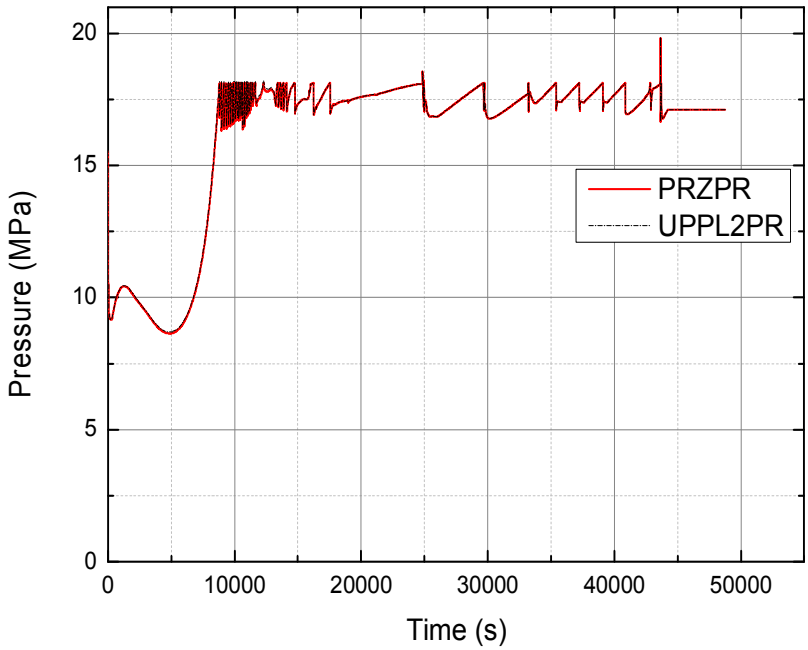

FIG. 4. Primary (pressurizer and upper plenum) pressure.

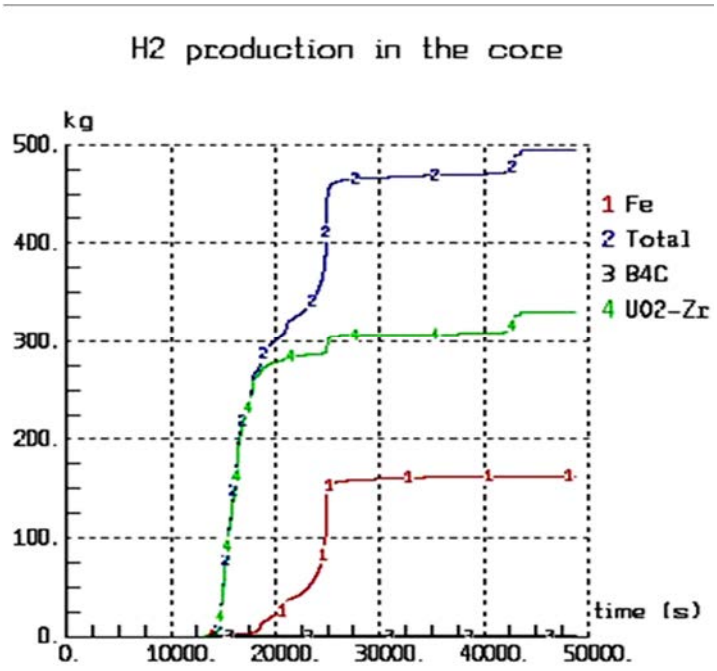

FIG. 5. Cumulative hydrogen generation.

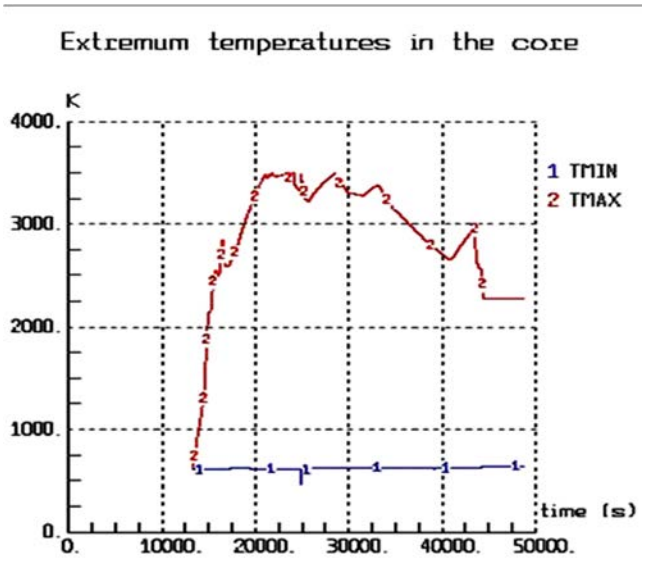

FIG. 6. Core extreme surface temperature.

5. LOCA WITH SBO

5.1. Results and Discussion

The double-ended rupture in the cold leg and station black out are assumed to occur simultaneously as an initiating event. Reactor coolant pumps (RCPs) trip, reactor scram, main feed water and auxiliary feed water pumps trip and pressuriser electrical heaters also trip due to complete loss of A.C. power supply. The turbine shut off valves also close due to SBO. Due to large pressure difference across the break primary flow reversal takes place in the broken cold leg and the primary flow rate increases till it attains critical flow. Further primary pressure (Fig. 7) is governed by the containment pressure. The maximum containment pressure reached due to LOCA is around 4.6bar

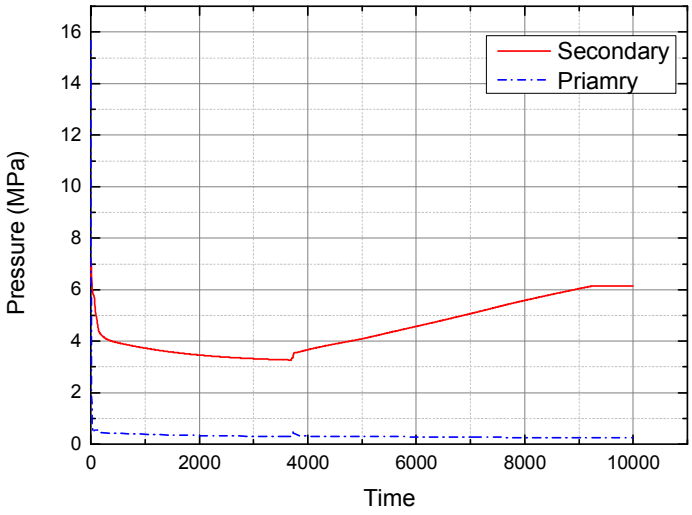

FIG.7. Primary and Secondary pressure.

As the cold leg break event coincides with the SBO, the active high-pressure and low-pressure emergency core cooling systems are unavailable. The passive hydro accumulators HA-I are considered to be available and actuate at primary pressure less than 5.89 MPa. The credit of second stage hydro accumulators and passive decay heat removal system designed for mitigation of severe accidents are not taken into account for this analysis. Due to injection of HA-I inventory in primary circuit from 4 to 100s, core maximum temperature decreases but later on it again increases due to unavailability of heat sink as shown in Fig. 8. Increase in temperature of the core results in further loss of primary inventory and melting of structural material. As a result, at 1667.4 s, the core gets completely uncovered and first slumping of corium to the lower plenum occurs at 1756 s. Metal water reaction rate increases momentarily due to slumping of corium mass in the lower plenum as shown in Fig. 9. As a result of oxidation heat and decay heat, fuel temperature continues to rise up to UO_2 melting temperature (3500 ^{O}C) as shown in Fig. 8. On the other hand, secondary pressure starts to increase at around 3700 s due to large heat generated from metal water reaction as shown in Fig 7. Corium mass that slumped into the lower plenum heats the RPV leading to its failure on temperature criteria at around 9269 s.

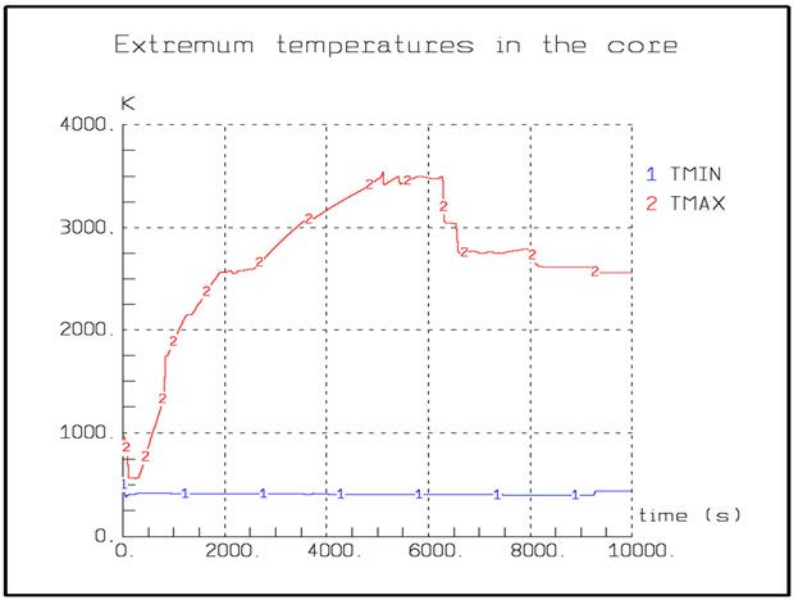

FIG. 8. Core extreme surface temperature.

The total amount of hydrogen generated due to metal water reaction is around 113 kg. Maximum hydrogen mole fraction shown in Figure 9 inside the containment during accident progression is less than 1%. Hydrogen mole fraction increases in zones C5, C7 and C2 after hydrogen gets generated in the core and released through the break in C6. Later, H_2 concentration increase in other zones due to mixing and redistribution. Increase in H_2 concentration is due to sudden increase in H_2 generation due to slumping of corium mass into the lower plenum. Hydrogen concentration in the topmost zone (dome), C17, keeps increasing as hydrogen is a lighter gas. The maximum local H_2 mole fraction during the accident progression is around 1 % (Figure 10), which is below the deflagration limits. This is because the total amount of H_2 generated during the LOCA+SBO scenario is quite less and is much less compared to other severe accident scenarios like MSLB and SBO due to steam lean atmosphere during the accident progression.

Two cases were analyzed with different time steps. The first case was analyzed with time step of 0.1 s up to 50 s, 0.5 s up to 1000 s and 1.0 s up to 10000 s. The second case was with the 0.1 s throughout the analysis. Trends of the core extreme temperature predictions are similar however with larger time step, the core temperature of 4100 K is predicted which is higher than the melting point of fuel. H_2 production and corium mass in the lower plenum prediction varied with time step.

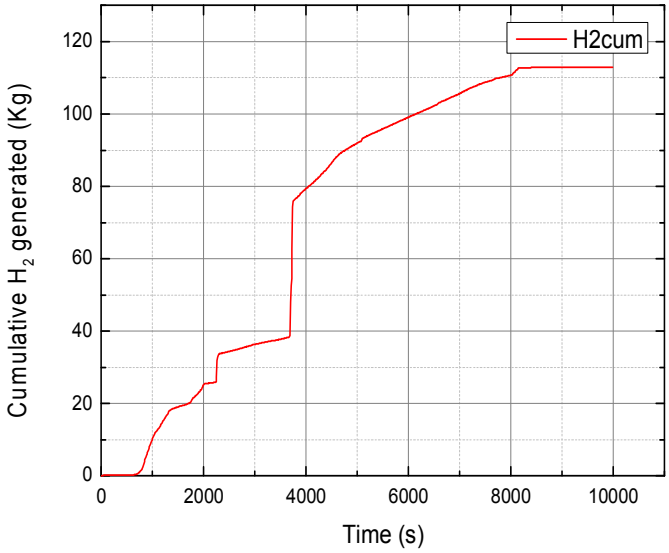

FIG. 9. Cumulative hydrogen generation.

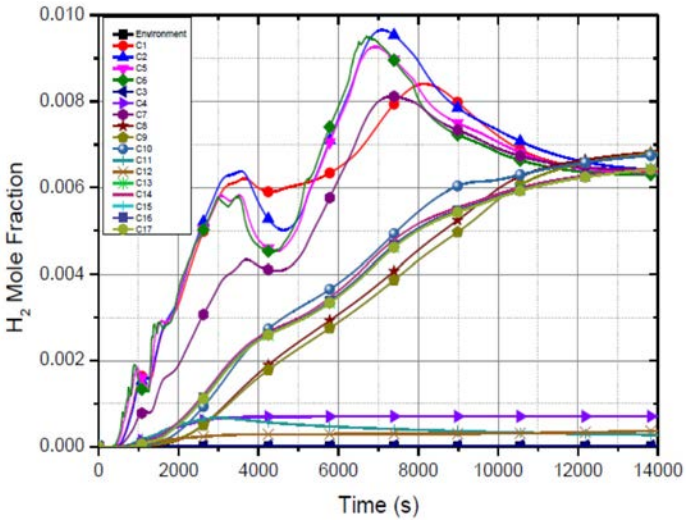

FIG. 10. Hydrogen distribution.

6. STATION BLACKOUT

6.1. Results and discussion

Station Blackout (SBO) results in trip of all RCPs, turbine and main feed water pumps. Reactor scram is initiated at 1.6s because of 3 out of 4 RCPs trip. This causes pressure and temperature in the primary and secondary to rise. Pressuriser-PSD (PORV) and SG-PSD open at regular intervals to relieve primary and secondary pressures as shown in Fig. 11. Heat removal from the primary decreases as the secondary inventory is lost through PSDs.

ICARE module starts automatically based on primary system void fraction at around 13508s. Oxidation of structural material (mainly Zircaloy) starts almost instantaneously after start of ICARE module as shown in Fig. 12. Heat generated due to metal water reaction is also added in the core leading to further increase in core temperature as shown in Fig. 13. Melting of structural material starts and molten pool formation in the core is predicted at 17056 s. Subsequently, due to loss of primary inventory, total core uncovery takes place at 21021.1 s. First slumping of molten material to the lower plenum occurs at 22467 s. The maximum core temperature reached during the accident progression is around 3500^{o}C (melting temperature of UO_2). On the other hand, corium that slumped to lower plenum increases the temperature of RPV and ultimately leads to failure of the lower plenum at 58450 s.

Total mass of corium in the lower plenum at the time of vessel failure is predicted to be about 7031 kg. Hydrogen produced during the in-vessel progression is 510 kg. SBO is a slow progressing and high pressure event. In order to avert high pressure melt ejection in high pressure scenarios like SBO, Pressuriser-PSD (PORV) is opened when primary fluid temperature reaches 650^{o}C and remains open thereafter. Primary system is depressurized when PORV is opened at 15995 s as shown in Fig. 14. Primary inventory further lost through PORV leading to complete core uncovery at 16042 s. Accumulators get actuated as primary pressure reaches below 5.89 MPa. Injection from the accumulator lasts up to 20099 s till accumulator level reaches a value less than 1.2 m. Core temperature begin to increase again. Total H_2 generation is predicted to be around 593 kg (Fig. 15).

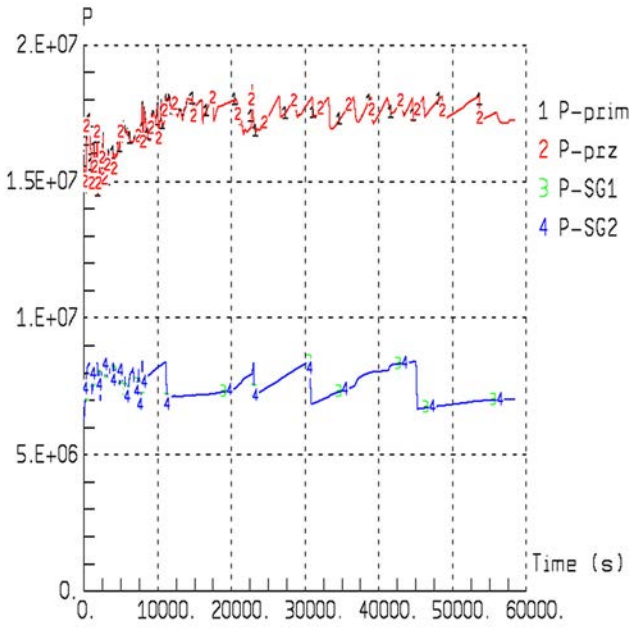

FIG. 11. Primary and Secondary Pressure.

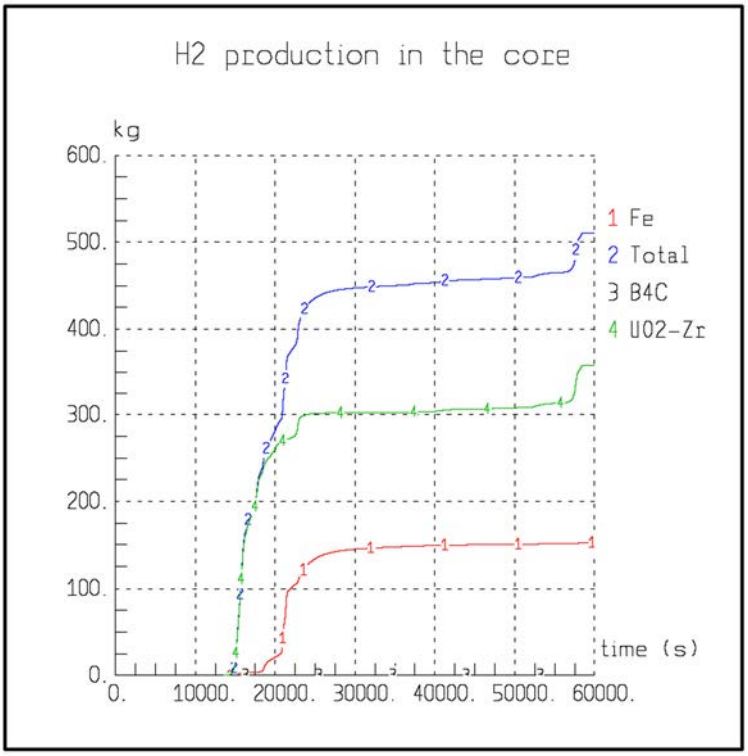

FIG. 12. Cumulative H_2 production.

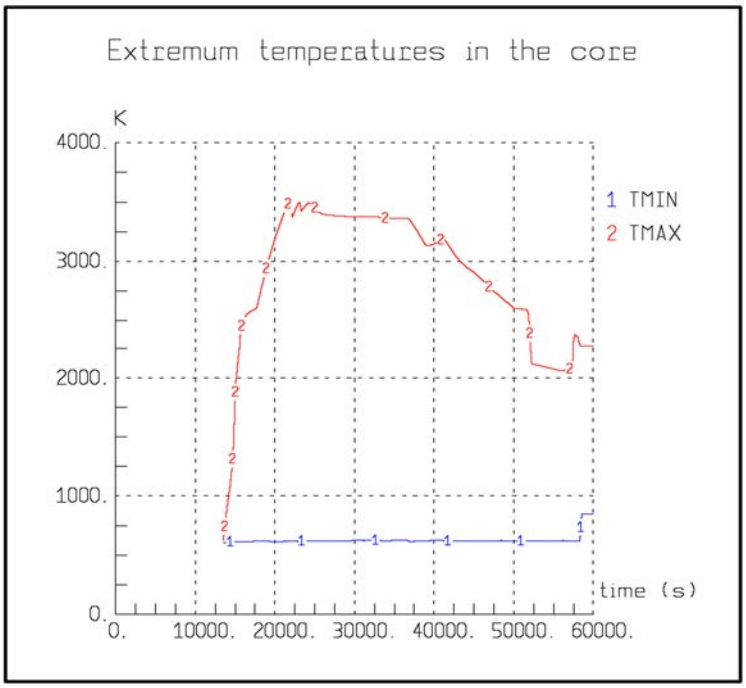

FIG. 13. Core extreme temperature.

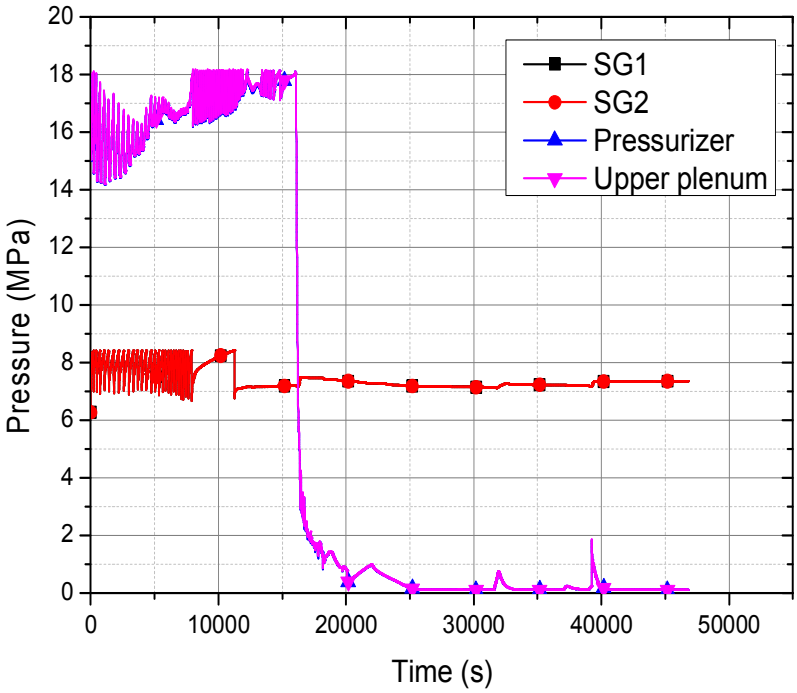

FIG. 14. Primary and secondary pressure.

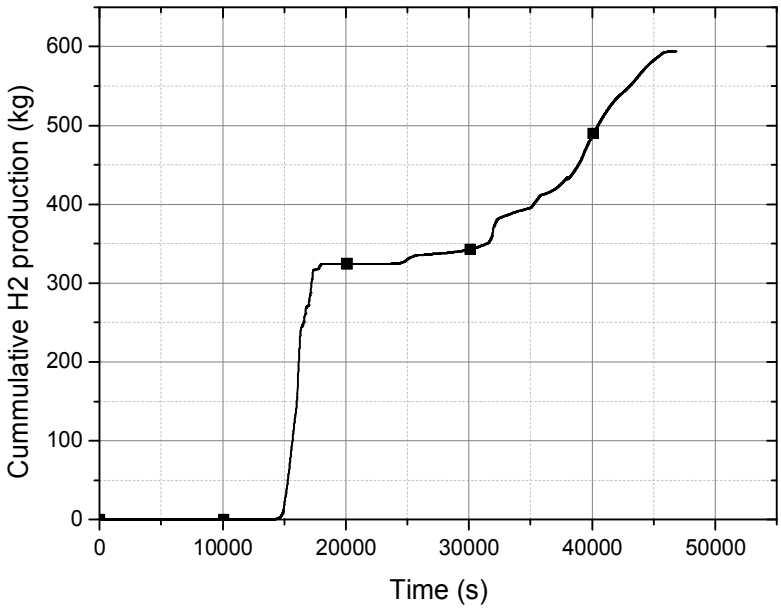

FIG. 15. Cumulative H_2 generation (SBO + PORV).

Molten pool formation is predicted at around 28305 s. Corium that slumped into lower plenum heats the walls of RPV and ultimately leads to lower head vessel failure at 45148 s based on temperature criteria.

Though opening of PORV may avert high pressure melt ejection, it has some other consequences like early vessel failure and higher amount of hydrogen generation compared to when PORV is not opened.

7. CONCLUSIONS

Severe accident analysis was carried out using ASTEC-V2r2 for the following scenarios, which include high & low pressures and slow & fast progressions:

a) Simultaneous rupture of all four steamlines (MSLB ALL).
b) Simultaneous occurrence of LOCA and SBO.
c) Station blackout (SBO).

Higher amount of hydrogen generation is predicted in case of slow transients (SBO & MSLB ALL) compared to the fast transients (LOCA + SBO) due to slow core heat-up and steam availability. In case of fast transients, higher amount of molten material slumped to the lower plenum before vessel failure compared to slow transients. PORV opens on core exit temperature reduced the primary pressure and averted the risk of high pressure melt ejection in case of SBO. Sensitivity analysis shows some effect on predictions such as core maximum surface temperature, molten material and hydrogen generation.

REFERENCES

[1] CHATELARD, P. and REINKE, N., Overview of the integral code ASTEC V2.0, Project reference ASTEC-V2/DOC/09-05, June (2009).

EXTENDED STATION BLACKOUT ANALYSIS FOR VVER-1000 MWE REACTOR

A. J. GAIKWAD, R. S. RAO, S.P. LAKSHMANAN, A. GUPTA
Atomic Energy Regulatory Board, Mumbai,
India
Email: avinashg@aerb.gov.in

Abstract

Post Fukushima, the plant behaviour for an extended station black-out (ESBO) scenario with only passive system availability for about 7 days has become imperative. Thermal hydraulic analysis of ESBO with the availability of passive heat removal system (PHRS), passive first stage and second stage hydro accumulators were carried out to demonstrate the design capabilities. Two different cases having primary leak rates of 2.2 tons/hr and 6.6 tons/hr were analyzed to study sustenance of natural circulation. For the study, out of 4 PHRS trains, one PHRS train was assumed to be in failure mode. The objective here is to predict the core cooling capability for a period of 7days under ESBO conditions with the available water inventories from first and second stage hydro-accumulators only. Over simplified energy balance studies cannot ascertain sustenance of natural circulation in the primary system, steam generators (SGs) and PHRS. The analysis was carried out by using system thermal hydraulic safety code RELAP5/SCDAP/MOD 3.4. It is inferred that the inventory in the first stage accumulators and second stage accumulators compensate the leak and decay heat is removed effectively with the help of passive heat removal systems. It is also observed that even after 7 days of ESBO a large inventory is still available in the second stage accumulators and the primary system remains subcooled.

1. INTRODUCTION

1.1. VVER System Description

The basic design comprises a pressurized water reactor of 3000 MW thermal power with four primary loops; four secondary loops with one turbo-generator producing 1000 MW of electric power. The primary system consists of a reactor pressure vessel, four primary reactor coolant pumps and one pressurizer. The reactor pressure vessel has four inlet nozzles of 850 mm ID and four outlet nozzles of 850 mm ID to connect to the four primary loops. There are also four inlets of 280 mm ID for safety injection of boron solution to the upper and lower plenums in case of loss of coolant from the primary circuit. Reactor core is divided into five radial regions by grouping similarly powered fuel assemblies together. The bottom of the pressurizer is connected to the hot leg of third loop. At the top, the pressurizer spray system is connected with the cold leg of the fourth loop. The secondary system consists of main feed water system, auxiliary feed water system, horizontal U-tube steam generators (SG), steam pipe lines, main steam isolation valves (MSIV), SG-PSDs (steam generator pulse safety devices), atmospheric steam discharge valves (BRU-A), condenser steam discharge valves (BRU-K), main steam line header, governor valve, turbine stop valve, and condenser.

1.1.1 Passive Heat Removal System

Passive Heat Removal System (PHRS) is designed for prolonged residual heat removal from the reactor core during BDBA with loss of all alternate current power supply sources (including failure of diesel generators) both in condition of intact primary circuit, and in cases of leaks in primary and secondary circuits. In case of loss of coolant accident (LOCA), PHRS operates together with stage II ECCS Hydro-Accumulators. It consists of four independent natural recirculation circuits/channels i.e. one for each SG (Figure 1). Each circuit/channel consists of three heat exchanger modules, steam condensate path pipe lines with valves, supply and discharge air ducts and dampers. The elevation of the PHRS loop is about 20 m to assist the natural circulation flow. Heat removal capacity of PHRS has 33 % redundancy, i.e. three channels are enough for removing 2 % of nominal reactor heat capacity i.e. 60 MWt.

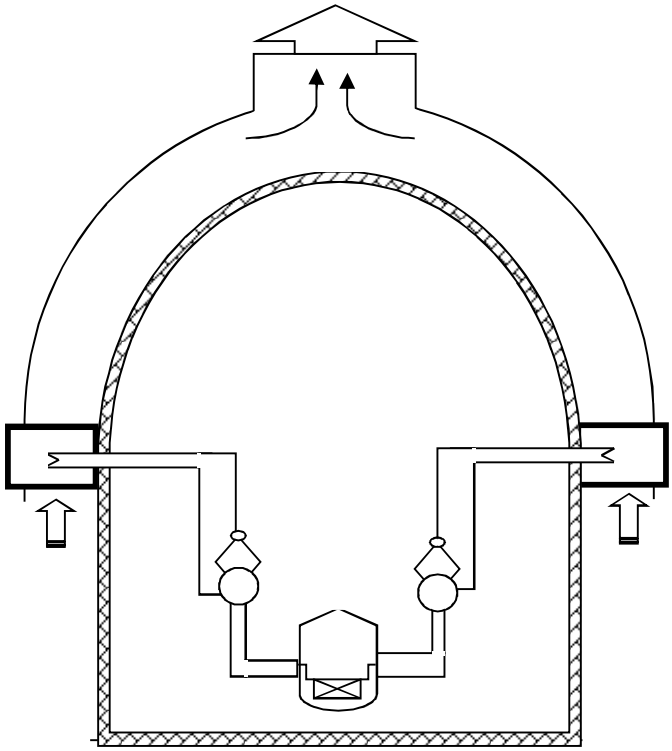

FIG. 1. VVER – PHRS schematic.

2. NUMERICAL MODEL

The computer code RELAP5/SCDAP/MOD3.4 is an integrated code which handles the overall reactor coolant system thermal hydraulic response, core damage progression and fission product releases and transport in primary circuit during transients, design basis accident conditions and in severe accidents. RELAP5/MOD3.4 calculates the overall PHT thermal hydraulics, reactor kinetics while SCDAP code models the core behaviour. In the current study, an input deck was developed that included the modelling of all major components of the PHT, SG, PHRS and emergency core cooling systems. The nodalization for the various components was done using RELAP5 components like pipe, valves, junctions and heat structures for modelling the hydro dynamics and heat transfer [1-3]. The pressure and temperature boundary conditions were modelled using time dependent volumes. The nodalization schemes for reactor vessel, primary loop and PHRS systems are shown in Figures 2, 3 & 4 respectively.

3. RESULT AND DISCUSSION

The initiating event, SBO, leads to tripping of RCP pumps, make-up pumps and main feed water pumps and BRU-K. The shut-off valves of the turbine are closed. Trip of RCPs generates reactor trip signal. Reactor trip occurs at 1.9 seconds of the accident progression. Stoppage of RCP pumps leads to increase in primary coolant heat-up and rise in primary pressure. After RCP pumps trip, flow through the core is established by flow coast-down until 104 seconds, followed by natural circulation. On station black out, closure of the turbo-generator stop valve leads to secondary pressure build-up. Secondary pressure reaches the set point of BRU-A opening (7.2 MPa) in about 1 s. BRU-As operated for about 100 s (opening and closing depending on their set-points) and closed finally when secondary pressure reduced to 6.3 MPa. PHRS started at 30 seconds into the transient on failure of DGs to start on demand and reached nominal power in 90 seconds. PHRS is not simulated for first 90 s of the transient.

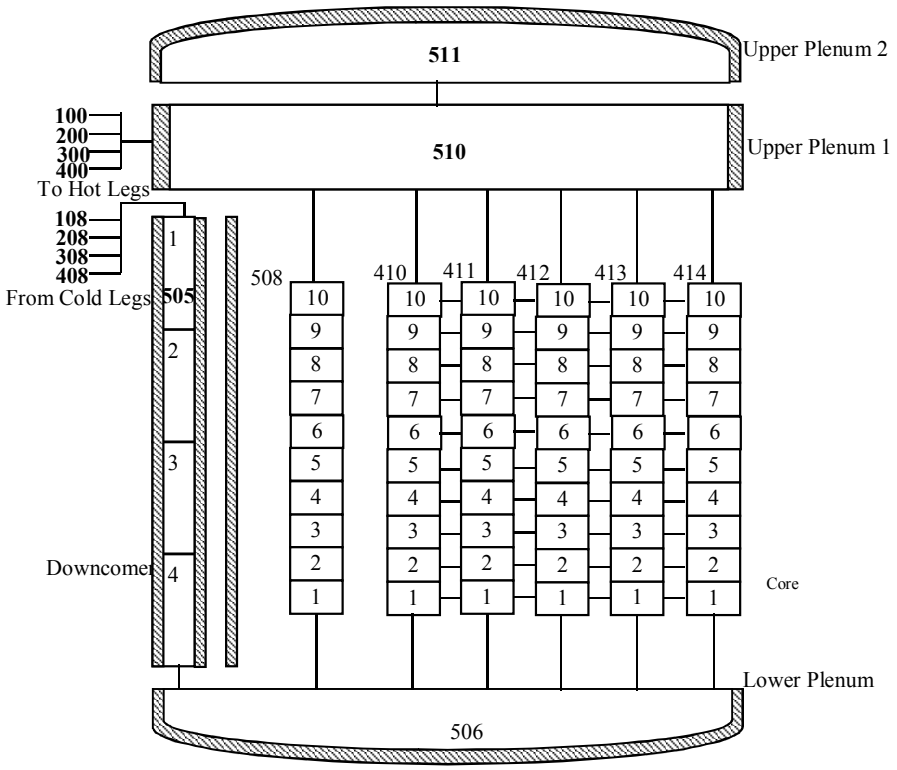

FIG. 2. Nodalisation of Reactor Vessel.

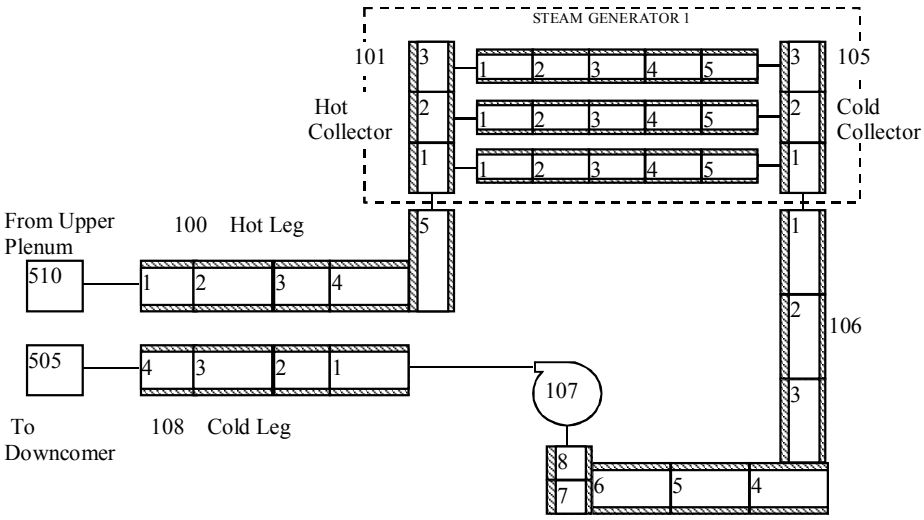

FIG. 3. Nodalisation of Primary loop-1.

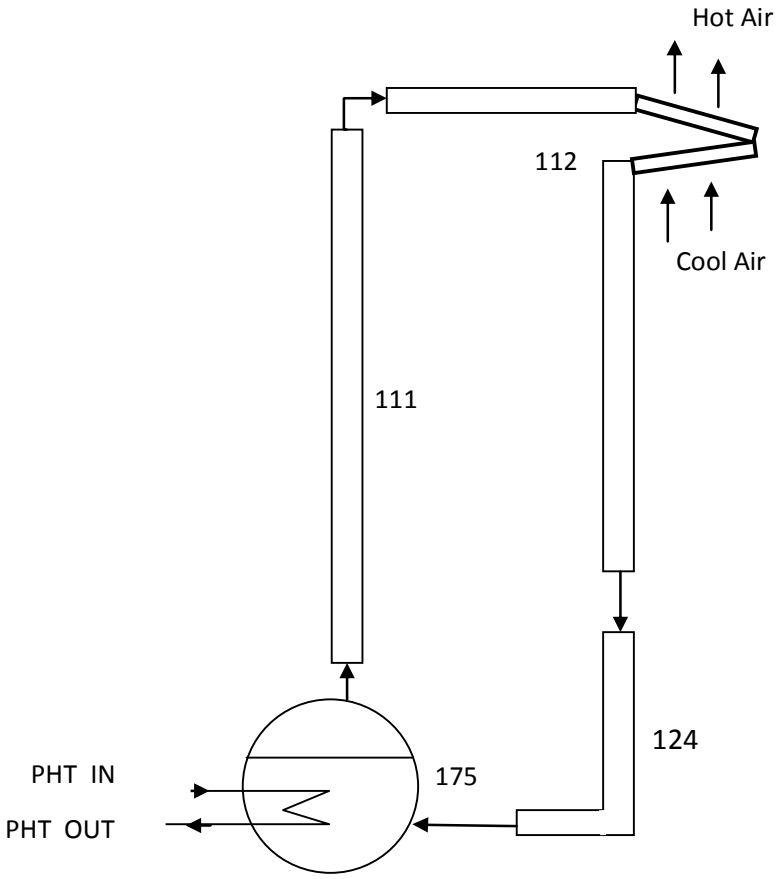

FIG. 4. Nodalisation of PHRS loop.

Two cases with different primary leak rates were analyzed. For case-1, a leak rate of 2.2 tons/hr was considered, and a leak rate of 6.6 tons/hr was considered for Case-2. For both cases only 3 PHRS trains are credited for the analysis, assuming one PHRS train to be in failure mode. All active systems are assumed to be unavailable due SBO event and the analysis take credit of only passive systems like PHRS, first and second stage accumulators. The chronological sequence of the events during ESBO is shown in Table 1.

Figure 5 shows the primary pressure variation during the SBO scenario. The pressure initially increases due to loss of heat removal. Subsequently, pressure decreases because of increase in heat removal through BRU-A opening and actuation of PHRS. 1st stage hydro-accumulators (HA1) actuates when primary pressure reduces to 58.9 MPa. HA1 actuates at about 12 hrs in case of 2.2 t/hr (Case-1) and at 5.52 hrs in case of 6.6 t/hr leak (Case-2). The 2nd stage hydro-accumulators (HA2) actuates when primary pressure reduces to 1.5 MPa in about 89.44 hrs and 30.6 hrs for Case-1 and Case-2, respectively. HA1 isolates on accumulator level less than 1.2 m at 68.9 and 91.3 hrs for Case-2 and Case-1, respectively. The primary system depressurizes faster due to higher leak rate in Case-2 (around 15 hrs). However, the rate of depressurization in both cases is similar in the later period.

Figures 6 and 7 show the secondary pressure variation for cases 1 and 2, respectively. Failure of the PHRS train in the 4th loop is assumed. The primary pressure increases initially due to sudden closure of turbine stop valves. Subsequently pressure reduces due to opening of BRU-As (7.25 MPa) and operation of PHRS. MSIVs are closed on its set-point. However, pressure in the fourth loop remains at a higher level for some period as the respective PHRS train is assumed to be in failure mode. Pressure in the fourth loop starts reducing when HA2 actuates.

TABLE 1. CHRONOLOGICAL SEQUENCES OF EVENTS

Time (s/hr/days) Case-1	Time (s/hr/days) Case-2	Event	Set point of Event
0.0	0.0	Total Loss of power including loss of diesel-generator i.e. Station Black-out	Initiating event (IE)
0.0	0.0	Trip of all RCP sets Auxiliary feed water supply disconnection Switch-off Make-up and blow-down system BRU-K trip Switch-off Pressurizer TEH and spray system Turbo-generator stop valves closing Turbine driven MFPs trip Generation of signal for starting diesel-generator Scram signal generation	Consequences of IE
1 s	1 s	BRU-A open	Main steam header pressure > 7.2 MPa
1.9 s	1.9 s	Reactor trips	Due to three out of four RCPs switched-off
101 s	101 s	BRU-A Close	Main steam header pressure < 6.3 MPa
120.0 s	120.0 s	Beginning of PHRS operation in SG-1, SG-2, SG-3 loop and SG-4 (120 s - full power) as applicable.	On failure of diesel generators to start (30 s delay + 90s for fully effective)
6742.360 s 6742.660 s 6734.850 s 6705.880 s	6872.13 s 6872.17 s 6869.17 s 6835.90 s	MSIV-1 closure MSIV-2 closure MSIV-3 closure MSIV-4 closure	Coincidence of signal: SG pressure below 4.9 MPa and Difference in Tsat. of the primary and secondary > 75^0C
44513.72 s (12.36 hrs)	19876.1 s (5.52hrs)	1st stage accumulators actuation	Primary pressure < 5.89 MPa
321984 s (89.44 hrs)	110000.0 s (30.6 hrs)	2nd stage accumulators actuation	Primary Pressure < 1.5 MPa
91.3 hrs	68.9 hrs	1st stage accumulators isolation	Level of HA1< 1.2 m
8 days	7 days	End time	
4.0 bar	6.03 bar	Primary pressure	End State
130 ^{o}C	131 ^{o}C	Clad surface temperature	
907 m^3	699 m^3	Total HA2 volume available	

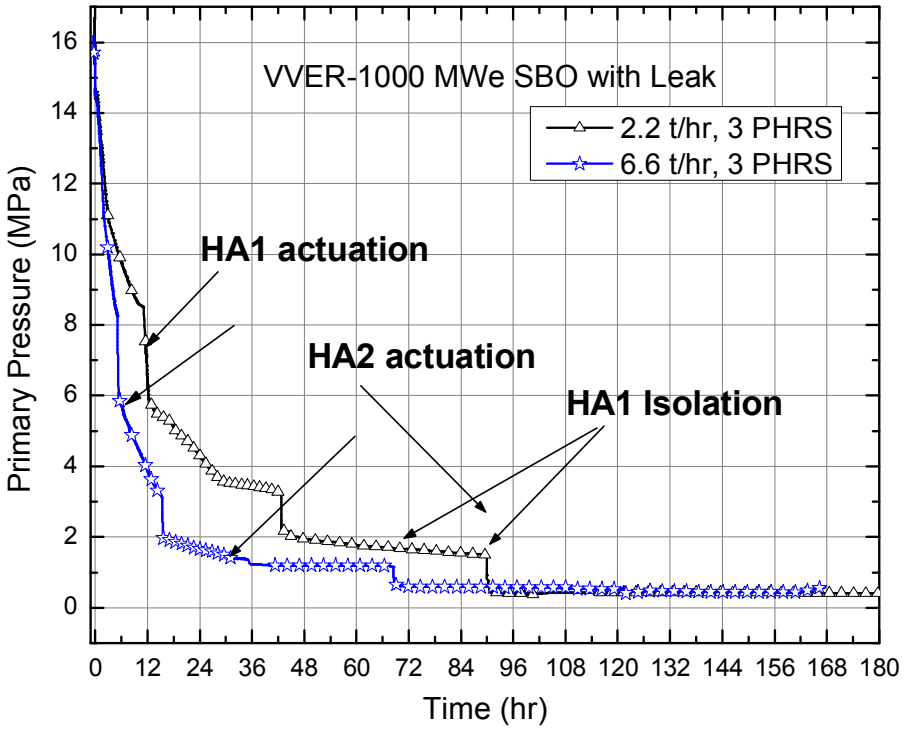

FIG 5.Primary Pressure.

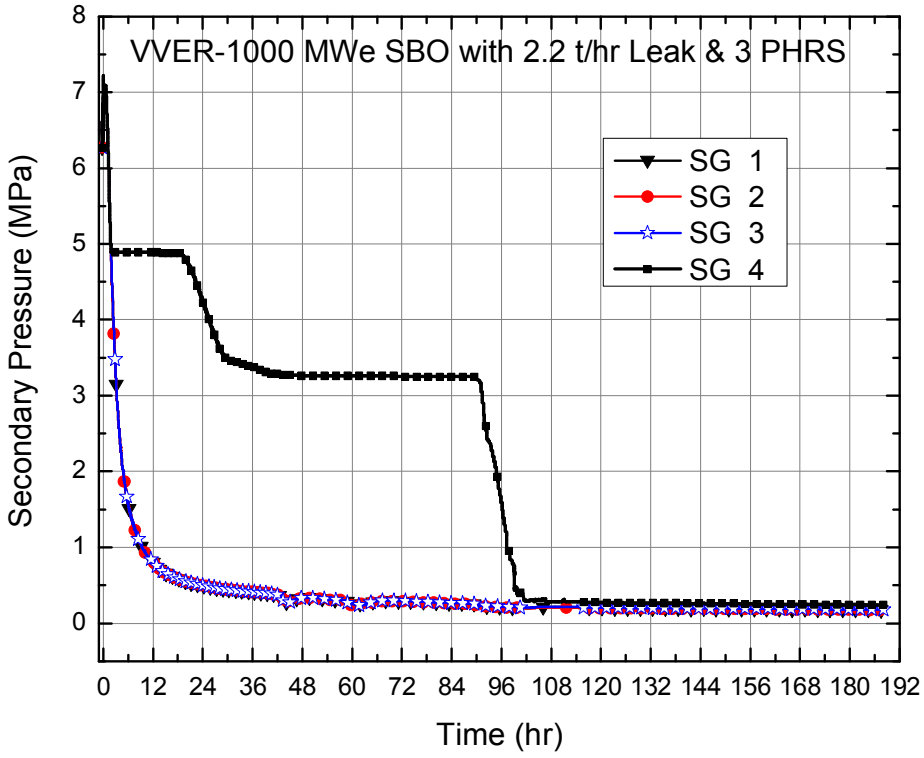

FIG 6. Secondary Pressure (Case-1).

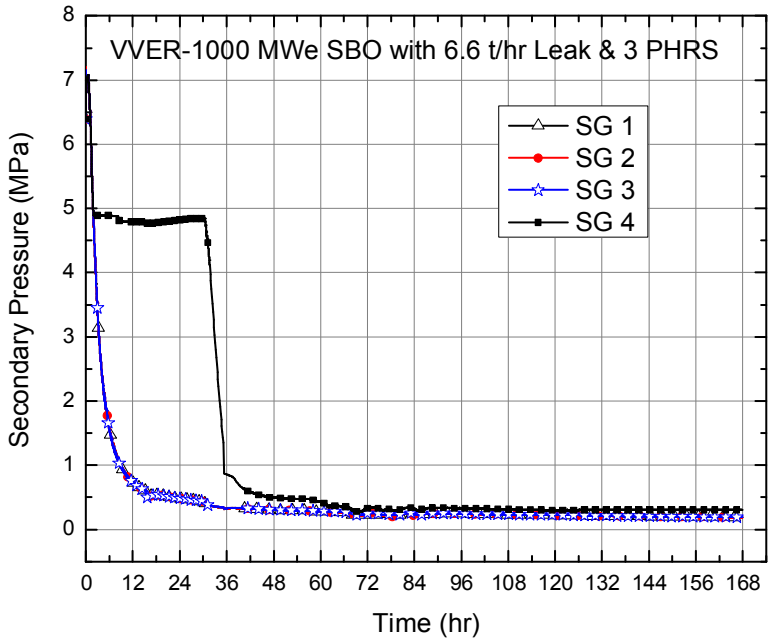

FIG 7. Secondary Pressure (Case-2).

The flow rate in all four primary loops for cases 1 and 2 are shown in Figures 8 and 9, respectively. Flow reduces significantly from the steady state value due to pumps trip (SBO) and coast down. Subsequently, natural circulation flow is established in the primary circuit because of heat removal by PHRS. Flow rate in loops 1, 2 and 3 is similar; however, in loop 4 where the PHRS is not functional, the flow ceases to exist. A significant increase in flow is observed when HA2 actuates and found to be oscillatory due to natural circulation instabilities. Figure 10 shows the leak rate from the primary system for both cases. The leak rate decreases with the pressure. The sudden drop in leak rates is due to sudden decrease in pressure which in turn depends on the small increase in flow due to unstable natural circulation in the primary loops.

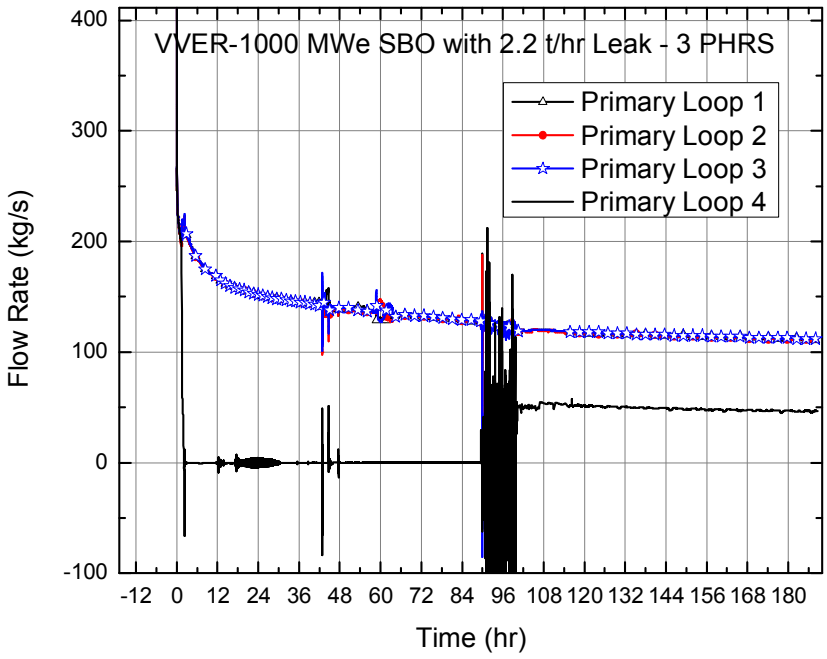

FIG 8. Primary flow rate (Case-1).

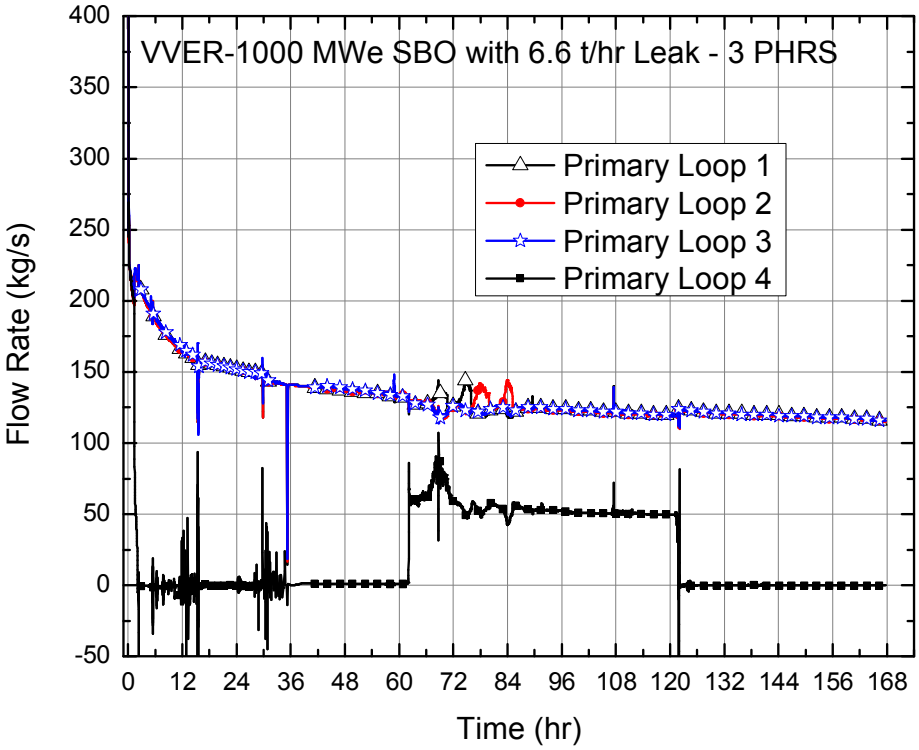

FIG 9. Primary flow rate (Case-2).

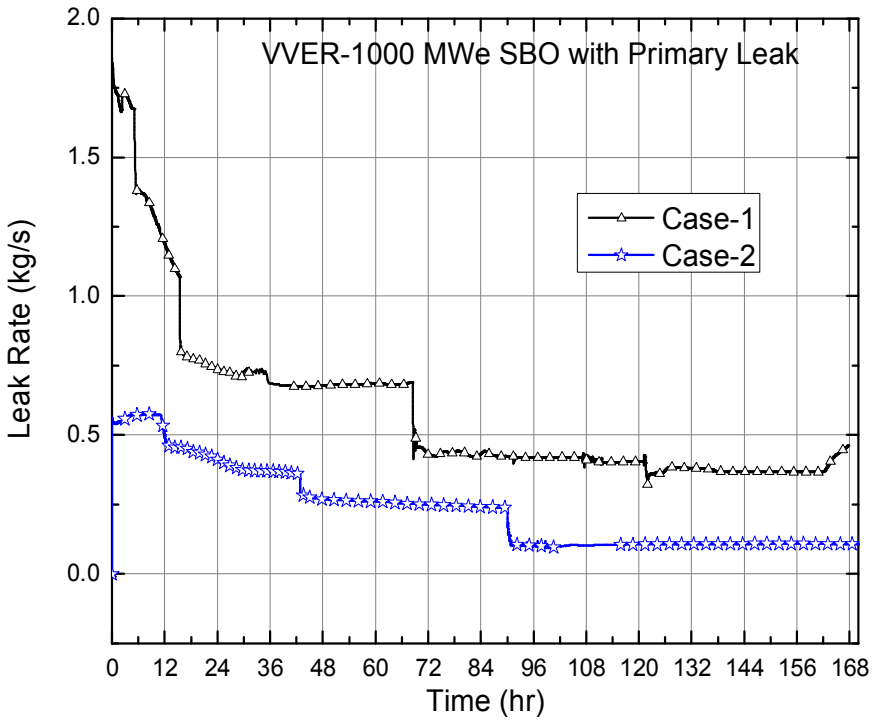

FIG 10. Primary leak rate.

Second stage hydro accumulator actuates when primary pressure reduces to 1.5 MPa. This system actuates early for the cases with 6.6 t/hr leak (case-2). Although it got actuated on low primary pressure, the first stage hydro accumulators are still not isolated and both the first and second stage accumulators are overlapping. As shown in Figures 11 and 12, the inventory level of the HA2 connected to the 4th loop starts reducing as there is no heat removal through the PHRS system. Total inventory injected from the HA2 into the primary is about 50 m^3 and 261 m^3 for cases 1 and 2, respectively. The maximum clad surface temperatures are shown in Figure 13. It was predicted that the fluid and clad temperature behave similarly and decrease at a faster rate in the early stages of the event. Maximum clad surface temperature predicted for both cases is well within the acceptable limits.

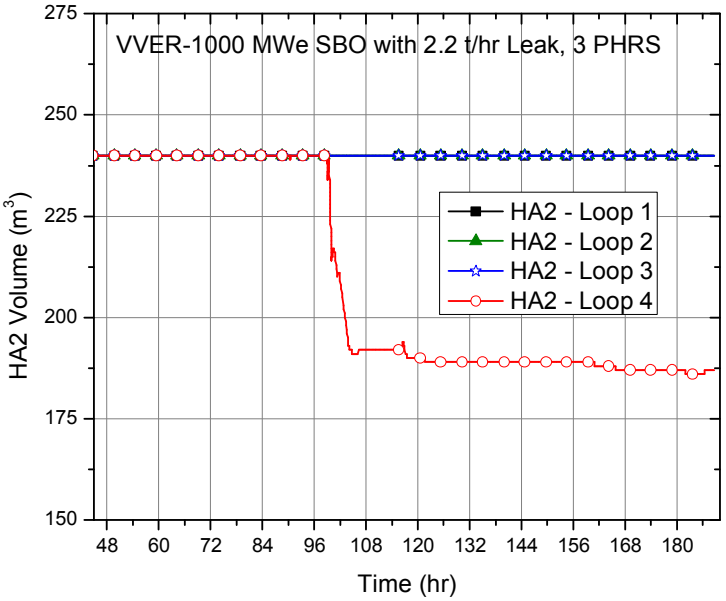

FIG 11. Second stage hydro-accumulator volume (Case-1).

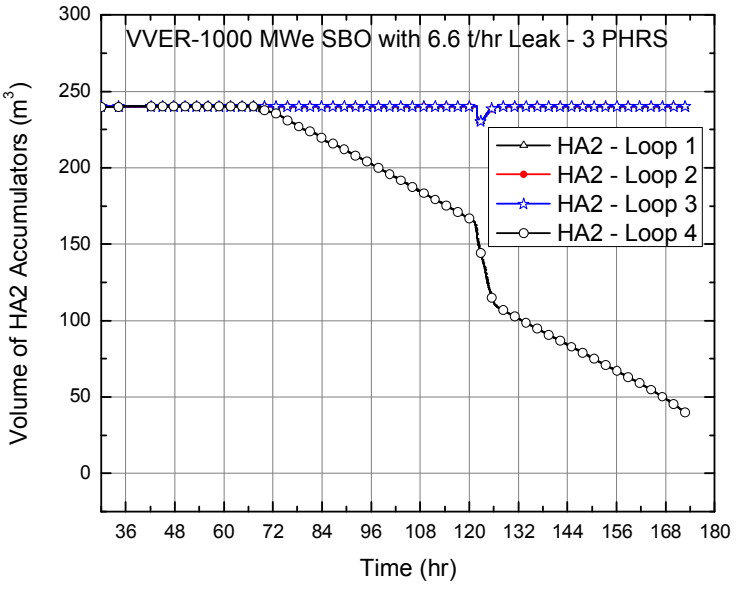

FIG 12. Second stage hydro-accumulator volume (Case-2).

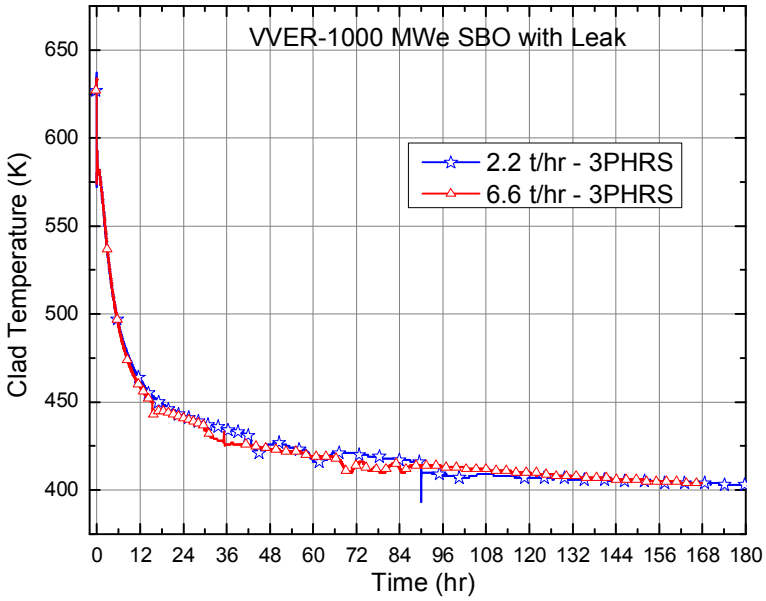

FIG 13.Clad temperature.

4. CONCLUSIONS

Extended station blackout (SBO) for KK VVER 1000 MWe was analysed using SCDAP/RELAP5/MOD3.4. Two cases were analysed viz. Case-1 with leak rate of 2.2 t/hr and with the availability of three PHRS trains, and Case-2 with leak rate of 6.6 t/hr and with the availability of three PHRS trains. All active systems are assumed to be unavailable due to the event SBO. Passive systems such as 1st stage hydro-accumulators, 2nd stage hydro-accumulators, and passive heat removal system were credited in the analysis. The analysis was carried out for about 7 days for both cases.

- The inventory in the first stage accumulators and second stage accumulators compensate the leak and decay heat is removed effectively with the help of passive heat removal systems. Also the primary system coolant remains subcooled at the end of 7 days.
- Natural circulation in the primary was established and sustained for more than 7 days with thermal hydraulic parameters (clad temperature) within the acceptable limits.
- It was predicted that the thermal-hydraulic parameters for both cases, such as pressure, temperature etc. are following similar trends except for the initial period in the cases with higher leak rates.
- It was also inferred that a large inventory of around 900 m^3 (2.2 t/hr, 3 PHRS) and 699 m^3 (6.6 t/hr, 3 PHRS) was still available in the second stage accumulators. It is the specific design feature of connecting HA2 at the top and bottom of accumulator that helps in removal of any uncertainty in injection with prompt and sustained injection flow. This design almost ensures that the whole inventory of HA2 participates in the cooling of the primary system by mixing.

REFERENCE

[1] RELAP5/SCDAP Development Team, SCDAP/RELAP5/MOD3.2 Code Manual Volume I: SCDAP/RELAP5 interface theory, NUREG/CR-6150-Rev 1 (1997).

[2] GAIKWAD, A.J., et al., Effect of Coolant Inventories and Parallel Loop Interconnections on the Natural Circulation in Various Heat Transport Systems of a Nuclear Power Plant during

Station Blackout", Science and Technology of Nuclear Installations Volume 2008, Article ID 458316 (2008).

[3] PRASAD, M.H., GAIKWAD, A.J., SRIVIDYA, A., VERMA, A.K., Failure Probability Evaluation of Passive System Using Fuzzy Monte Carlo Simulation, Nuclear Engineering and Design (2011).

EMERGENCY PREPAREDNESS AND RESPONSE AT NUCLEAR POWER PLANTS IN PAKISTAN

L.A. KHAN, M.A. QAMAR, M.R. LIAQUAT
Pakistan Atomic Energy Commission,
Islamabad, Pakistan
Email: samasl@yahoo.com

Abstract

Emergency preparedness and response arrangements at Nuclear Power Plants (NPPs) in Pakistan have been re-evaluated in the light of Fukushima Daiichi accident. Appropriate measures have been taken to strengthen and effectively implement the on-site and off-site emergency plans. Verification of these plans is conducted through regulatory review and by witnessing periodic emergency drills and exercises conducted by the NPPs in the fulfilment of the regulatory requirements. Emergency Planning Zones (EPZs) have been revised at NPPs. A multi discipline reserve force has been formed for assistance during severe accidents. Nuclear Emergency Management System (NEMS) has been established at the national level in order to make necessary arrangements for responding to nuclear and radiological emergencies. Training programs for first responders and medical professionals have been launched. Emergencies coordination centres have been established at national and corporate levels. Public awareness program has been initiated to ensure that the surrounding population is provided with appropriate information on emergency planning and response. To share national and international operational experience, Pakistan has arranged various workshops and developed a strong link with International Atomic Energy Agency (IAEA).

1. INTRODUCTION

Emergency preparedness and response arrangements at nuclear installations play a significant role in the safety of the facility, workers, environment and public at large. Emergency preparedness and response is assessed through the implementation of comprehensive on-site and off-site emergency plans. The concept of defence in depth, which concerns the protection of both the public and workers, is fundamental to the safety of nuclear installations [1]. A basic safety principles for nuclear power plants states, "All safety activities, whether organizational, behavioural, equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large". The continuous growth in knowledge, the development of safety concepts, the increasing expertise, and experience gained from operating nuclear power plants under normal and abnormal conditions and from accidents have led to more comprehensive and systematic approaches to safety [2].

1.1. Lessons learned from major nuclear accidents

The accident at Three Mile Island, USA, in 1979 emphasized the importance of human factors, the man-machine interfaces and long term effective containment. In addition, investigation of the progression of severe accidents has indicated that, in most cases, there is a substantial period of time from the initiating event of an accident up to the point where core damage can no longer be prevented. It was appreciated that this time span can be used for taking on-site measures for accident management before core degradation occurs [3].

The Chernobyl accident in the Ukrainian Republic of the USSR in 1986 demonstrated the possible consequences of inadequate defence in depth and the importance of organizational issues such as the need for an effective regulatory regime and for a safety culture. It also focused attention on medium and long term contamination due to radioactive releases and the role of off-site emergency planning.

The accident at Fukushima Daiichi in Japan in 2011 highlighted the importance of emergency response capabilities as an ultimate action for protection of public, workers and the environment. As per independent investigation commission on Fukushima it was revealed that the main causes of the Fukushima accident were: the structure of the Fukushima plant

was not capable of withstanding the effects of the earthquake and the tsunami; Tokyo Electric Power Company (TEPCO) and the regulator were aware of the risks from such natural disasters but no steps were taken to put preventive measures in place; and the plant was not prepared to respond to a severe accident. The situation continued to deteriorate because the crises management system, the regulators and other responsible agencies did not function properly [4]. Based on this experience, the IAEA recommended to its member states to evaluate the designs of their reactors in the context of "specific extreme natural hazards" [3].To better prepare for future accidents, the formation of national rapid response teams that could be made available internationally was also recommended. The most significant of the recommendations included strengthened international oversight of NPPs. It was also suggested to enhance reviews of member states regulations against IAEA standards. Every member state with nuclear power plants was recommended to voluntarily host at least one IAEA Operational Safety Review Team (OSART) mission, with the main focus on older nuclear power plants. It is also learned from the Fukushima events that efficient and effective communication is necessary among all responsible organizations to manage during the emergency situations [5].

After the Fukushima Daiichi accident, Pakistan Atomic Energy Commission (PAEC) corporate management formed a task force for re-assessment of plant safety in the light of lessons learnt from the Fukushima Daiichi accident and the IAEA Nuclear Safety Action Plan. Areas were identified for improvement in terms of availability of safety functions in case of severe accidents and extreme natural hazards such as mobile emergency power sources, Hydrogen control & mitigation systems, off-site emergency planning and preparedness, etc. PAEC also provided financial resources for the implementation of the Fukushima Response Action Plan (FRAP) on priority basis.

Pakistan is in the process of enhancing its emergency response capabilities and upgrading its infrastructure to respond to any emergency at nuclear installations in the country. In the light of lessons learned from Fukushima Daiichi accident, steps taken to strengthen the emergency preparedness and response at NPPs in Pakistan are described in the ensuing sections.

2. EMERGENCY PREPAREDNESS AND RESPONSE AT NPPS IN PAKISTAN

Emergency preparedness and response arrangements at NPPs have been re-evaluated and strengthened in the light of the Fukushima Daiichi accident. Pakistan has taken appropriate steps to ensure that there are on-site and off-site emergency plans for NPPs, which are routinely tested and cover the activities to be carried out in the event of an emergency. For new nuclear installations, such plans are prepared and reviewed before the commencement of operation. Emergency preparedness plans have the capability for managing accidents, mitigating their consequences if these do occur, protecting the site personnel, public and the environment. In addition, appropriate steps have been taken to ensure that the surrounding population is provided with necessary information for emergency planning and response.

2.1. Regulatory requirements

Emergency preparedness plans are required to maintain the capability for managing accidents, mitigating their consequences if these do occur, protecting the site personnel, public and the environment. These plans are to be submitted to the Regulatory Body for approval and adhered to in the event of an emergency. In addition, an emergency plan is required to be tested in an exercise before the commencement of operation and at periodic intervals thereafter. Some of these exercises shall be integrated and shall include the

participation of as many as possible of the organizations concerned. The plans shall be subject to review and updating in the light of experience gained from the exercises. The Pakistan Nuclear Regulatory Authority (PNRA) Regulations PAK/909 “Regulations for Licensing of Nuclear Installations in Pakistan (Rev. 1)” [6] set the requirement for preparing an emergency preparedness plan prior to the introduction of nuclear material into the system. PNRA Regulations PAK/913 "Regulations on the Safety of Nuclear Power Plants Operation (Rev. 1)" [7] requires to establish appropriate emergency arrangements from the time that nuclear fuel is brought to the site and to put in place emergency preparedness plans before the commencement of operation. Further, the PNRA Regulations PAK/914 “Regulations on Management of a Nuclear or Radiological Emergency (Rev. 0)” [8] require that licensee shall develop, test, and put in place an infrastructure according to the hazard category as defined in the Regulations. In addition, the licensee shall ensure a timely, managed, controlled, coordinated and effective response at the installation and emergency planning zones anticipated to be affected by the nuclear or radiological emergencies.

2.2. Emergency plans

Pakistan is presently operating three nuclear power plants, C-1 and C-2 at Chashma and K-1 at Karachi. These plants have developed on-site and off-site emergency plans. These emergency plans describe on-site and off-site response organizational setups, classification of emergencies, assessment and declaration of emergencies, emergency facilities, on-site and off-site notification systems, emergency planning zones, intervention and derived intervention levels, environmental dose measurement and assessment facilities, application of protective measures, recovery operations and termination of emergency, public information, records and reports pertaining to exercises and drills, etc. Emergency plans also give brief details of plant systems, demography and regional climatology. The operating organizations, on-site and off-site emergency response organizations are described in the emergency plans covering the role of each responsible person during an emergency situation. Emergency facilities like emergency control centre, auxiliary emergency control centre, communication facilities, radiation monitoring system, post-accident monitoring system, medical facilities, decontamination facilities, etc. are described in the emergency plans.

In order to ensure an appropriate response, emergencies are classified according to the severity of an event or accident. Emergencies have been categorized into four classes in increasing order of severity as standby emergency, plant emergency, site emergency and general emergency. The details of the initiating conditions and actions to be taken during these emergencies are defined in the emergency plans. The initial assessment of the accidents and determination of associated emergency class is specified in relevant plant procedures to be exercised by the on duty Shift Supervisor (SS).

C-1 and C-2 have separate on-site emergency plans and a common off-site emergency plan. Both units have developed a joint procedure for interface during radiological emergency to establish communication link between Emergency Control Centre (ECC) and Main Control Room (MCR) in case of emergency at C-1 and/or C-2. In case of emergency at any one unit, its MCR Shift Supervisor will notify the other unit to declare the same emergency class. Consequently, both units will perform actions in accordance with their respective emergency plans and procedures. After the situation comes under control and the plant is brought to a safer mode, SS terminates the emergency with the authorization of Site Emergency Director (SED). According to C-1 on-site emergency plan, 'CHASNUPP Emergency Response Organization' (CERO) is responsible for initiation and completion of recovery operation and is regarded as recovery organization while the Technical Support Centre (TSC) is meant to

provide technical support to the MCR crew in case of an emergency. Both CERO and TSC are activated by SS in case of emergency.

Both C-1 and C-2 Emergency Plans (on-site and off-site) [9] have been revised in 2011 and 2012 respectively. C-1 and C-2 off-site emergency plan is endorsed both by the district as well as provincial governments.

For K-1 the emergency plans namely KANUPP Off-Site Radiological Emergency Plan (KOFREP) and KANUPP On-Site Radiological Emergency Plan (KONREP) are available for management of off-site and on-site emergencies, respectively [10, 11].

2.3. Verification and improvements of emergency plans

Emergency Plans of the licensee first undergo an internal review to verify that they contain essential elements of emergency preparedness and response in line with the regulatory requirements. Verification of emergency plans is conducted through regulatory review and by witnessing periodic emergency drills and exercises conducted by the licensee in the fulfilment of the regulatory requirements. Prior to the conduct of exercise, the licensee prepares and submits emergency exercise scenario for review and evaluation to the Regulator. PNRA inspectors and PAEC corporate office witness the exercises. On the basis of the results of drills and exercises a report is prepared describing the actions to be taken for improvement of emergency plans and procedures. Later, through periodic inspections by the Regulator, it is verified that the implementing procedures are developed, emergency response organizations are equipped with necessary means, and response personnel have adequate qualifications and training.

2.4. Emergency response organization

The off-site emergency plans of NPPs include role and responsibilities of all the response organizations. District government headquarters are designated as off-site ECC. If the consequences are beyond its control, the off-site ECC may request support of Provincial and Federal Governments. Nuclear Emergency Management System (NEMS) has been established at national level in order to make necessary arrangements for responding to nuclear and radiological emergencies at NPPs in Pakistan. Various response Agencies, Provincial Governments, District Governments, Police, Fire Management Departments, etc. have been assigned responsibilities to combat the nuclear emergencies. Meetings and exercises have been conducted to check the effectiveness of NEMS.

The need for strong institutional and policy arrangements has already been fulfilled by promulgation of the National Disaster Management Ordinance 2007 (NDMO). Under this Ordinance, Government of Pakistan established a National Disaster Management Commission (NDMC) headed by the Prime Minister. It also established a National Disaster Management Authority (NDMA) to serve as the focal point and coordinating body to facilitate implementation of disaster management. All stakeholders including government departments / agencies and armed forces work through and form a part of NDMA in all stages of disaster risk management. At present, Provincial Disaster Management Authority (PDMA) will provide necessary assistance as per emergency plans. Standard Operating Procedures (SOPs) for sheltering, distribution of Potassium Iodide (KI) tablets and evacuation have already been prepared and approved. These arrangements are exercised on regular basis according to the requirements of plans and procedures.

2.5. Revision of emergency planning zones

The EPZs at C-1 and C-2 were revised after the Fukushima Daiichi accident. Impact of simultaneous accidents at both units on EPZ is being assessed. Reassessment of surveillance program for emergency equipment/ supplies expected from other off-site support organizations following extreme external hazards is being taken into consideration. EPZ for K-1 was initially 3 km. After Fukushima Daiichi accident, the EPZ was revisited and set as 5 km where around 3000 people reside. KI tablets have been procured and maintained in sufficient quantity to meet the requirement of the population up to 16 Km around the plants.

2.6. Formation of multi discipline reserve force

At, C-1, C-2 and K-1 a multi discipline (Operation, Maintenance, Health physics etc.) reserve force has been formed for assistance during a severe accident [5]. Necessary competencies and qualifications for such a reserve force team have been identified. It was assessed that plant operations and maintenance staff is enough all the times; however, more radiation protection and environment monitoring staff would be needed for which the efforts are being made. A database for other organizations in the country, which have these capabilities, has been compiled.

2.7. Training program

An inter-departmental training program is underway to supplement the personnel required in case of emergencies, which includes the training of first responder and training of medical professionals.

2.7.1. Training of first responder

In case of an emergency, the rescue person is always one of the first persons reaching at the scene of the accident. The trained rescuers can play an important role to avoid spreading of contamination and overexposure to the personnel. In order to train the first responder, National Regulator has developed liaison with relevant public departments. For the use and awareness of the first responders, pamphlets and booklets have been prepared regarding nuclear and radiation emergencies which may be used in case of a nuclear or radiological emergency.

2.7.2. Training of medical professionals

Overexposure to radiation or radioactive contamination may cause radiation injuries in case of a nuclear or radiological emergency. It is obvious that medical professionals would also be among the first responders in such accidents. Regulatory Body along with PAEC is working towards the development of national capability for the management and treatment of radiation injuries in collaboration with other national organizations and hospitals. The authorities are paying special attention to the training of medical personnel to ensure that adequate level of such capability exists among medical doctors and paramedical staff. In this regard, short courses have been arranged in different hospitals for medical doctors. These courses are based on basic medical techniques for treatment of overexposed and contaminated individuals at the site and in isolated rooms in hospitals in case of a nuclear or radiological emergency.

2.8. Radiation emergency coordination centres

The radiation emergency coordination centres have been established at national and corporate levels. The salient features of these centres are described below.

2.8.1. National Radiation Emergency Coordination Centre (NRECC)

National Radiation Emergency Coordination Centre (NRECC) is established at PNRA Headquarters for coordination of response to nuclear accidents or radiological emergencies and remains functional round the clock. NRECC is the focal point for regulatory response in case of an emergency (abroad or domestic). It is also the National Warning Point (NWP) in Pakistan for the Conventions on "Early Notification of a Nuclear Accident" and "Assistance in the Case of a Nuclear Accident or Radiological Emergency".

NRECC is adequately equipped with communication facilities, radiation detectors, Mobile Radiological Monitoring Laboratory (MRML) vans and Personal Protective Equipment (PPE). Periodic emergency exercises are conducted in order to test the readiness and operation of NRECC and training of response personnel.

An Emergency Preparedness and Review (EPREV) mission was conducted in May 2011 and a team comprised of international experts reviewed the arrangements of NRECC. Most of the Mission recommendations were related to the development of a National Radiation Emergency Plan, which are being addressed in the national Nuclear Emergency Management System.

2.8.2. Emergency Response Coordination Centre (ERCC)

PAEC being the owner of all the NPPs in Pakistan has established a corporate safety office. Under this office an ERCC has been formed. This centre acts as a coordination centre in responding to emergencies at NPPs. This centre maintains various emergency response teams, Mobile Hazard Monitoring Laboratories (MHMLs) and radiation monitoring equipment that will be utilized during emergencies.

2.9. Public awareness program

A two pronged strategy for implementation of public awareness program has been adopted. First, as part of implementation of off-site emergency plan, the NPPs are implementing site specific public awareness programs in areas around nuclear installations. Assistance from other local organizations such as local governments, educational institutions, etc., is sought for providing awareness about emergencies and response of the public. National Regulator is also developing public awareness program at the national level to educate the public through electronic and print media and other communication means. Subject specific written material has been prepared in the form of leaflets, pamphlets and other literature in Urdu, English and local languages for distribution to the public.

2.10. International cooperation

Pakistan is participating in a number of international projects sponsored by the IAEA in the area of emergency planning and preparedness. To share national and international operational experience, Pakistan has arranged various workshops and developed a strong link with the IAEA.

2.10.1. IAEA ConvEx3 exercises

Pakistan participates in IAEA ConvEx3 exercises which are conducted to test the accuracy, availability and accessibility of contact points, adequacy of response time and capability to exchange information through ENAC35 website. These exercises, especially the large scale ones like ConvEx3, helped in testing the planning and preparedness. The evaluations of the exercises at IAEA have shown that in most cases the system worked as planned and intended. Corrective measures were introduced where the response varied from the expected one.

2.10.2. International conventions

As a contracting party to the Convention on Early Notification of a Nuclear Accident, and to the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, Pakistan will exchange information or consider provision of assistance in case of a nuclear accident or radiological emergency in line with the provisions of the Conventions.

2.10.3. Response Assistance Network (RANET) of the IAEA

IAEA Response Assistance Network (RANET) is an integrated system established under the International Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency and is designed to provide international assistance to member states to minimize the radiological consequences of accidents. Being the state party to the Convention, Pakistan has registered National Assistance Capabilities (NAC) in the RANET at the IAEA.

In 2011, the RANET scope and areas of assistance were revised by IAEA. The expertise and resources were re-evaluated at PNRA and PAEC in the light of the revised RANET documents. During the year 2012, National Regulator arranged a national workshop on technical arrangements of activating/deploying national assistance capabilities under RANET. Pakistan has participated in IAEA RANET related workshops/meetings to review the areas of RANET, preparation of RANET documentation and proposals for inclusion of new areas of assistance in RANET pool after the Fukushima Daiichi Accident.

3. CONCLUSIONS

The PAEC in collaboration with PNRA has taken appropriate measures to ensure the effectiveness of on-site and off-site emergency plans for nuclear power plants. These plans are fully implemented and verified to ensure that the implementing procedures are developed, emergency response organizations are equipped with necessary means and response personnel have adequate qualifications and training. Various Areas including emergency planning and preparedness were identified for improvement on the basis of lessons learnt from the Fukushima Daiichi accident and the IAEA Nuclear Safety Action Plan. The work to address these issues is in progress. PAEC has efficient and effective coordination with the National Regulator. An extensive coordination with all concerned governmental bodies, national and international organizations and the public has also been established. This coordination is being strengthened by the process of enhancing its response capabilities and upgrading of the necessary infrastructure to handle nuclear and radiological emergencies at Nuclear Power Plants.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards, Safety Requirements No. GS-R-2, IAEA, Vienna (2002).

[3] AMRICAN NUCLEAR SOCIETY, A report by The American Nuclear Society Special Committee on Fukushima, June (2012).

[4] The official report of the Fukushima Nuclear Accident Independent Investigation Commission (2012).

[5] CONVENTION ON NUCLEAR SAFETY, Special report by the Government of Islamic Republic of Pakistan for second extra ordinary meeting (2012).

[6] Regulations for Licensing of Nuclear Installations in Pakistan, PAK/909 (Rev. 1), PNRA Regulation (2012).

[7] Regulations on the Safety of Nuclear Power Plants Operation, PAK/913 (Rev.1), PNRA Regulations (2008).

[8] Regulations on Management of a Nuclear or Radiological Emergency, PAK/914 (Rev. 0), PNRA Regulations (2008).

[9] CHASNUPP On-Site Emergency Plan and CHASHNUPP Off-Site Emergency Plan (2012).

[10] KANUPP Off-Site Radiological Emergency Plan (KOFREP), (2012).

[11] KANUPP On-Site Radiological Emergency Plan (KONREP), (2012).

ROLE OF THE REGULATORY BODY IN IMPLEMENTING DEFENCE IN DEPTH IN NUCLEAR INSTALLATIONS - REGULATORY OVERSIGHT IN EGYPT

B. M. EL-SHEIKH
Egyptian Nuclear and Radiological Regulatory Authority
Cairo, Egypt
Email: badawymel@yahoo.com

Abstract

The fundamental objective of all nuclear safety regulatory bodies is to ensure that nuclear facilities are operated at all times in an acceptably safe manner including the safe conduct of decommissioning activities. Defence in depth is recognized as one of the fundamental safety principles that underlie the safety of nuclear power plants. Defence in depth is implemented to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within nuclear power plants and events initiated outside plants. The Regulator Body plays an important role in implementing defence in depth in nuclear installations in the context of a clear allocation of responsibilities with an operating organization. This role starting with setting safety objectives and by its own independent review and technical assessment of the safety justifications provided by the operating organization in addition to safety culture investigating within relevant organizations. This paper briefly reviews this role in normal operation and post accidents, and its effects on overall nuclear safety in nuclear installations with reference to Egyptian regulatory oversight.

1. INTRODUCTION

According to the IAEA Safety Glossary the following definition of Defence in Depth (DiD) is provided [1]: Defence in depth: a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

Defence in depth is a comprehensive approach to safety that has been developed by nuclear power experts to ensure with high confidence that the public and the environment are protected from any hazards posed by the use of nuclear power for the generation of electricity. Properly applied, defence in depth ensures that no single human error or equipment failure at one level of defence, nor even a combination of failures at more than one level of defence, propagates to jeopardize defence in depth at the subsequent level or leads to harm to the public or the environment [2].

Also, the concept of defence in depth is fundamental to the safety of nuclear installations. Nuclear safety does not rely on one line of defence but is achieved using a range of complementary means. These factors start with the design and building of a nuclear facility which requires choosing a good design and appropriate site, use of high-quality construction materials and testing before operation. They also cover the whole range of organizational and behavioural issues that are critical to operating a nuclear installation. Also, the strategy for defence in depth is, above all, about preventing accidents. However, if prevention fails, the strategy limits an accident's potential consequences as much as possible and prevents any escalation to more serious conditions.

This concept has a historical development according to IAEA Documents [3]; in 1988– INSAG-3, the concept of DiD was outlined and emphasized by the International Nuclear Safety Advisory Group (INSAG) in its report produced two years after the Chernobyl accident in 1988 entitled 'Basic Safety Principles for Nuclear Power Plants': "All safety activities, whether organizational, behavioural or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defence in depth...".

In 1996, INSAG produced a report fully devoted to the consideration of the DiD concept [INSAG-10]. The report provided a detailed discussion on the concept of DiD in nuclear and

radiation safety including objectives, strategy, and implementation. In 1999, an update of the INSAG-3 report was issued, INSAG-12. The report provided objectives (what is to be achieved) and principles (how to achieve it) in relation to nuclear safety. The central place was given to the DiD concept. In 2005, the IAEA published a report in the Safety Report Series (NO. 46) "Assessment of Defence in Depth for Nuclear Power Plants". This report described a method for assessing the defence in depth capabilities of an existing plant, including both its design features and the operational measures taken to ensure safety. A systematic identification of the required safety provisions for the siting, design, construction and operation of the plant provides the basis for assessing the comprehensiveness and quality of defence in depth at the plant.

The fundamental safety objective is "to protect people and the environment from harmful effects of ionizing radiation". Ten Safety Principles are formulated to provide the basis for nuclear safety considerations. Principle 8 'Prevention of Accidents' states that "all practical efforts must be made to prevent and mitigate nuclear or radiation accidents". DiD is referred to as the primary means of preventing and mitigating the consequences of accidents in nuclear installations.

General Safety Requirements GSR Part 4 was issued that provided requirements that need to be followed to assure that the main principles established in Safety Fundamentals are satisfied. Requirement 13: "Assessment of defence in depth" addresses the importance of observing compliance with DiD. Specific Safety Requirements 2/1, Update of NS-R-1 was issued in 2012, Requirement 7: Application of defence in depth: the design of a nuclear power plant shall incorporate DiD. The levels of DiD shall be independent as far as practicable.

One of the most important organizational and behavioural issues of complementary means that contribute to achieving defence in depth is the regulatory body. Every country operating nuclear facilities has to establish a legal framework for regulating the use of nuclear technology. These laws cover plant and equipment, materials and personnel. There is also a clear assignment of responsibilities for nuclear safety in a wide range of fields such as power generation, medicine and research. The government is responsible for adopting the necessary legislation. Within this legal framework, the operating organization — which might be a power company or research institute — has the prime responsibility for nuclear safety. In addition, legislation establishes a regulatory body, responsible for inspection work and for enforcing the legal requirements established at the national level.

The Convention on Nuclear Safety is commonly recognized as the cornerstone of the international legal framework on nuclear safety and, before the Convention, nuclear safety was considered to be a fully national legal matter. Due to that, the Convention should be the starting point of the international legislation analysis. Article 7 establishes four content requirements for legislative and regulatory frameworks. The frameworks must contain [4]: 1) applicable national safety requirements; 2) a system of licensing; 3) a system of regulatory inspection and assessment; and 4) the enforcement mechanism.

Article 8 of the Convention requires the establishment of independent national regulatory body with adequate resources for implementation of the legislative and regulatory frameworks. Article 14 states that the regulatory authority must review the comprehensive and systematic safety assessments which must be carried out before the construction and commissioning of a nuclear installation and throughout its life.

Article 19 allows the regulator to demand from the operator to report incidents significant to safety in a timely manner. The importance and responsibility of regulatory body regarding the safety of all regional nuclear activities are underlined in IAEA safety standards, in particular: "IAEA Safety Standards for protecting people and the environment, Fundamental Safety Principles, Safety Fundamentals No. SF-1" [5].

This paper briefly reviews this role of regulatory body in implementing defence in depth, and its effects on overall nuclear safety in nuclear installations with reference to Egyptian regulatory oversight.

2. ROLE OF REGULATORY OVERSIGHT IN IMPLEMENTING DEFENCE IN DEPTH IN NUCLEAR INSTALLATIONS

The regulator conducts oversight activities at facilities to gain assurance that activities are being conducted in a safe manner. Because accidents prevention is the strategy for defence in depth, the major lesson from the latest major accidents is the need for the regulator to be sensitive to such early signs of weaknesses and problems and to take pre-emptive actions to require improvements before severe accidents can occur. There are today, many sources of information available to the regulator pertaining to safety at any nuclear facility, such as inspection reports, operating experience reports, research results, periodic safety reviews, probabilistic safety analysis (PSA) results, insights from IAEA reviews and other similar information.

The responsibility of regulatory body in implementing defence in depth in nuclear safety is generally assigned in IAEA a specific report, Defence in Depth in nuclear safety (INSAG-10)[6]: Under section 3.9, para.(102, 103). In the context of a clear allocation of responsibilities between an operating organization and the regulatory body, the latter plays a role in implementing defence in depth by setting safety objectives and by its own independent review and technical assessment of the safety justifications provided by the operating organization. This review is to check the consistency and the completeness of these justifications. Deficiencies in the implementation of defence in depth may also be detected by regulatory inspections; these actions increase general confidence in the safety of plants and may be considered a contribution to defence in depth. The regulatory body, in addition, investigates safety culture within relevant organizations.

More details about the role and responsibilities of regulatory bodies giving in following sections (2.1 – 2.4).

2.1. Role of independent regulatory body in setting safety objectives

As noted before the regulatory body plays a role in implementing defence in depth by setting safety objectives. It is the responsibility of the regulatory body to set safety objectives and standards, and to monitor and enforce them within the established legislative and statutory framework. No other responsibility is to jeopardize or conflict with safety, its primary mission. An important condition for the proper functioning of the regulatory body in discharging its responsibilities is its effective independence from organizations or bodies that promote nuclear activities. This is necessary so that its judgements may be made, and enforcement actions taken, without undue pressure from interests that may compete with safety. The need for this separation of functions has long been acknowledged. Such a separation is included as an obligation for Parties to the Convention on Nuclear Safety [7] and for Parties to the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management [8].

It is recognized that the application of the fundamental principles of nuclear safety and the approach to the regulation of safety within the overall legislative framework may differ from country to country based on their legal systems, cultures, and practices; however, in all cases the regulatory body must have the statutory authority, competence, and resources in order to [9]:

1. Set safety standards.
2. License and inspect installations.
3. Set, monitor and enforce licence conditions.

4. Ensure that corrective actions are taken wherever unsafe or potentially unsafe conditions are detected.

The IAEA has developed a comprehensive array of safety standards in the fields of nuclear energy, radiation protection, radioactive waste management and the transport of radioactive materials. At times, this has been done jointly with other international organizations. The standards are updated from time to time to ensure they can provide guidance on up-to-date methods for achieving a high level of safety.

2.2. Role of regulatory review and safety assessment in verification defence in depth

Regulators carry out a number of safety reviews throughout the life of a facility. Initial safety reviews help to identify the safety significant systems, components and procedures that the regulator will expect to monitor during the commissioning and operation of the facility. During the construction, commissioning and operation of any facility there are usually a considerable number of design changes which the regulator will review to ensure that they do not reduce the overall safety of the facility and that their implementation is properly reflected in operating rules or technical specifications. In addition, most regulators now require periodic safety reviews to give an across the board assessment of the safety of the facility and its components compared to the design basis. Such reviews provide the operator and regulator with detailed information about any ageing degradation of structures and components, and inform decisions about replacing obsolete equipment.

According to the INSAG report "Defence in depth in nuclear safety (INSAG-10)", under section 3.8, para (90-94) [6], safety assessment and verification of defence in depth. Paragraph 90: "the safety assessment for the plant serves:

a) to identify the ways in which normal and potential exposures could be incurred;
b) to assess the quality and extent of the protection and safety provisions; and
c) to determine the expected magnitudes of normal exposures, and to estimate the probabilities and magnitudes of potential exposures."

Paragraph 91 states that "safety assessment focuses on possible challenges to levels of defence. An essential element of such an assessment is a judgement of whether and to what extent the safety functions (controlling the power, cooling the fuel and confining the radioactive material) are ensured by different levels of defence". Paragraph 92 states that "systematic assessment of the implementation of defence in depth is performed throughout the lifetime of the plant, and account is taken of operating experience and significant new safety information from all relevant sources. Such assessments are based on: the definition of the initial safety requirements for the plant; demonstration of compliance with these requirements; insights about deficiencies from incidents or investigations (e.g. from operating experience and the use of probabilistic evaluations); consideration of equipment ageing; and the general extension of knowledge". Paragraph 93 states that "the verification process takes into account data relating to design, manufacture, construction, commissioning, maintenance, tests, in-service inspections, modifications, component failures, component replacements, operator actions, incidents, plant and systems availability, radiation doses and radioactive releases, as appropriate. Trend analysis is a useful tool; the results of trend analyses are reviewed not only to verify that relevant parameters remain as expected but also to demonstrate that they remain within design safety limits and will remain within these limits throughout the planned life of the equipment. Paragraph 94 states that the verification process takes advantage of two complementary methods, the deterministic method and the probabilistic method. These methods each have inherent strengths and weaknesses. The demonstration of an efficient implementation of defence in depth requires their appropriate application, with account taken of their merits and limitations".

2.3. Regulatory independent inspection and enforcement activities

Central to any regulator's attempts to gain assurance that a facility is being operated safely is the need to "go and see". This requires that the regulator must have complete and unfettered access to all nuclear facilities that it regulates. Actual observation of the performance of the facility and the safety attitudes of its staff by trained, critical, professional regulators is vitally important. Inspections are carried out to verify compliance with licence conditions and other regulatory requirements. Deficiencies in the implementation of defence in depth may also be detected by regulatory inspections.

According to Ref. [10] para (2.1-2.5): "regulatory inspection and enforcement activities shall cover all areas of regulatory responsibility. The regulatory body shall conduct inspections to satisfy itself that they operator is in compliance with the conditions set out, for example, in the authorization or regulations. In addition, the regulatory body shall take into account, as necessary, the activities of suppliers of services and products to the operator. Enforcement actions shall be applied as necessary by the regulatory body in the event of deviations from, or non-compliance with, conditions and requirements." The principal objectives of regulatory inspection and enforcement are to provide a high level of assurance that all activities performed by the operator at all stages of the authorization process (see Appendix in Ref. [11]) and all stages during the lifetime of a nuclear facility (siting, design, construction, commissioning, operation and decommissioning or closure) have been executed safely and meet the safety objectives and licence conditions. Regulatory inspection is performed to make an independent check on the operator and the state of the facility, and to provide a high level of confidence that operators are in compliance with the safety objectives prescribed or approved by the regulatory body.

Regulatory inspection should include a range of planned and reactive inspections over the lifetime of a nuclear facility and inspections of other relevant parts of the operator's organization and contractors to ensure compliance with regulatory requirements. The methods of inspection should include examination and evaluation of the facility, procedures, records and documentation, and surveillance and interviewing of personnel, as well as tests and measurements. In addition to the regulatory body's staff, outside consultants may be used for inspection tasks. Regulatory inspections may be carried out by resident or non-resident inspectors, depending on the regulatory regime and the size of the State (Ref. [12], paras 3.20–3.22). The findings of regulatory inspections should be documented in inspection reports drawn up by the regulatory body. The technical bases for these reports — their scope, layout, content, timing and distribution — should be determined by the regulatory body. A program to monitor and follow up inspection findings should also be in place.

Regulatory enforcement actions are actions taken to deal with non-compliance by the operator with specified conditions and requirements. These actions are intended to modify or correct any aspect of an operator's procedures and practices or of a facility's SSCs as necessary to ensure safety. Enforcement actions may also include the imposition or recommendation of civil penalties and other sanctions.

2.4. Regulatory oversight of safety culture

IAEA definition and framework of safety culture is defined as "that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance. This statement was carefully composed to emphasize that Safety Culture is attitudinal as well as structural, relates both to organizations and individuals, and concerns the requirement to match all safety issues with appropriate perceptions and action [13, 14]."

The nature of the relationship between the regulator and the operator can influence the operator's safety culture at a plant either positively or negatively. According to CNRA report 32 [4], the regulatory body has a dual role in the field of safety culture – promoting safety culture through its own example and evaluating the safety culture of licensees through performance or process based inspections and other methods. This means, for example, that the regulatory body [15] should be technically competent, set high safety standards for itself, conduct its dealings with operators in a professional manner and show good judgement in its regulatory decisions. At the same time the regulator ensures that the licensee properly discharges this prime responsibility for safety according to the first fundamental safety principle that states [16]: "The prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks". Therefore, licensees are expected to foster a strong safety culture in their organizations.

Also, with regards to safety culture, the regulatory body should develop general requirements and enforce them in order to ensure the authorized parties have properly considered these requirements. On the other hand, the regulatory body should avoid prescribing detailed level requirements. The regulatory body should not impose detailed requirements, should not regulate safety culture as a whole, but may use the general requirement on management systems to address safety culture expectations.

2.4.1. Pillars of regulatory oversight of safety culture [13]

Regulatory oversight of safety culture is based on three pillars:

(1) Common understanding of safety culture. Its understanding is crucial in achieving a common language and framework that supports both the regulator and the licensee in their communications and promotion of the significance of safety culture in safety performance.
(2) Dialogue: to gain a better understanding of safety culture, dialogue is necessary to share information, ideas and knowledge that is often qualitative. Dialogue enables the licensee and the regulator to have open discussion with respect to each other's roles.
(3) Continuousness: Safety culture improvement needs continuous engagement of the licensee. Regulatory oversight of safety culture therefore ideally relies on a process during which the regulator continuously influences the engagement of the licensee.

2.4.2. The role of the nuclear regulator in evaluating safety culture

It is important that the safety regulator have the capability to inspect and recognize early signs of declining performance. The regulatory evaluation strategy is based on the performance model shown below (Figure 1), where it is assumed that when a weak safety culture exists for a period of time, signs of declining safety performance will appear. If the root causes are not found and corrected, actual safety problems will eventually appear. Therefore, the regulator will have to look for signs of declining performance and subsequently evaluate whether there are signs of a weak safety culture, which may be the root cause of the declining performance [15].

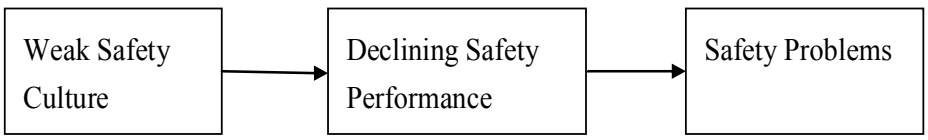

FIG. 1. Safety Culture.

In carrying out this role, the regulator may use new techniques in addition to the traditional regulatory tools and methods developed over the years to evaluate safety performance. Experience in several countries has shown that a good approach is to have senior on-site inspectors who can observe the day-to-day operations of the plant. These observations can be augmented by periodic specialist team inspections that include experienced inspectors who bring a fresh perspective to the site. To facilitate the recognition of declining plant processes and performance, the regulator may perform periodic safety assessments of a facility. This should be a systematic assessment of performance based on co-ordinated discussions and reviews by the regulatory staff (Often it requires an analysis using Probabilistic Safety Assessment (PSA) methodology). The assessment may include the following:

- observations by site inspectors and specialist inspectors;
- reviews by regulatory safety specialists;
- reviews of trends in event reports;
- review of the effectiveness of operator's controls to identify, correct and prevent problems;
- review of work backlog and delays in implementing prescribed actions;
- assessment of day-to-day incidents, which can reveal both organizational weaknesses and inadequate response by individuals; and
- review of operating events to look carefully for safety significant events or conditions that may be precursors to serious accidents.

In recent years [13], an increasing number of regulators have developed an approach to safety culture oversight. These approaches include the following: self-assessment review, independent assessment review, interaction with the licensee at a senior level, focused safety culture on-site review, oversight of management system, and integration into regulatory activities.

A key principle for the regulatory oversight of safety culture is to use multiple data collection methods and data sources, regulatory bodies are encouraged to use not only one approach, but to select a combination of several approaches.

3. EGYPT REGULATORY BODY ENRRA OVERSIGHT

ENRRA is presently the national regulatory authority for the regulation, licensing, inspection and safeguards of all nuclear and radioactive materials and nuclear facilities in Egypt.

3.1. Egypt nuclear regulatory body - a long road towards independence

At the beginning within the Atomic Energy Authority, the establishment of a competent regulatory body in Egypt goes back to 1982. In 1984, based on the EAEA decree No. 9/1984, this committee was changed to be the Nuclear Regulatory and Safety Centre with main responsibility of research on nuclear and radiation safety in addition to making proposals for the legislations, regulations, code of practices, rules related to the nuclear safety and licensing of nuclear installations.

- In 1991 This Centre was transferred to the National Centre for Nuclear Safety and Radiation Control (NCNSRC) by the President Decree No. 47/1991.
- In 1999, based on the EAEA decree No. 622/1999, the regulatory inspection of nuclear facilities inside the AEA became one of the responsibilities of NCNSRC.
- In March 2010 the government of Egypt issued an ordinance creating an independent regulatory body: the Egypt Nuclear and Radiological Regulatory Authority (ENRRA).

According to LAW NO. 7/2010, The main duties of NRRA are:

1. Issuing license, permit authorization or approval for personnel or facilities or procedure, or safety documents.
2. Developing Regulations, Rules and Procedures Related to Nuclear and Radiation Safety Issues.
3. Review and assessment of safety reports of nuclear and radiation facilities.
4. Conducting regulatory inspections of nuclear and radiation activities.
5. Carrying out safeguard inspection for nuclear materials.
6. Control of transportation of radioactive materials on-land or in the Suez Canal.
7. Conducting research in areas relevant to nuclear and radiation safety.

In 2011 (26-Oct.), the code of practice was issued, and in 2012 (5-March), full independence of NRRA was achieved.

According to the law 7/010, the main Characteristics of ENRRA became: independent administrative authority, has powers and necessary resources to fulfil its obligations, and it reports directly to the prime minister. Its functions and responsibilities are developed in: cultural shift (e.g. from research to regulatory oversight), changes of activities from basic research to safety and regulatory research and management of organizational change process should be used to make adjustments.

According to law 7/010, the main functions of regulatory body are: authorization, review and assessment, inspection and enforcement, development of regulations and guides and the complementary functions are: coordinating and monitoring research and development, emergency preparedness, and international co-operation.

Radiation protection in law: according to law 7/010, The Nuclear Law specifies a set of specific regulations, to international standards, required for NPP operation, transport and storage of radioactive materials and storage/disposal of waste. Details for implementation will be prepared by regulatory body after restructuring. In the absence of national regulations, IAEA Safety Standards will be used as a basis for nuclear power regulation.

Regulatory inspection in law: Nuclear Energy Law 7/2010 (art. 53) states that inspection of the nuclear installations and installations that use ionizing radiation shall be performed by the NRRA in order to ensure that the licensing requirements and nuclear safety regulations are complied with. Also, the law gives the right to inspectors to visit the facility /designer during all stages of the authorization process for complementary information, check of the claims made in the documentation, improvement in practical understanding of safety issues, establishment of links with operator's specialists, and checking of the QA system of the operator, manufacturers, and suppliers.

Security and Physical Protection in law: the Nuclear Law ensures that all necessary legal instruments and arrangements would be in place. The development of "Design Basis Threat" (DBT) and "unacceptable consequences" defined at state level have not been established yet. Egypt in cooperation with the IAEA and the consultant will establish a program for selection & qualification of staff.

Radioactive waste in law: the Nuclear Law revised and updated laws and regulations for handling low and medium level waste. A consultant will help in assigning responsibility to follow international developments for high level waste disposal. The Consultant will also help in planning for enhancing waste disposal programs and facilities, and will include waste volume and toxicity minimization provisions, and adequate on-site storage, in bid specification.

3.2. Overview of nuclear safety oversight programs in Egypt

The Egyptian regulatory framework for nuclear safety oversight consists of three key strategic performance areas: nuclear facilities safety, radiological facilities safety, and safeguards, in addition to the nuclear safety institute. According to the regulatory framework the main activities regulated are:

- Nuclear installations safety
  - Planned nuclear power plants
  - Research reactors
    1) ET-RR -The first research reactor,
       - 2 MW tank type, Russian technology.
       - Applied for extended shutdown
    2) ET-RR2 (The second research reactor)
       - 22 MW, Argentina technology.
       - In operation.
       - Undergoing re-commissioning for some systems, due to core modification (MO-99).

    The Licenses issued by NCNSRC:

    - Licensing Requirements of Research Reactors (RRs), 1997.
    - Licensing of Operators of Research Reactors (RRs), 1998.
    - Regulatory inspection program 2004.
    - Inspection Requirements for Nuclear Facilities at EAEA, 2005.
  - Fuel cycle installations
    - Fuel Fabrication Facility (MTR fuel elements).
    - In operation.
- Radiological installations safety
  - Main activities:
    - Medical and industrial installations using radioactive sources.
    - Handling of radioactive materials and radiation sources.
  - Main radiation installations in Egypt
    - Two gamma irradiation units (one under construction).
    - Radioisotope production facility.
    - Low and medium radioactive waste treatment unit.
    - Gamma radiotherapy unit.
    - 6000 open and sealed sources.
  - The licenses issued by NCNSRC
    - Basic regulatory rules for the protection against ionizing radiation, 1998.
    - Safety regulations concerning radio-active waste, 2004.
    - Licensing of charged particles accelerators.
    - Licensing of gamma irradiators, 2006.
    - Relicensing of gamma irradiator, 2012.
- Safeguard and security section.
- Nuclear safety institute.

3.3. Regulatory body challenges

In the light of Fukushima Daiichi accident on March 2011, the philosophy of regulation has been expanded to include the assumption of large scale natural disasters. The ENRRA body should apply what it called an 'exhaustive defence in depth concept' in which multiple safety systems would work independently of each other to avoid accidents.

Further directives on the Regulatory inspection program, procedure, and conduct of inspection should be prepared. Accordingly, this inspection may be conducted periodically or without prior notification.

The need to have full time staff for performing assessments or evaluating the adequacy of the assessments (currently performed for the NRRA by consultants). This manpower requirement and technical competence applies also to regulatory inspections.

The need to have staff composed largely of individuals possessing broad technical expertise for engineering judgment and nuclear health and safety skills, who are capable of assessing on an overall basis the safety of a nuclear power plant.

Details of Emergency Plan arrangements have not been developed. However, part of the Nuclear Law covers those issues. It is expected that the international consultant will help in identifying a detailed approach.

Operating experience must be taken into account for the further enhancement of the safety of nuclear facilities. NRRA has to conduct the operational experience feedback activities by reviewing the event reports submitted by the licensee and the annual summary of operational feedback activities.

4. CONCLUSIONS

Defence in depth is one of the fundamental safety principles that underlie the safety of nuclear power plants. The importance of role and responsibilities of the regulatory bodies in implementing this concept should be emphasized. The regulatory bodies should be sensitive to the early signs of weaknesses and problems and to take pre-emptive actions to require improvements before severe accidents can occur. In Egypt, the regulatory body should be aware to these responsibilities toward defence in depth implementation to be ready to conduct all oversight activities at facilities to gain assurance that activities are being conducted in a safe manner.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Glossary, Terminology Used in Nuclear Safety And Radiation Protection, IAEA, Vienna (2007).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of. Defence in Depth for Nuclear Power Plants, Safety Reports Series No. 46, IAEA, Vienna (2005).

[3] BAJS, T., Concept of Defence-in-Depth (DiD), National Training Course on Safety Review and Assessment (TC PROJECT EGY9/040), Cairo, 17 - 21 June (2012).

[4] PTASEKAITE, R., The Role of the Regulator: Nuclear Safety and Nuclear Safety Culture, Dissertation for the International School of Nuclear Law, Montpellier 2011, Stockholm (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series, Safety Fundamentals No. SF-1, IAEA, Vienna (2006)

[6] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Convention on Nuclear Safety, Legal Series No. 16, IAEA, Vienna (1994).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management, INFCIRC/546, IAEA, Vienna (1997).

[9] ALI, M.F., Nuclear Energy: Safety – Regulatory Control of Nuclear Power Plants: Part 1, Chapter 40, 25 October (2012).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Inspection of Nuclear Facilities and Enforcement by the Regulatory Body, Safety Standards Series No. GS-G-1.3, IAEA, Vienna (2002).
[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Documentation for Use in Regulating Nuclear Facilities, Safety Standards Series No. GS-G-1.4, IAEA, Vienna (2002).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Organization and Staffing of the Regulatory Body for Nuclear Facilities, Safety Standards Series No. GS-G-1.1, IAEA, Vienna (2002).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Oversight of Safety Culture in Nuclear Installations, IAEA-TECDOC-1707, IAEA, Vienna (2013).
[14] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Safety Culture, INSAG Series No. 75-INSAG-4, IAEA, Vienna (1991).
[15] OECD/NEA, The Role of the Nuclear Regulator in Promoting and Evaluating Safety Culture, Paris, June 1999.
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

METHODOLOGY FOR THE ASSESSMENT OF CONFIDENCE IN SAFETY MARGIN FOR SMALL BREAK LOSS OF COOLANT ACCIDENT SEQUENCES

D.B. NAGRALE, M. PRASAD, R.S. RAO, A.J. GAIKWAD
Nuclear Safety Analysis Division,
Atomic Energy Regulatory Board,
Mumbai, India
Email: avinashg@aerb.gov.in

Abstract

Deterministic Safety Analysis and Probabilistic Safety Assessment (PSA) analyses are used concurrently to assess the Nuclear Power Plant (NPP) safety. The conventional deterministic analysis is conservative. The best estimate plus uncertainty analysis is increasingly being used for deterministic calculation in NPPs. The PSA methodology aims to be as realistic as possible while integrating information about accident phenomena, plant design, operating practices, component reliability and human behaviour. The peak clad temperature (PCT) distribution provides an insight into the confidence in safety margin for an initiating event. The paper deals with the concept of calculating the peak clad temperature with 95 percent confidence and 95 percent probability ($PCT_{95/95}$) in small break loss of coolant accident (SBLOCA) and methodologies for assessing safety margin. Five input parameters mainly, nominal power level, decay power, fuel clad gap conductivity, fuel thermal conductivity and discharge coefficient, were selected. A Uniform probability density function was assigned to the uncertain parameters and these uncertainties are propagated using Latin Hypercube Sampling (LHS) technique. The sampled data for 5 parameters were randomly mixed by LHS to obtain 25 input sets. A non-core damage accident sequence was selected from the SBLOCA event tree of a typical VVER study to estimate the PCTs and safety margin**.** A Kolmogorov– Smirnov goodness-of-fit test was carried out for PCTs. The smallest value of safety margin would indicate the robustness of the system with 95% confidence and 95% probability. Regression analysis was also carried out using 1000 sample size for the estimating PCTs. Mean, variance and finally safety margin were analysed.

1. INTRODUCTION

Safety analysis for NPPs requires evaluations with both deterministic and probabilistic assessments as a defence-in-depth principle of safety assessment. The deterministic safety analysis generally follows two methods - conservative and best estimate, depending on analysis objectives and issues involved. For a new NPP, the utility is expected to follow conservative analysis. For reauthorization of an existing NPP, analysis with conservative approach is considered although best estimate approach with uncertainty analysis (i.e. selection of input parameters and their range, sampling technique, modelling etc.) is preferred.

Safety Margin (SM) is the difference between the reference limiting value of any assigned parameter as accepted by the regulatory body and the calculated value via deterministic methods. There are various areas where assessment of SM is carried out for making regulatory decision such as:

a) To demonstrate that adequate margins exist for events such as Anticipated Operational Occurrences (AOOs) and Design Basis Accidents (DBAs) considered in the design.
b) To show that adequate safety margins exists in the proposed modification in the plant structures, systems or components.
c) Re-evaluation/improvement of safety margin by screening out extra conservatism in input parameters, using latest state-of-the-art codes, latest knowledge about a sensitive parameter, etc.

In the conservative analysis there is one value of the safety margin corresponding to the single output of a parameter. However, in the best estimate plus uncertainty analysis (BEPU) there is a range and hence a probability distribution for the safety margin due to multiple output values of a parameter. Fig.1 shows schematically the safety margin for deterministic assessment [1].

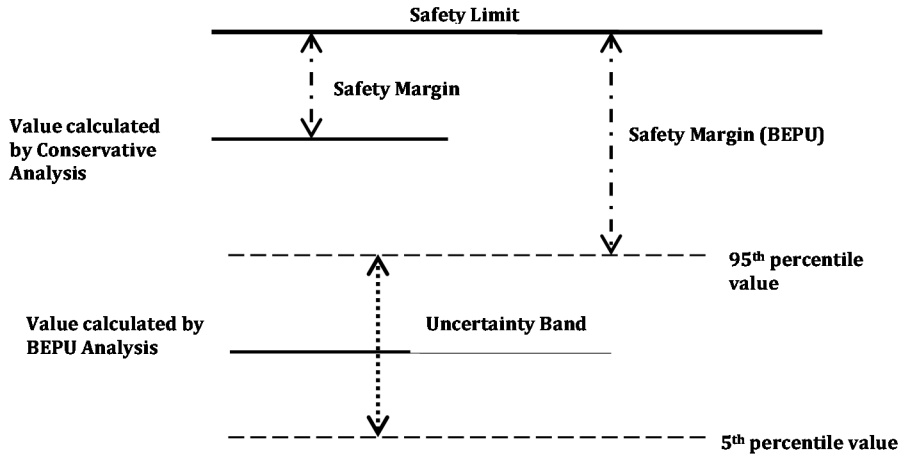

FIG. 1. Safety Margin Illustration.

In the deterministic approach a reduced number of limiting transients are analysed for which conservative rules for system availability and parameter values are often applied. The accident phenomenology and the related timings are estimated as complete as necessary. In the probabilistic approach completeness of the set of different scenarios and best estimate methods is emphasized. The approaches have been developed rather independently from each other. It is imperative that a safety margin be evaluated by BEPU for the possible accident sequences obtained from PSA event tree.

This paper discusses thermal hydraulic analysis for estimation of PCT for the accident sequence of SBLOCA event tree, safety margin uncertainty distribution and linear regression analysis for obtaining more data on safety margin along with overall conclusions.

2. DEFENCE IN DEPTH AND SAFETY MARGIN

The implementation of defence in depth (DID), throughout design and operation, provides a graded protection under various plant states, including those resulting from equipment failures or human actions within the plant, and events that originate outside the plant. The number of physical barriers required is a function of the potential internal and external hazards and the potential consequences of failures. The barriers are in the form of the fuel matrix, the fuel cladding, the reactor coolant system pressure boundary and the containment.

The application of the concept of DID to the design of a plant provides a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.

i. The aim of the first level of defence is to prevent deviation from normal operation, and prevent system failures.
ii. The aim of the second level of defence is to detect and intercept deviations from normal operating conditions in order to prevent anticipated operational occurrences from escalating to accident conditions.
iii. The third level of defence is provided to control the consequences of design basis accidents should they occur. It is assumed that although very unlikely, the escalation of certain anticipated operational occurrences or PIEs may not be arrested by a preceding level and a more serious event may develop.

iv. The aim of the fourth level of defence is to address consequences of severe accidents, should they occur, in which the design basis event may have been exceeded and to ensure that radioactive releases are kept as low as practicable.
v. The fifth level of defence is aimed at mitigation of the radiological consequences of potential releases of radioactive materials to the environment that may result from accident conditions and severe accidents [2].

The acceptance criteria are directly or indirectly related to the barriers. The safety margins are introduced at several stages of the analysis where successive acceptance criteria are defined. The safety margin of each level of DID is very important and safety margin evaluation at each level of DID is necessary.

3. CLASSIFICATION OF UNCERTAINTIES

Uncertainty analysis is an essential part of a complex system. Specifically uncertainty analysis refers to the determination of the uncertainty in analysis. The two fundamental types of uncertainty are “Aleatory” and “Epistemic” uncertainty.

3.1. Aleatory uncertainty

Aleatory uncertainty results from the effect of inherent randomness or stochastic variability. It represents the non-deterministic and unpredictable random nature of the performance of the system and its components. It is quantified by probability i.e., probability of an event is considered as a quantitative measure of the chance of occurrence of that event.

Variables subject to aleatory uncertainty have intrinsic probability distributions, which represent random laws. These distributions are usually derived from statistical data. It can be associated with the question “what can occur and with which probability?”. Aleatory uncertainty as such is the subject of PSA to express probabilistically how safe the system is. In this context aleatory uncertainty is primarily associated with:

- Occurrence of initiating events.
- Initial conditions i.e., the state of the plant at the beginning of an accident.
- Performance of system components and humans during an accident, etc.

3.2. Epistemic uncertainty

Epistemic uncertainty results from the imperfect knowledge regarding values of parameters of the underlying computational model. The parameters as such are deterministic in nature, i.e. they have fixed and invariable values which are not precisely known. It can also be quantified by probability i.e., probability distributions associated with uncertain parameters represent the state of knowledge about the right values of the parameters. Such probability distributions for uncertain parameters are very often derived from expert judgment. Epistemic uncertainty can be reduced, at least in principle, and sometimes even eliminated by improving the state of knowledge, e.g., by doing more investigations, experiments and research. It can be associated with the question “which value is the right one and how well do we know that value?”[3]

4. ESTIMATION OF UNCERTAIN PARAMETERS FOR SBLOCA ACCIDENT SEQUENCE

A number of approaches to uncertainty have been developed, including differential analysis, response surface methodology, Monte Carlo analysis etc. Sampling based approaches to uncertainty

analysis are both effective and widely used. There are a large number of parameters that need to be considered for uncertainty analysis [4]. Some of these are as follows:

i. Reactor operating power level.
ii. Decay heat.
iii. Fuel thermal conductivity.
iv. Fuel clad gap conductivity.
v. Heat transfer coefficient to the coolant.
vi. Two phase frictional pressure drop coefficient.
vii. Discharge coefficient.

However, with limited resources the five parameters selected in this analysis to observe the impact on clad temperature were nominal reactor power, decay power, discharge coefficient, fuel conductivity and fuel clad gap conductivity. The probability distribution for each of the parameters was assumed to be uniform in view of the lack of selected knowledge in the experimental field. The nominal values of the parameters and their ranges were based on available literature and judgment. These parameters are shown in Table 1.

TABLE 1. UNCERTAINTY PARAMETERS VALUES

Sr. No.	Parameter	Probability Distribution	Nominal Value		Normalized Minimum/Maximum Values
1	Nominal Reactor Power (P)	Uniform Distribution	3000 MW_{th}		1.0 – 1.04
2	Decay Power (Pd)	Uniform Distribution	1.0		1.0 – 1.2
3	Discharge Coefficient (Cd)	Uniform Distribution	1.0		1.0 – 1.2
4	Fuel Conductivity (K_f)	Uniform Distribution	T	W/m-K	0.95 – 1.1
			273.0	8.1	
			293.0	8.0	
			1100.0	3.75	
			1700.0	2.50	
			2700.0	2.65	
			3100.0	3.50	
			3330.0	3.50	
5	Fuel Clad Gap Conductivity (K_g)	Uniform Distribution	T	W/m-K	0.95 – 1.05
			273.0	0.141	
			500.0	0.211	
			700.0	0.278	
			900.0	0.335	
			1100.0	0.389	
			2500.0	0.389	

5. DESIGN MATRIX FORMULATION USING LATIN HYPERCUBE SAMPLING

There are several sampling strategies available, including random sampling, importance sampling and Latin Hypercube Sampling (LHS). LHS is very popular for use with computationally demanding models as it allows for the extraction of a large amount of uncertainty and sensitivity information with relatively small sample size.

The LHS method consists of three steps to obtain an 'N' x 'K' design matrix where 'N' is the number of LHS samples (and hence the number of code runs) and 'K' is the number of input variables. The first step is dividing each input variable X_i (i = 1 to K) into N intervals with equal probability of (1/N). The second step is obtaining X_{ij} (j = 1 to N) for each input variable X_i. The third step is random coupling of X_{ji} (j = 1 to N, i = 1 to K). The sample size is greatly reduced if the LHS technique is used to generate the sample. The number of latin hypercube sample, 'N', for 'K' input variables is sufficient if it is (4/3) K. However, if running time of model is not excessive then 'N' can vary from 2K to 5K. In this study the number of input variables is 5, hence a sample size of 25 is considered.

6. SBLOCA ANALYSIS EVENT TREE

The events consisting of SBLOCA inside the containment include the LOCAs which are not compensated by normal make up. Accident sequence is modelled without core damage occurred at the operation of RPS system, the operation of hydro-accumulators, HPECCS and LPECCS which ensures the maintenance of coolant inventory in the core. This further extended to loss of offsite power that leads to loss of heat removal through the turbine condenser. The main assumption considered for the event is RPS action is not required for achievement and maintaining of reactor sub criticality as the reactivity feedbacks are negative.

There are four function events for the event tree, namely power supply system from grid, emergency heat removal system, hydro-accumulators (HA), high pressure emergency core cooling system (HPECCS) and low pressure emergency core cooling system (LPECCS). The HPECCS begins the delivery of water into the primary circuit when the primary pressure is less than 7.89 MPa and LPECCS delivers water into the primary circuit when the primary pressure is less than 2.5 MPa. The safety systems with the success criteria are shown in Table 2.

TABLE 2. SAFETY SYSTEMS FOR LBLOCA EVENT TREE

Sr. No.	System	Safety Function	Success Criteria
1	Power Supply from Grid	Power supply to plant after shutdown	Availability of grid power after unit shutdown
2	Emergency Heat Removal System	Cooling	Operation of EHRS on one of four SGs.
3	1st stage Hydro-accumulators	Maintain coolant inventory	Operation of one of four HA trains
4	High Pressure Emergency Core Cooling System (HPECCS)	Maintain coolant inventory	Boron solution charging into the core by two HPECCS trains when primary pressure is less than 7.9 MPa
5	Low Pressure Emergency Core Cooling System (LPECCS)	Maintain coolant inventory	Operation of one LP ECCS train for coolant injection mode when primary pressure is less than 2.5 MPa

The accident sequence considered for this analysis is representative and does not represent the full event tree as shown in Figure 2 which indicates the initiating event and safety systems as function events and non-core damage states where the clad temperatures are expected to be below 1200^{0} C. The accident sequences are indicated in the figure.

7. SBLOCA ACCIDENT SEQUENCE ANALYSIS

Thermal hydraulics analysis was carried out for 105 mm pipe (SBLOCA) of the cold leg of first loop using a thermal hydraulics code. Nodalisation of the primary circuit involves the reactor, circulation loops and pressurizer. The reactor pressure vessel is simulated by four elements: reactor core, downcomer, lower plenum and upper plenum. The reactor core is simulated by maximum power channel, average power channel and bypass channel. Each channel is divided into 10 volumes. The downcomer is divided into four volumes. The lower plenum is simulated by single volume and two volumes simulate the upper plenum. The primary coolant system is represented by four circulation loops. Each loop is divided into hot leg (five volumes), SG hot collector (Three volumes), SG tubing (fifteen volumes), SG cold collector (three volumes), main circulation coolant pipeline (eight volumes), reactor coolant pump (RCP) and cold leg (four volumes). The RCP has been simulated by pump characteristics, rated flow, head and speed. Pump trip is simulated by coast down speed, which is given as input. The pressurizer is divided into 10 volumes. The connecting pipeline between pressurizer and hot leg is divided into three volumes. Relief line is simulated by single volume and PSDs are simulated by trip valves. Nodalisation of the secondary circuit involves steam generators, steamlines, MSIVs, electrical isolation valve on second steam line, main steamline header, turbine stop valve and governor valve. Feedwater is simulated as a boundary condition.

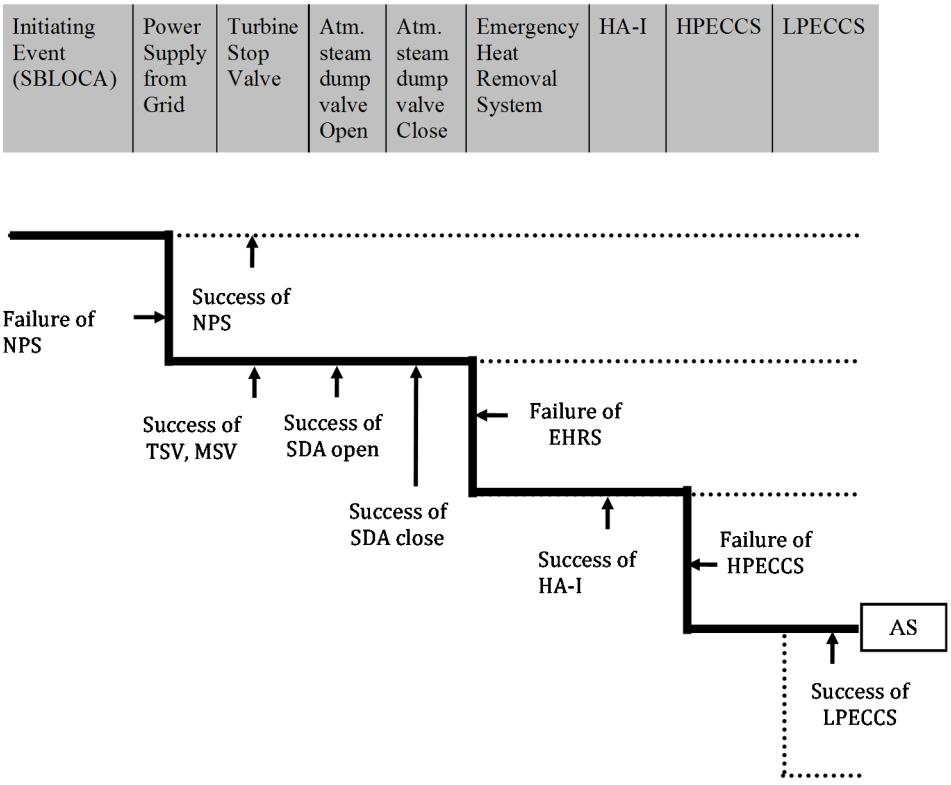

FIG. 2. Representation of accident sequence considered.

The steady state has been obtained after modelling of the various reactor components. The steady state was run for 1000 seconds. The steady state values are used as the initial conditions for the accident scenario considered. Some of the initial conditions are shown in Table 3. The SBLOCA analysis was considered for another 1000 s for the estimation of PCT. It is assumed that the core will be cooled subsequently.

The thermal hydraulic code calculations were performed for accident sequence (AS). In this accident sequence, power supply from grid, turbine stop valve, atmospheric steam dump valve open and close, emergency heat removal system, Hydro-accumulator-I, HPECCS and LPECCS are modelled. The accident sequence mainly consists of success of the turbine stop valve, atmospheric steam dump valve open and close, HA-I, LPECCS system and failure of power supply, emergency heat removal system and HPECCS is considered. The success of HA-I is incorporated in the code run by considering one train out of four success of HA. Similarly, the LPECCS success is included as one train success. The overall peak in the total transient analysis for 1000 seconds for AS accident sequence is obtained. The maximum PCT reached in one of the code run for maximum power channel accident sequence is indicated in Figure 3. The histogram for PCT of SBLOCA at 100% power is indicated in Figure 4.

TABLE 3. INITIAL CONDITIONS

Parameter	Value
Coolant temperature at reactor inlet, ^{0}C	293.0
Coolant pressure at the core outlet, MPa	15.7
Coolant flow rate through reactor, m^3/h	82200.0
Level in steam generator, m	2.2
Steam pressure in SG steam header, MPa	6.27
Steam rate to turbine kg/s	1696
Feed water flow rate into one SG, kg/s	424.0
Feed water temperature, ^{0}C	210.0
Maximum radial peaking factor	1.86
Fuel temperature coefficient of reactivity, 1/ ^{0}C	-0.000033
Effective fraction of delayed neutrons, %	0.77
Prompt lifetime, μs	35.0
Fraction of coolant flow rate in the core bypass channel %	3.0

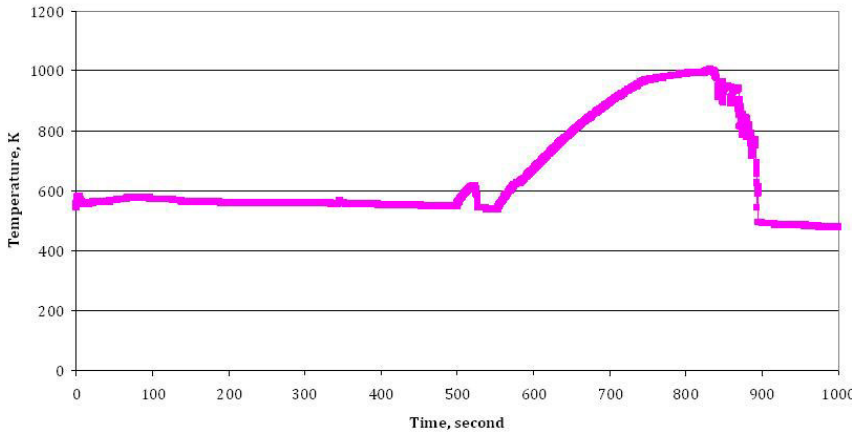

FIG. 3. Clad Temperature of maximum power channel for Accident Sequence (AS).

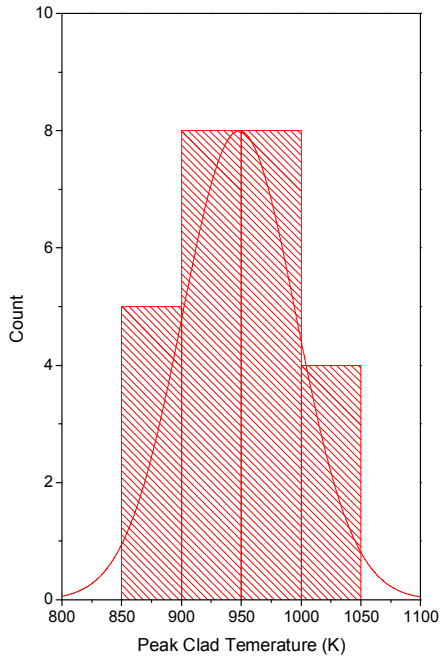

FIG. 4. Histogram of PCT for Accident Sequence (AS).

8. METHODOLOGY FOR PCT UNCERTAINTY ESTIMATION

Five uncertain input parameters, namely, nominal power level, decay power, fuel clad gap conductivity, fuel thermal conductivity and discharge coefficient were selected. These parameters and their nominal, minimum and maximum values were selected based on sensitivity studies reported in literature and engineering judgment. Twenty five code runs were carried out using various combinations of the above five parameters and peak clad temperatures were obtained for 25 runs.

If the population mean and standard deviation are unknown, and the sample mean (μ_s) and sample standard deviation (σ_s) are known, the interval that contains P% of the population measurements with confidence coefficient of (1 – α) is determined by considering a tolerance limit factor, K, as

$$(\mu_s - K\sigma_s, \mu_s + K\sigma_s) \quad (1)$$

where the value of 'K' is a function of the number of samples type of probability distribution, N, P and confidence coefficient 1-α [5]. These values of K are tabulated for various values of the variables N, P and α for a particular probability distribution.

To determine the type of probability distribution for the data on PCT Kolgomorov-Sminroff goodness-of-fit test should be performed for all the five accident sequences [6]. In this test, the observed values in the increasing order $PCT_1 \leq PCT_2 \leq \ldots\ldots\ldots \leq PCT_{25}$ should be recorded. Then D_1 and D_2 are calculated for all the PCTs, with a hypothesized probability distribution function f(PCT) [with cumulative distribution function F(PCT)].

The maximum of the D_1 and D_2 is compared with D_c (critical value of D) for the confidence level of interest. The values of Dc are tabulated for the Kolgomorov-Sminroff method and depend on N and 1-α.

$$D_1 = \max |(\frac{i}{N}) - f(PCT_i)| \quad \text{for i = 1,2……..N} \tag{2}$$

$$D_2 = \max |f(PCT_i) - (\frac{i-1}{N})| \quad \text{for i = 1,2……..N} \tag{3}$$

$$D = \max((D_1, D_2)) \tag{4}$$

If $D < D_{criti}$, then the sample data follows the assumed distribution for which the goodness-of-fit test is performed. For testing by the Kolgomorov-Sminroff method, for this accident sequence, the hypothesis is that the output data follows normal distribution and the goodness-of-fit test indicated that the hypothesis is true. Thus the PCT in each of the accident sequence follows a normal distribution.

It is noted that $D < D_{criti}$, so the sample data follows the assumed normal distribution for which the goodness-of-fit test is performed and it is passed.

In this analysis, the lower 95% probability value with 95% confidence limit on SM is desired [7]. The one sided tolerance limit factor, K, was calculated from equation (5).

$$K = \frac{Z_{1-P} + \sqrt{(Z_{1-P})^2 - a*b}}{a} \tag{5}$$

$$a = 1 - \frac{(Z_{1-\alpha})^2}{2(N-1)} \; ; \quad b = (Z_{1-P})^2 - \frac{(Z_{1-\alpha})^2}{N} \tag{6}$$

where N = sample size, P = percentage probability, 1- α = percentage confidence

with N = 25, P = 0.95 and 1 - α = 0.95, $Z_{1-P} = 1.64$, $Z_{1-\alpha} = 1.64$. From the above equation,

a = 0.9439667 and b=2.582016

Based on equation (5), the tolerance limit factor is 2.2695, i.e., K=2.2695.

The safety margin (SM) for each of the 25 PCT for an the accident sequence is calculated from

$$SM_i = 1473 - PCT_i \text{ where i = 1, 2…….25} \tag{7}$$

The 25 values for SM for each accident sequence would follow normal distribution as the PCT for each accident sequences follows normal distribution. The maximum likelihood estimator for the mean and standard deviation of SM are given by:

$$\mu = \frac{\Sigma SM_i}{N} \quad \text{where i = 1, 2……..25, N = 25} \tag{8}$$

$$\sigma = [\frac{\Sigma(SM_i - \mu)^2}{N-1}]^{0.5} \quad \text{where i = 1, 2……..25, N = 25} \tag{9}$$

From equations (8) and (9):

μ = 528.8914 °K and σ = 47.3669

For Accident Sequence (AS):

Safety margin corresponding 95% confidence and 95% probability values is calculated from

$$SM = \mu_{AS} - K * \sigma_{AS} \tag{10}$$

where μ_{AS} and σ_{AS} are the mean and standard deviation of the normal distribution which the SM is follows. The mean, standard deviation and lower limits for safety margin are calculated from equation (10), SM = 416.91 °K

9. LINEAR REGRESSION FOR SAFETY MARGIN

To obtain more values of PCT for all accident sequences, a multiple second order linear regression model was used. The form of the model is as shown below:

$$Y = A_0 + \Sigma A_i * X_i + \Sigma A_i * X_i^2 + \Sigma(\Sigma B_{jk} * X_j * X) \text{ …..i = 1 to 5, j = 1 to 4, k =1 to 4} \tag{11}$$

where Y is the PCT and X_i are the 5 input uncertain parameters considered in the analysis and A_o, A_i and B_{jk} are the regression coefficients. In the squared terms, all the five input parameters are considered and in the product terms, four parameters (except discharge coefficient) are considered. The above model was used for AS. The LHS sampling technique is considered and 1000 sample size were generated. With the data available for PCT from various code runs, the coefficients were obtained using a FORTRAN program. With the linear equation obtained, PCT values were obtained for accident sequence 4. The safety margin corresponding to each PCT should be obtained. The mean, standard deviation and safety margin corresponding to 95/95 estimated PCT data (N = 1000) were calculated. With regression analysis, the calculated mean was 944.77 °K and the variance is 59.39. The histogram of PCT generated from regression analysis is shown in Figure 5. The calculated safety margin using regression analysis is 393.46 °K.

10. SUMMARY AND CONCLUSIONS

In the present study, uncertainty quantification using sampling based method has been used for estimating peak clad temperature and safety margin. For uncertainty quantification of thermal hydraulic transient analysis with a large computer code where limited time and resources are present, the LHS method is very efficient and useful. The Kolgomorov-Sminroff method goodness-of-fit test is useful for probability testing for smaller data set. In the present uncertainty analysis for SBLOCA only five parameters were considered. However, for more rigorous analysis many other uncertain parameters may also need to be considered to examine their effect on available SM for more realistic and reliable results. However, the study has provided insights into the realistic results expected during possible accident sequence drawn from event tree for SBLOCA. The measure of robustness of the safety system design can also be judged from the available $SM_{95/95}$. The minimum of the lower tolerance limit for SMs from the accident sequences would indicate the 95 percent confidence with 95 percent probability of the robustness of the safety systems.

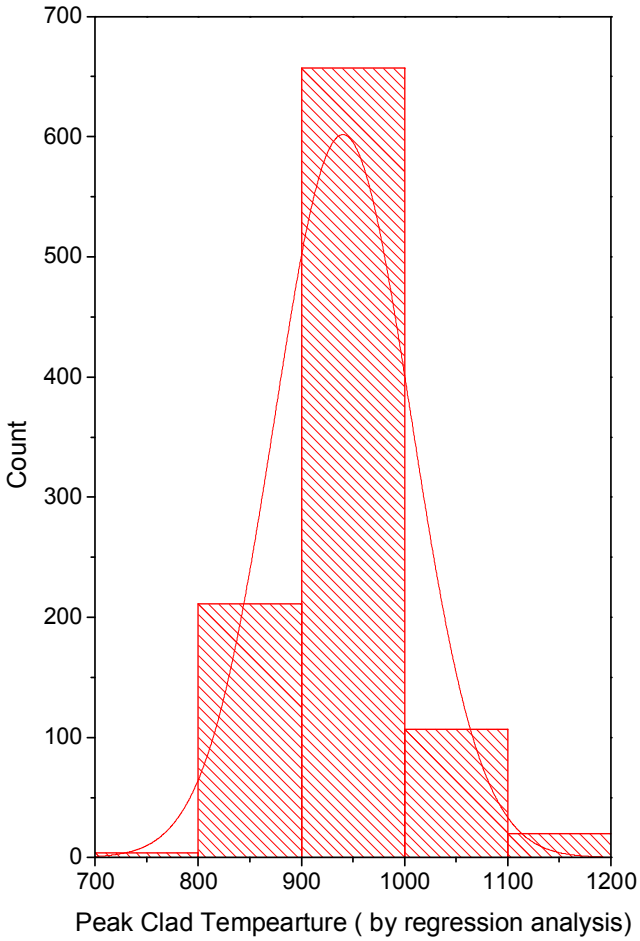

FIG. 5. Histogram of PCT for Accident Sequence (AS) using regression analysis.

The specific conclusions drawn from the present analysis are:

a) The uncertainty methodology using sampling based technique is relatively simple and efficient and easy to apply.
b) The safety margin for 25 code runs of non-core damage accident sequence was predicted as 416 °K in SBLOCA and mean PCT was 948.25 °K and standard deviation is 47.52.
c) The PCT obtained from Regression analysis is a good fit and the safety margin obtained is 393 °K and mean PCT obtained is 944.76 °K and the standard deviation is 59.39.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Implication of Power Uprate on Safety Margin, IAEATECDOC- 1418, Vienna (2003).

[2] ATOMIC ENERGY REGULATORY BOARD, Safety code on Design of pressurised Heavy water reactor based Nuclear power plants, AERB/NPP-PHWR/SC/D (Rev. 1) (2009).

[3] Final Report – Safety Margin Action Plan – Task Group on Safety Margins Action Plan (SMAP), NEA /CNNI/r(2007)9, July (2007).

[4] PARK, S-R., et al., Development of an Uncertainty Quantification Method of the Best Estimate large LOCA Analysis, Nuclear Engineering and Design, Volume 135, 367-378 (1992) .

[5] MONTGOMERY, D.C., AND RUNGER, G.C., Applied Statistics and Probability for Engineers, John Wiley& Sons (1994).

[6] EBELING, C.E., An Introduction to Reliability and Maintainability Engineering, Ninth Reprint, Tata McGraw –Hill, Ninth Reprint (2008).

[7] NIST/SEMATECH e-Handbook of Statistical Methods, http://www.itl.nist.gov/div898/handbook/, 2009.

SAFETY MANAGEMENT AND SAFETY CULTURE SELF ASSESSMENT OF KARTINI RESEARCH REACTOR

S. SYARIP
Centre for Accelerator and Material Process Technology,
National Nuclear Energy Agency (BATAN),
Yogyakarta, Indonesia
E-mail: syarip@batan.go.id

Abstract

The self-assessment of safety culture and safety management status of Kartini research reactor is a step to foster safety culture and management by identifying good practices and areas for improvement, and also to improve reactor safety in a whole. The method used in this assessment is based on questionnaires provided by the *Forum for Nuclear Cooperation in Asia* (FNCA), then reviewed by experts. Based on the assessment and evaluation results, it can be concluded that there were several good practices in maintaining the safety status of Kartini reactor such as: reactor operators and radiation protection workers were aware and knowledgeable of the safety standards and policies that apply to their operation, readily accept constructive criticism from their management and from the inspectors of regulatory body that address safety performance. As a proof, for the last four years the number of inspection/audit findings from Regulatory Body (BAPETEN) tended to decrease while the reactor utilization and its operating hour increased. On the other hands there were also some comments and recommendations for improvement of reactor safety culture, such as that there should be more frequent open dialogues between employees and managers, to grow and attain a mutual support to achieve safety goals.

1. INTRODUCTION

The management of safety at the research reactor facility will be effective if the operating organization develops a safety culture to a high level. The safety culture will influence the actions and interactions of all individuals and organizations engaged in activities relating to nuclear technology. The concept of safety culture is described in INSAG-4, which sets conditions at three levels: (a) at the policy level; (b) for managers; and (c) for individuals [1]. The objective of this research work is to complete the self-assessment of safety culture and safety management system status as part of efforts to assure safety of Kartini reactor operation. Kartini research reactor is one of the three research reactors operated in Indonesia, located at the Centre for Accelerator and Material Process Technology (CAMPT). CAMPT was founded in 1964 as one of the research facilities under the authority of the National Nuclear Energy Agency (BATAN). Kartini reactor has been in operation since 1979 and the latest operation license from Regulatory Body (BAPETEN) valid until 2019 [2].

Nuclear safety culture and safety management is one of special precautions that are required to protect the nuclear facility worker and the public from the consequences of an accident. With a good nuclear safety culture and safety management in place, it is possible to minimize the risk of working in the nuclear energy application and to minimize the risk to the public. It is therefore, very important to upgrade our understanding to support of a better nuclear safety culture. The self-assessment of safety culture and safety management status of Kartini research reactor is a step to foster safety culture and management by identifying good practices and areas for improvement, and also to improve reactor safety as a whole.

2. METHOD

The method used in this assessment is based on questionnaires provided by the *Forum for Nuclear Cooperation in Asia* (FNCA) then reviewed by experts [3]. Each question and topic contained in FNCA questionnaire were considered and discussions were held between the review members and the Reactor Division staff and Safety Division staff, then good practices (GP) or potential areas for improvement were identified. The objective is to identify good practices and suggest practical and sustainable recommendations for areas where improvement may be made and

to share the knowledge among the assessment team so that improvements may be achieved among all related staff. Assessment results were grouped as follows: *Organization and Management, Safety Objectives of Organization, Activities to Foster Safety Culture, Emergency Plan, Education & Training, Operation & Maintenance, Radiation Protection, Treatment and Reduction of Radioactive Waste, and Measures of Importance to Safety.*

Whiles, to provide the comprehensiveness of the reactor utilization improvement program, the SWOT (strength, weakness, opportunity, and threat) analysis method is used.

3. RESULT AND DISCUSSION

3.1. Safety Culture Assessment Result

Based on the assessment and evaluation results, it can be concluded that there were several good practices in maintaining the safety status of Kartini reactor such as: reactor operators and radiation protection workers were aware and knowledgeable of the safety standards and policies that apply to their operation, readily accept constructive criticism from their management and from the inspectors of regulatory body that address safety performance. Figure 1 shows that, for the last four years, the number of inspection and audit findings from Regulatory Body (BAPETEN) tended to decrease while the reactor utilization/services and its operating hour increased (see Table 1 and Figure 2.) [4, 5].

On the other hands there were also some comments and recommendations for improvement of reactor safety culture, such as that there should be more frequent open dialogues between employees and managers to grow and attain a mutual support to achieve safety goals. It was realized that the success in developing a safety culture depends on the knowledge and effectiveness in recognizing and responding to safety deficiencies. The matter was also underlined in the national regulations [6].

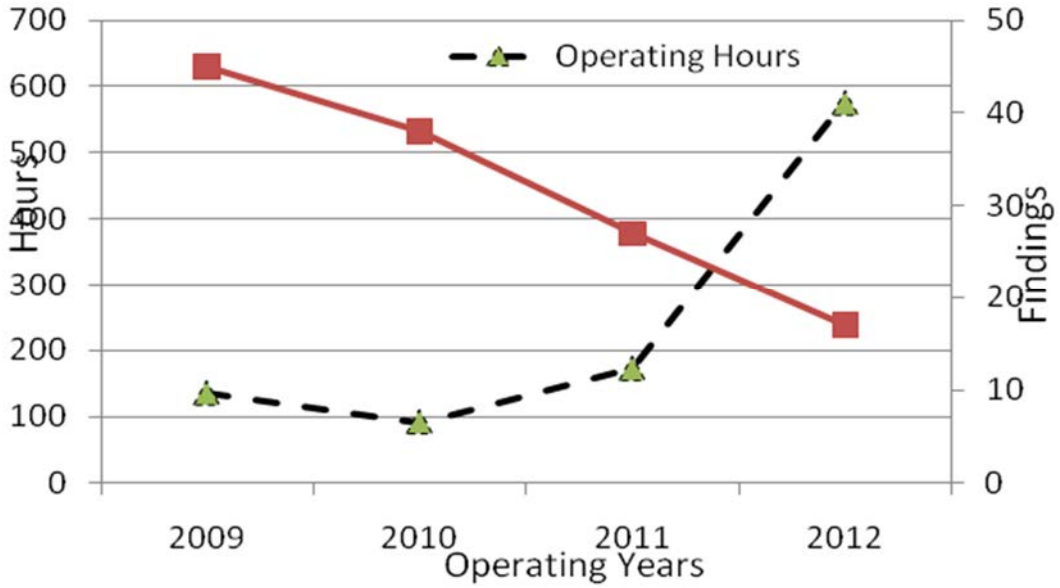

FIG.1. Regulatory Body inspection findings and reactor utilization (2009-2012).

TABLE 1. KARTINI REACTOR SERVICES (2012)

Product type	Service (hour)
Irradiation	391.1
Experiment/research	84.3
Calibration/tests	8.23
Student Practices	90.3
Inspection	1.35
Total	575.9
Average	5.1 hours/operation

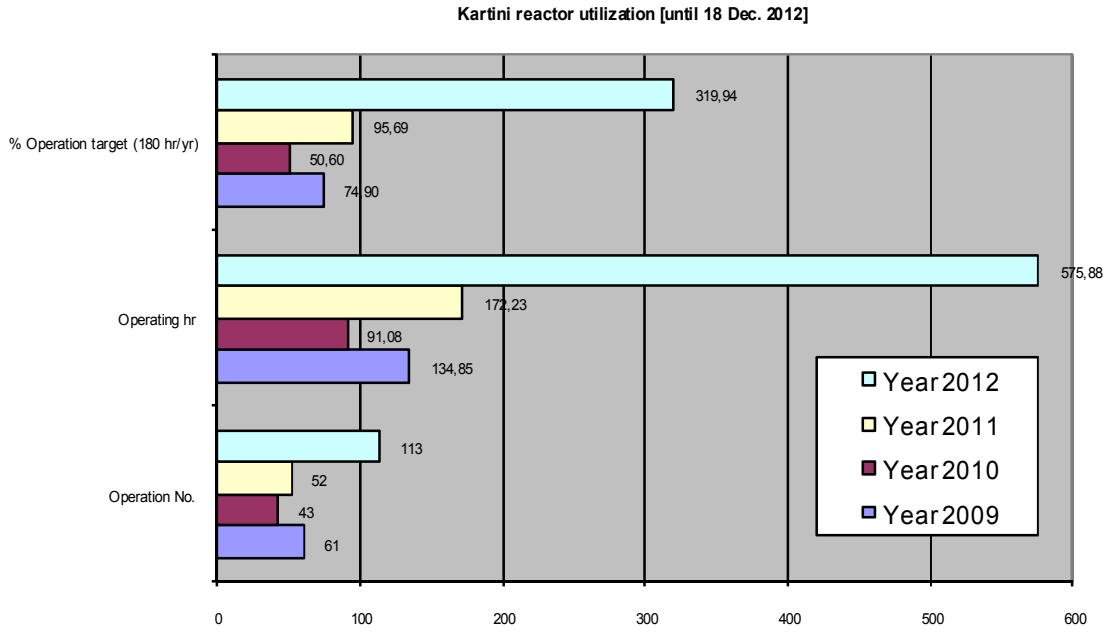

FIG.2. Kartini reactor utilization (2009-2012).

Resume results on Good Practice (GP):

- All activities of the CAMPT are carried out by its own staff and the interface problem which might be caused by introducing external manpower is avoided.
- A family-like atmosphere and mutual support among staff is noted and this may be a positive indication for enhancing safety culture.
- Kartini reactor has annual open houses for the public and many tours for students to show the value of the research reactor and to help public acceptance of nuclear research facilities.
- It appears that there is a positive safety culture at CAMPT. Staff demonstrated pride in their workplace and competence. There was strong evidence of respect for team members and consideration of safety in work practices. It was apparent that workers feel that they can make suggestions for improvement.
- The resource requirements for safety functions are reviewed regularly by senior management and the results are in the form of recommendations for the Director. The

CAMPT organization provides adequate resources for safe operation of the reactor by providing budget prioritized to safety related systems.

- Kartini reactor shares experiences and equipment with other two research reactors in the country, i.e. Bandung and RSG GA Siwabessy reactors and the top management provides a way to inform the experiences from other reactors or countries through a group e-mail system and staff forum held twice a year. Members of Kartini reactor staff have also been participating in regional and international meetings, thus ensuring awareness of best practices and issues at other research reactors.

3.2. SWOT Analysis Result for Kartini Reactor Utilization

The summary results of SWOT analysis for the Kartini reactor utilization improvement program are as follows [3, 5].

- ❑ Strength
  - ✓ Operation Licence from Regulatory Body (BAPETEN) until 2019.
    - No. 3513/PI01/PIBN/XII/2010 and
    - No. 4681/IO/Bapeten/6-XII/2010
  - ✓ Increasing reactor utilization and services (see Fig. 2 and Table 1).
  - ✓ Collaboration with universities (STTN, UGM, UNS, UNY).
- ❑ Weakness
  - ✓ Lack of public knowledge on neutron applications.
  - ✓ Funding problems and weak human resource policies for R&D (human resource ageing).
- ❑ Opportunities
  - ✓ Analytical technique for supporting mining exploration.
  - ✓ Collaboration with Pharmacy Faculty (anticancer development).
  - ✓ Collaboration with IT Malaysia, Hongkong City University (web base reactor laboratory).
  - ✓ Collaboration with Energy and Mineral Resources Ministry (Nuclear Training Centre).
- ❑ Threats
  - ✓ Earthquake 500 year period.
  - ✓ Volcanic eruption (Merapi mountain).
  - ✓ Operator Aging.
  - ✓ SSC Ageing.
  - ✓ Population growth around the reactor location.

It is shown from the SWOT analysis that the balance from the long term and short term programs perspectives was good enough (Figure 3). Whiles, balance between internal business process and stakeholders & customers perspectives, shows that the activities still rest on internal business processes, or the weight tends to internal business process, and this should be improved (Figure 4).

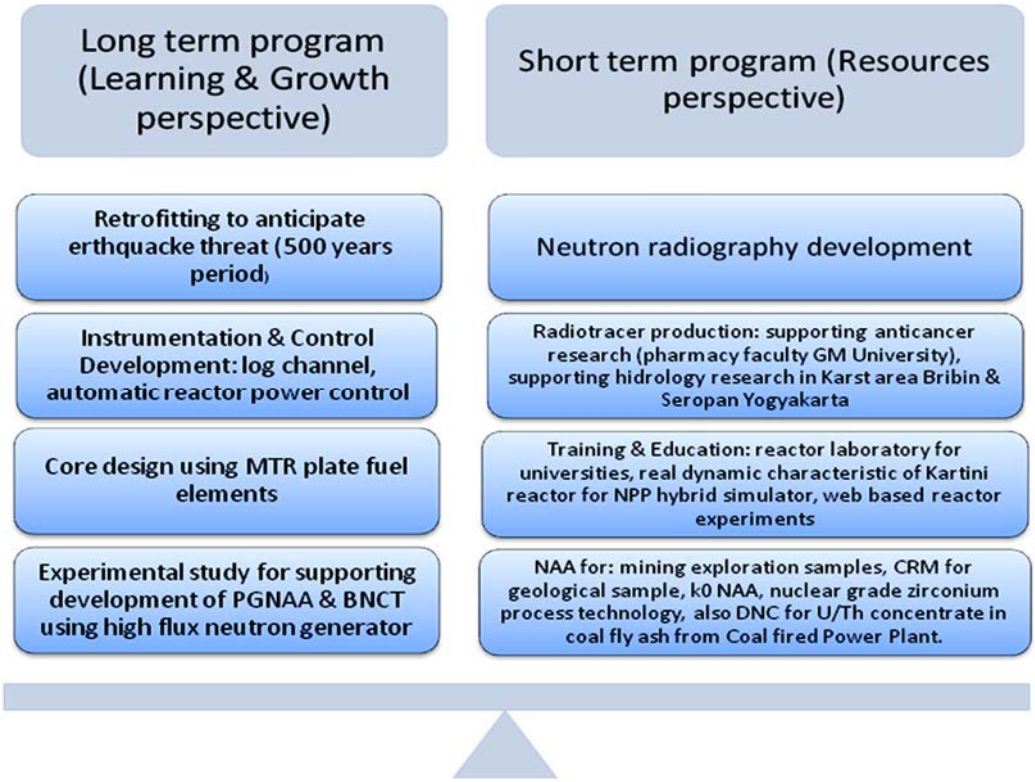

FIG. 3. Balance from the long term and short term programs perspectives.

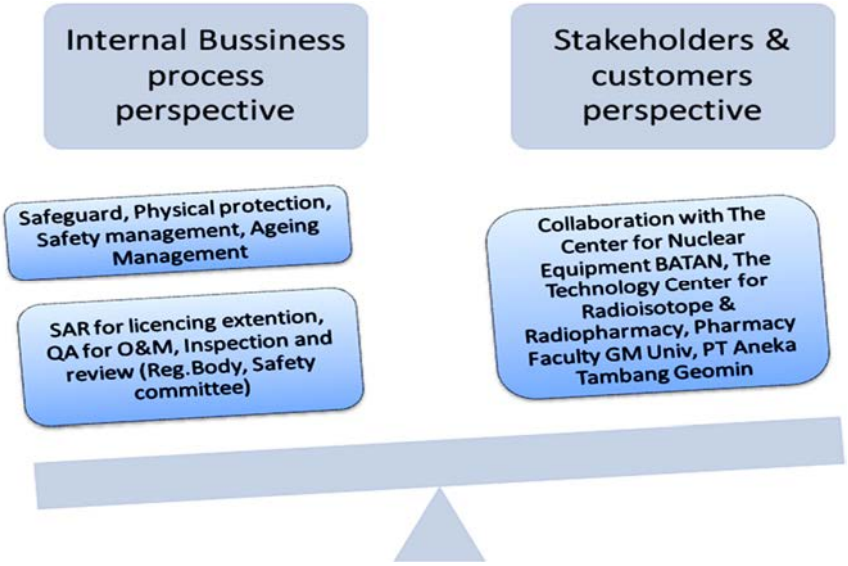

FIG .4. Balance between internal business process and stakeholders/customers perspectives.

4. CONCLUSIONS

Based on the assessment and evaluation results, it can be concluded that there were several good practices in maintaining the safety status of Kartini reactor such as: reactor operators and radiation protection workers were aware and knowledgeable of the safety standards and policies

that apply for their operation, readily accept constructive criticism from their management and from the inspectors of the regulatory body that address safety performance.

Safety culture implementation is a site specific program, and this safety management system and safety culture survey portrays the strength and weakness of the culture at a particular moment, and therefore it offers room for improvement. It was realized that the success in developing a safety culture depends on the knowledge and effectiveness in recognizing and responding to safety deficiencies. Since Kartini is a simple research reactor where good safety culture can be easily demonstrated, BATAN may wish to consider using it as a basic training facility for trainee operators for the other research reactors, and even for supporting National Nuclear Power Program.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP (INSAG), Safety Culture, INSAG Series No. 75-INSAG-4, IAEA, Vienna (1991).

[2] KARTINI REACTOR LICENSE, Decree of Chairmen of BAPETEN No. 3513/PI01/PIBN/XII/2010 and No. 4681/IO/Bapeten/6-XII/2010.

[3] FORUM FOR NUCLEAR COOPERATION IN ASIA (FNCA), Safety Management Systems for Nuclear Facilities Project, http: //www.fnca.mext.go.jp/english/sms/ e_ws_2012.html (2012).

[4] Status of Kartini Reactor Utilization in Supporting HRD Program, paper presented at the National Coordination Meeting in Bandung 21 December (2012).

[5] CAMPT, Kartini Quarterly Report Doc. No. LOR-T4/BR/2012.

[6] GOVERNMENT REGULATION NO. 63 Year 2000, on the Provision of Health and Safety on the Ionizing Radiation, and the Decree of Chairmen of BAPETEN No. 5-P / 2003 on the Guidelines of Implementation of Emergency Planning and Preparation.

LIST OF PARTICIPANTS

Argentina	Fabbri, S	CNEA Av. Libertado 8259 1429 BUENOS AIRES ARGENTINA Fax: +541167727318 EMail: fabbri@cnea.gov.ar
	Perrin, C	Autoridad Regulatoria Nuclear Av. Libertador 8250 1429 BUENOS AIRES ARGENTINA EMail: cperrin@arn.gob.ar
	Versaci, R	Comisión Nacional de Energía Atómica Avda. del Libertador 8250 1419 BUENOS AIRES ARGENTINA EMail: versaci@cnea.gov.ar
Armenia	Grigoryan, O	Haykakan Atomayin Elektrakayan CJSC Armenian Nuclear Power Plant 0910 METSAMOR ARMENIA Fax: +374 10 288580 EMail: anpp@anpp.am
Austria	Hossain, S	University of Natural Resources and Life Sciences (BOKU) Gregor Mendel Strasse 33 1190 VIENNA AUSTRIA EMail: shaheed.hossain@univie.ac.at
	Scheiner, S	QUANTEC Technologies Consulting Company Ltd Moelkergasse 3/15 1080 VIENNA AUSTRIA Fax: +43 1 369 5597 EMail: scheiner@quantec.at
	Weimann, G	NIMBUS Institute Buchbergstrasse 13 1140 VIENNA AUSTRIA Fax: +4315773915 EMail: geert.weimann@europe.com
Belgium	Fiorini, G-L	FANC Federal Agency for Nuclear Control Rue Ravenstein straat 36 1000 BRUSSELS BELGIUM EMail: gian-luigi.fiorini@orange.fr
	Hakimi, N	FANC Federal Agency for Nuclear Control Rue Ravenstein Straat 36 1000 BRUSSELS BELGIUM EMail: nourdine.hakimi@FANC.FGOV.BE
	Scheveneels, G	SCK CEN Boeretang 200 2400 MOL BELGIUM

		EMail: guy.scheveneels@SCKCEN.BE
Brazil	Kassab Junior, F	USP/EP/PTC Av. Praf. Luciano Gualberto -tv 3, 158 05508-010 SAO PAULO BRAZIL Fax: +55 11 3091 5275 EMail: fuad@lac.usp.br
	Marques, R	University of Sao Paulo USP/EP/PTC, Av Praf. Luciano Gualberto -tv.3, 158 05508-010 SAO PAULO BRAZIL Fax: +55 11 3091 5275 EMail: rpm@lac.usp.br
	Oliveira Neto, J	Centro Tecnologico da Marinha em São Paulo Av. Prof. Lineu Prestes, 2468 Cid. Universitaria Butanta CEP 05508-00 SÃO PAULO BRAZIL EMail: messias@ctmsp.mar.mil.br
Bulgaria	Rashkov, K	Kozloduy NPP Plc Kozloduy, Block 72-A-3 BULGARIA EMail: kprashkov@yahoo.com
Canada	Dermarkar, F	Ontario Power Generation 889 Brock Rd, 6th Floor E2 Pickering L1W3J2 ONTARIO CANADA Fax: +1 905 837 3986 EMail: fred.dermarkar@opg.com
	Lun, K	Canadian Nuclear Safety Commission Directorate of Regulatory Improvement and Major Projects Management 280 Slater Street PO Box 1046, Station B K1P 5S9 OTTAWA CANADA EMail: Kenneth.Lun@cnsc-ccsn.gc.ca
	Winfield, D	248 Burkes Road, R.R -1 Deep River KOJ 1PO ONTARIO CANADA EMail: winfieldddavid@bell.net
China	Liu, S	Nuclear Power Institute of China No.25,Third Section South Second Ring Road CHENGDU CHINA Fax: +862885908191 EMail: liusongtao.npic@gmail.com
	Liu, T	Institute of Nuclear and New Energy Technology Tsinghua University 10008 BEIJING CHINA 19 Fax: +86 1062797135 EMail: Liu-tao@tsinghun.edu.cn

	Shi, G	Shanghai Nuclear Engineering Research & Design Institute 29 Hongcao Road Xuhui District 200233 SHANGHAI CHINA 20 Fax: +86 21 61860728 EMail: shi@snerdi.com.cn
	Wang, Y	China Nuclear Power Design Co. Ltd CGNPC (China Guangdong Nuclear Power Holding Co. Ltd) No.7018 Beihuan Ring Road Xia Meilin, Futian District SHENZHEN CHINA Fax: +86 755 84432200 EMail: wangyuhong@cgnpc.com.cn
Czech Republic	Hojny, V	State Office for Nuclear Safety (SUJB) Senovazne námesti 9 11000 PRAGUE 1 CZECH REPUBLIC Fax: +420221624821 EMail: Vaclav.Hojny@sujb.cz
	Kaderabek, T	SUJB (State Office for Nuclear Safety) Senovazne namesti 9 110 00 PRAGUE CZECH REPUBLIC Fax: +420 221 624 821 EMail: tomas.kaderabek@sujb.cz
	Misak, J	Nuclear Research Institute Rez Voskovcova 1130-30 Hlubocepy PRAGUE 5 CZECH REPUBLIC EMail: mis@ujv.cz
	Stuller, J	State Office for Nuclear Safety Senovazne nam. 9 11000 PRAGUE CZECH REPUBLIC Fax: +420 221 624 821 EMail: jan.stuller@sujb.cz
Egypt	Elsheikh, B	Nuclear and Radiological Regulatory Authority 3 Ahmed El Zomor St Nasr City 11762 CAIRO EGYPT Fax: +202 22740238 EMail: badawymel@yahoo.com
	Salem, W	Nuclear and Radiological Regulatory Authority (NRRA) 3 Ahmed El-Zomor Str. Nasr City, PO Box 7551 11762 CAIRO EGYPT Fax: +202 22740238 EMail: wafaasalem21@yahoo.com

	Tawfik, F	Egyptian Nuclear and Radiological Regulatory Authority (NRRA) 3 Ahmed El-Zomor St Nasr City, PO Box 7551 11762 CAIRO EGYPT Fax: +202 22740238 EMail: basant572000@yahoo.com
Finland	Aaltonen, H	Radiation & Nuclear Safety Authority (STUK) Emergency Preparedness Department PO Box 14 Laippatie 4 FI-00881 HELSINKI FINLAND EMail: hannele.aaltonen@stuk.fi
	Järvinen, M	STUK - Radiation and Nuclear Safety Authority Laippatie 4 PO Box 14 00880 HELSINKI FINLAND Fax: +358 9 7598 8382 EMail: Marja-Leena.Jarvinen@stuk.fi
	Routamo, T	STUK – Radiation and Nuclear Safety Authority PO Box 14 Laippatie 4 00881 HELSINKI FINLAND EMail: Tomi.Routamo@stuk.fi
France	Barbaud, J	EDF 12 avenue Dutrievoz 69628 Villeurbanne PARIS FRANCE EMail: jean.barbaud@edf.fr
	De Bois, F	AREVA 1 Place Jean Millet La Defense 92084 FRANCE EMail: Francoise.debois@areva.com
	de L'Epinois, B	AREVA 33 rue la Fayette Cedex 09 75442 PARIS FRANCE EMail: bertrand.delepinois@areva.com
	Feron, F	Autorité de sureté nucléaire (ASN) 15 rue Louis Lejeune CS 70013 Montrouge 9251 FRANCE Fax: +33 1 46164431 EMail: fabien.feron@asn.fr
	Forest, I	ASN- Autoritéde Sureté Nucléaire 15 rue Louis Lejeune CS70013 Montrouge 92541 FRANCE

		EMail: isabelle.forest@asn.fr
	Herviou, K	IRSN BP 17 92 262 Fontenay aux rose FRANCE EMail: karine.herviou@irsn.fr
	Jamet, P	Autorité de Sureté Nucléaire (ASN) 15 rue Louis Lejeune CS70013 92541 MONTROUGE CEDEX FRANCE EMail: Philippe.JAMET@asn.fr
	Lacoste, A	15 rue Louis Lejeune CS70013 92541 MONTROUGE CEDEX FRANCE
	Lavarenne, C	IRSN BP17 92262 Fontenay aux roses Cedex FRANCE Fax: +33 158357867 EMail: caroline.lavarenne@irsn.fr
	Pouget-Abadie, X	EDF-DIN Cap Ampère 1 place Pleyel Saint Denis Cedex 93282 VILLEURBONNE FRANCE EMail: xavier.pouget-abadie@edf.fr
	Thiry, J	AREVA 10 Rue Juliette Récamier Cedex 06 69456 LYON FRANCE EMail: jeanmichel.thiry@areva.com
	Tiberi, V	IRSN/PSN-SRDS/CNR BP 17 Cedex FONTENAY AUX ROSES FRANCE EMail: vincenzo.tiberi@irsn.fr
Hungary	Elter, J	MVM Paks Nuclear Power Plant Ltd. PO Box 71 7031 PAKS HUNGARY Fax: +3675506949 EMail: elter@npp.hu
India	Gaikwad, A	Atomic Energy Regulatory Board CAERB Niyamak Bhavan Anushaktinagar 400094 MUMBAI INDIA Fax: +912225990499 EMail: avinashg@aerb.gov.in
	Pradhan, S	Tarapur based Reprocessing Plant Bhabha Atomic Research Centre (BARC) Via Boisar (WR)

		401502 MAHARASHTRA INDIA Fax: +91 2525 244158 EMail: spradhan@barctara.gov.in
Indonesia	Hardiyanti, H	Center for Nuclear Fuel Technology - National Nuclear Energy Agency Gd. 65 Kawasan Puspiptek Cisauk Tangerang Selatan 15314 INDONESIA Fax: +62 21 7560909 EMail: hrdyanti@batan.go.id
	Syarip, S	National Nuclear Energy Agency(BATAN) Centre for Accelerator and Material Process Technology (CAMPT) 55281 YOGYAKARTA INDONESIA Fax: +62 274 489762 EMail: syarip@batan.go.id
Iran, Islamic Republic of	Haghighi Shad, A	National Nuclear Safety Department of INRA of AEOI IRAN, ISLAMIC REPUBLIC OF Fax: +98 771 4117395 EMail: 1976negar@gmail.com
Israel	Hirschfeld, H	Israel Atomic Energy Commission Soreq Nuclear Research Center 81800 YAVNE ISRAEL Fax: +972-3-6428616 EMail: hirshfel@soreq.gov.il
Italy	Picca, P	ENEL spa Via Regina Margherita 135 ROME ITALY EMail: paolo.picca@enel.com
Japan	Ueda, N	Japan Nuclear Safety Institute 14F Mita Bellju Bldg 5-36-7 Shiba Minato-ku 108-0014 TOKYO JAPAN Fax: +81-3-5418-9314 EMail: ueda.nobuyuki@genanshin.jp
	Yamagata, H	Nuclear Regulation Authority Nuclear Regulation Division 1-9-9 Roppongi-First Bldg 5F Roppongi Minato-ku TOKYO JAPAN Fax: +81 3 5114 2178 EMail: hiroshi_yamagata@nsr.go.jp
Korea, Republic of	Baek, W-P	Korea Atomic Energy Research Instiute (KAERI) Daedeok-daero 898-111 Yuseong-gu 305-353 DAEJEON KOREA, REPUBLIC OF Fax: +82 42 868 8583 EMail: wpbaek@kaeri.re.kr

	Kim, K-J	KETEP Korea Institute of Energy Technology Evaluation and Planning teheran-ro 114gil 14 Gangnam-gu SEOUL KOREA, REPUBLIC OF EMail: kjkim32@ketep.re.kr
	Youm, H	KETEP Korea Institute of Energy Technology Evaluation and Planning Teheran-ro 114gil 14 Gangnam-gu SEOUL KOREA, REPUBLIC OF Fax: + 82 2 02 556 1033 EMail: hockey@ketep.re.kr
Lithuania	Legenis, V	Lithuanian State Nuclear Power Safety Inspectorate Gostalito 12 01108 VILNIUS LITHUANIA Fax: +370 5 261 4487 EMail: atom@vatesi.lt
Malaysia	Ramli, A	Universiti Teknologi Malaysia Physics Department, Faculty of Science 81310, Skudai, Johor MALAYSIA EMail: termiziramli@gmail.com
Pakistan	Khan, L	Pakistan Atomic Energy Commission PO Box 3416 ISLAMABAD PAKISTAN Fax: +92 51 9203921 EMail: samasl@yahoo.com
Paraguay	Aguinagalde Gallinar, N	Comisión Nacional de Defensa de Recursos Naturales (CONADERNA) 14 de Mayo esquina Avenida República Palacio Legislativo Cámara de Senadores 2do Piso ASUNCIÓN PARAGUAY Fax: +595214145244 EMail: conaderna@senado.gov.py
Peru	Rengifo, C	Ux Consulting Company 1501 Macy Drive 30076 ROSWELL UNITED STATES OF AMERICA EMail: christhian.rengifo@uxc.com
Poland	Czerski, P	PGE EJ 1 sp. z o.o. ul.Mokotowska 49 00-542 WARSAW POLAND Fax: +48223401041 EMail: Piotr.Czerski@gkpge.pl

Romania	Vieru, G	Institute for Nuclear Research Romanian Nuclear Energy Association 65 Polona Street Sector 1 PO Box 22-102 010494 BUCHAREST ROMANIA Fax: +40 21 3169400 EMail: g_vieru@yahoo.com
Russian Federation	Aydemirov, O	JSC Concern Rosenergoatom Ferganskaya str. 25 109507 MOSCOW RUSSIAN FEDERATION Fax: +7 495 6474389 EMail: aydemirov-oa@rosenergoatom.ru
	Fokin, R	The Permanent Mission of Russia Erzherzog-Karl-Strasse 182 1220 VIENNA AUSTRIA EMail: roman.fokin@rusmission.org
	Klyazhnikov, A	The Permanent Mission of Russia Erzherzog-Karl-Strasse 182 1220 VIENNA AUSTRIA EMail: alexander.klyazhnikov
	Kuznetsov, M	Federal State Unitary Enterprise VO "Safety" (FSUE Vo "Safety") Taganskaya St. 34a 109147 MOSCOW RUSSIAN FEDERATION Fax: + 7 495 912 0620 EMail: kuznetsov_mv@vosafety.ru
	Lankin, M	Scientific and Engineering Centre for Nuclear and Radiation Safety Malaya Krasnoselskaya St, 2/8 bld. 5 107140 MOSCOW RUSSIAN FEDERATION Fax: + 7 499 264 2859 EMail: lankin@secnrs.ru
	Maximov, Y	JSC Concern Rosenergoatom/Balakovo NPP Balakovo 26 Saratov Region 413866 RUSSIAN FEDERATION Fax: +7 845349 75 68 EMail: maym@balnps.rosenergoatom.ru
	Morozov, V	JSC Atomenergoproekt Bakuninskaya str. 7 Bld 1 105005 MOSCOW RUSSIAN FEDERATION Fax: +7 495 315 9337 EMail: morozov@aep.ru
	Moskalenko, A	GCE Group 6 Bukharestskaye st 192102 ST. PETERSBURG RUSSIAN FEDERATION EMail: gce@gce.ru
Slovakia	Turner, M	Nuclear Regulatory Authority of the Slovak Republic

		Bajkalska 27 PO Box 24 82007 BRATISLAVA SLOVAKIA Fax: +421 2 58221166 EMail: mikulas.turner@ujd.gov.sk
South Africa	Belal, M	South African Nuclear Energy Corporation Necsa Church Street West Pelindaba 0001 PRETORIA SOUTH AFRICA Fax: +27123055166 EMail: mohamed.belal@necsa.co.za
Sweden	Almberger, T	Swedish Radiation Safety Authority Department of Nuclear Power Plant Safety Solna Strandv 96 SE-17116 STOCKHOLM SWEDEN EMail: tomas.almberger@ssm.se
	Kastberg, I	SKB Swedish Nuclear Fuel and Waste Management Co PO Box 612 SE-572 29 OSKARSHAMN SWEDEN EMail: inge.kastberg@skb.se
	Lindahl, P	OKG AB SE-57283 OSKARSHAMN SWEDEN EMail: par.lindahl@okg.eon.se
	Myhrberg, B	Ringhals NPP Ringhalsverket 43285 VAROBACKA SWEDEN Fax: +46 340 637310 EMail: bjorn.myhrberg@vattenfall.com
	Persson, S	Forsmarks Kraftgrupp AB Forsmarksverken 742 03 ÖSTHAMMAR SWEDEN EMail: snn@forsmark.vattenfall.se
	Wallin Caldwell, L	Swedish Radiation Safety Authority 17116 STOCKHOLM SWEDEN Fax: +4687994010 EMail: lovisa.wallin.caldwell@ssm.se
United Arab Emirates	Eltawila, F	Federal Authority for Nuclear Regulation PO Box 112021 ABU DHABI UNITED ARAB EMIRATES Fax: +971 2 651 6661 EMail: farouk.eltawila@fanr.gov.ae
United Kingdom	Davies, L	Office for Nuclear Regulation 4S.3 Redgrave Court Merton Road Bootle Merseyside L20 7HS UNITED KINGDOM EMail: les.davies@hse.gsi.gov.uk

	Weightman, M	Office for Nuclear Regulation (ONR) Mill Bank Burwardsley Road Tattenhall Cheshire CH3 9NS UNITED KINGDOM EMail: mike_weightman@hotmail.com
United States of America	Langerman, N	Advanced Chemical Safety Inc PO Box 152329 92195 SAN DIEGO CA UNITED STATES OF AMERICA EMail: neal@chemical-safety.com
Vietnam	Nguyen, H	Vietnam Agency for Radiation and Nuclear Safety (VARANS) 14th Floor 113 Tran Duy Hung HANOI VIETNAM Fax: 0084 4 38220298 EMail: nhanh@varans.vn
ECC	Ranguelova, V	European Commission: Joint Research Centre CDMA 4/180 B1049 BRUSSELS BELGIUM EMail: vesselina.ranguelova@ec.europa.eu
IAEA	Aparkin, F	International Atomic Energy Agency Department of Nuclear Safety and Security Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: F.Aparkin@iaea.org
	Baciu, F	International Atomic Energy Agency Department of Nuclear Safety and Security Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: F.Baciu@iaea.org
	Buglova, E	International Atomic Energy Agency Department of Nuclear Safety and Security Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: E.Buglova@iaea.org
	Callen, J	International Atomic Energy Agency Department of Nuclear Safety and Security Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: J.Callen@iaea.org
	Duchac, A	International Atomic Energy Agency Division of Nuclear Installation Safety Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: A.Duchac@iaea.org
	Flory, D	International Atomic Energy Agency Department of Nuclear Safety and Security

	Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: D.Flory@iaea.org
Fukushima, Y	International Atomic Energy Agency Division of Nuclear Installation Safety Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: Y.Fukushima@iaea.org
Hughes, P	International Atomic Energy Agency Divsion of Nuclear Installation Safety Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: P.Hughes@iaea.org
Kenny, P	International Atomic Energy Agency Department of Nuclear Safety and Security Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: P.Kenny@iaea.org
Khartabil, H	International Atomic Energy Agency Divsion of Nuclear Installation Safety Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: H.Khartabil@iaea.org
Kim, M	International Atomic Energy Agency Division of Nuclear Installation Safety Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: M.Kim@iaea.org
Kuzmina, I	International Atomic Energy Agency Division of Nuclear Installation Safety Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: I.Kuzmina@iaea.org
Lipar, M	International Atomic Energy Agency Division of Nuclear Installation Safety Wagramerstrasse 5 1400 VIENNA AUSTRIA Fax: +43126007 EMail: m.lipar@iaea.org
Lyons, J	International Atomic Energy Agency Division of Nuclear Installation Safety Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: J.Lyons@iaea.org
Masood, S	International Atomic Energy Agency Wagramerstrasse 5 1400 VIENNA AUSTRIA EMail: S.Masood@iaea.org

McKenna, T
International Atomic Energy Agency
Department of Nuclear Safety and Security
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: T.McKenna@iaea.org

Nicic, A
International Atomic Energy Agency
Division of Nuclear Installation Safety
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: A.Nicic@iaea.org

Poulat, B
International Atomic Energy Agency
Division of Nuclear Installation Safety
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: B.A.Poulat@iaea.org

Rao, D
International Atomic Energy Agency
Division of Nuclear Installation Safety
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: D.V.Rao@iaea.org

Samaddar, S
International Atomic Energy Agency
Division of Nuclear Installation Safety
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: S.Samaddar@iaea.org

Shokr, A
International Atomic Energy Agency
Division of Nuclear Installation Safety
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: A.Shokr@iaea.org

Skarbo, B
International Atomic Energy Agency
Division of Nuclear Installation Safety
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: B.Skarbo@iaea.org

Ulses, A
International Atomic Energy Agency
Division of Nuclear Installation Safety
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: A.Ulses@iaea.org

Vilar Welter, P
International Atomic Energy Agency
Department of Nuclear Safety and Security
Wagramerstrasse 5
1400 VIENNA
AUSTRIA
EMail: P.Vilar-Welter@iaea.org

Yllera, J
International Atomic Energy Agency
Division of Nuclear Installation Safety
Wagramerstrasse 5
1400 VIENNA
AUSTRIA

		EMail: J.Yllera@iaea.org
OECD	Blundell, N	OECD, Nuclear Energy Agency Le Seine Saint German 12 boulevard des Iles 92130 LES MOULINEAUX FRANCE EMail: Neil.Blundell@oecd.org
	Shimomura, K	OECD, Nuclear Energy Agency Le Seine Saint Germain 12 boulevard des Iles 92130 ISSY LES MOULINEAUX FRANCE Fax: +33(0)1 4524 1110 EMail: Kazuo.SHIMOMURA@oecd.org
WANO	Ellis, K	WANO Level 35 25 Canada Square Canary Wharf E14 5LQ LONDON UNITED KINGDOM Fax: +44 20 7513 2937 EMail: ken.ellis@wano.org
	Lagriffoul, F	EDF-WANO 22-30 Avenue de Wagram 75008 PARIS FRANCE EMail: fabien.lagriffoul@ef.fr
	Regaldo, J	WANO Level 35 25 Canada Square E14 5LQ LONDON UNITED KINGDOM EMail: jacques.regaldo@wano.org
OBSERVER	Fadeeva, E	JSC Atomenergoproekt Bakuninskaya str. 7 Bld 1 MOSCOW 105005 RUSSIAN FEDERATION EMail: morozov@aep.ru
	Habib, U	Pakistan Nuclear Regulatory Authority PO Box 1912 ISLAMABAD PAKISTAN EMail: uzman@pnra.org
	Moskalenko, A	GCE Bucharestkaye 6 ST. PETERSBURG RUSSIAN FEDERATION EMail: gcd@gce.ru
	Sussman, S	Advanced Chemical Safety PO Box 152329 CA 92195 SAN DIEGO UNITED STATES OF AMERICA EMail: sharronsuss@gmail.com
	Tereschchenko, A	JSC Concern Rosenergoatom Ferganskaya str. 25 MOSCOW RUSSIAN FEDERATION

Tuomisto, H

FORTUM
Keilaniementie 1
ESPOO
FINLAND
EMail: harri.tuomisto@fortum.com

Wasylyk, A

World Nuclear Association
Carlton House
22a St. James's Square
SW1Y 4JH LONDON
UNITED KINGDOM
Fax: +44 207 839 1501
EMail: Wasylyk@world-nuclear.org