

# Topical Issues in Nuclear Installation Safety

## Safety Demonstration of Advanced Water Cooled Nuclear Power Plants

Proceedings of an International Conference  
6–9 June 2017, Vienna, Austria

Vol. 2



**IAEA**

International Atomic Energy Agency

# TOPICAL ISSUES IN NUCLEAR INSTALLATION SAFETY

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

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

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".

PROCEEDINGS SERIES

# TOPICAL ISSUES IN NUCLEAR INSTALLATION SAFETY

## SAFETY DEMONSTRATION OF ADVANCED WATER COOLED NUCLEAR POWER PLANTS

PROCEEDINGS OF AN INTERNATIONAL CONFERENCE  
ORGANIZED BY THE  
INTERNATIONAL ATOMIC ENERGY AGENCY  
AND HELD IN VIENNA, 6–9 JUNE 2017

*In two volumes*

### VOLUME 2

INTERNATIONAL ATOMIC ENERGY AGENCY  
VIENNA, 2018



## **COPYRIGHT NOTICE**

All IAEA scientific and technical publications are protected by the terms of the Universal Copyright Convention as adopted in 1952 (Berne) and as revised in 1972 (Paris). The copyright has since been extended by the World Intellectual Property Organization (Geneva) to include electronic and virtual intellectual property. Permission to use whole or parts of texts contained in IAEA publications in printed or electronic form must be obtained and is usually subject to royalty agreements. Proposals for non-commercial reproductions and translations are welcomed and considered on a case-by-case basis. Enquiries should be addressed to the IAEA Publishing Section at:

Marketing and Sales Unit, Publishing Section  
International Atomic Energy Agency  
Vienna International Centre  
PO Box 100  
1400 Vienna, Austria  
fax: +43 1 26007 22529  
tel.: +43 1 2600 22417  
email: [sales.publications@iaea.org](mailto:sales.publications@iaea.org)  
[www.iaea.org/books](http://www.iaea.org/books)

© IAEA, 2018

Printed by the IAEA in Austria

August 2018

STI/PUB/1829

### **IAEA Library Cataloguing in Publication Data**

Names: International Atomic Energy Agency.

Title: Topical issues in nuclear installation safety / International Atomic Energy Agency.

Description: Vienna : International Atomic Energy Agency, 2018. | Series: Proceedings series (International Atomic Energy Agency), ISSN 0074-1884 | Includes bibliographical references.

Identifiers: IAEAL 18-01171 | ISBN 978-92-0-104618-5 (paperback : alk. paper)

Subjects: LCSH: Nuclear reactors — Safety measures — Congresses. | Nuclear reactors — Design and construction. | Reliability (Engineering)

Classification: UDC 621.039.58 | STI/PUB/1829

## FOREWORD

The IAEA held the International Conference on the Safety of Nuclear Power: Strategy for the Future in Vienna in 1991. Recommendations from this conference prompted actions in subsequent years that advanced the safety of nuclear installations worldwide and included the establishment of the Convention on Nuclear Safety, which entered into force in 1996. In 1998, the IAEA organized the first of a series of international conferences on topical issues in nuclear safety. Subsequent conferences in the series have taken place in Vienna (2001 and 2013), Beijing (2004) and Mumbai (2008). These conferences have contributed significantly to the exchange of information and experience on the latest advances in the field of nuclear installation safety.

The sixth IAEA International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants was held in Vienna, 6–9 June 2017. Its purpose was to foster the exchange of information on the latest approaches, advances and challenges in the demonstration of the safety of nuclear power plants, in particular those using water cooled reactors, including small and medium sized or modular reactors. The conference focused on the safety demonstration of nuclear power plants that have been or soon will be licensed and constructed, which includes, among other aspects, the establishment of, and compliance with, comprehensive and rigorous requirements for siting, design and operation; the demonstration of adequate safety margins against external hazards; and a robust and reliable design to prevent early radioactive releases or radioactive releases large enough to require long term protective measures and actions.

The introduction of passive safety systems, digital instrumentation and a number of innovative safety features in the designs, as well as the inclusion of severe accidents in the design envelope of the new plants, are some of the developments that pose crucial challenges to the safety demonstration and licensing of new reactors. All these aspects are of central interest to design organizations, nuclear regulators, plant operators and technical support organizations in Member States.

More than 300 participants from 48 Member States and 5 international organizations attended the conference, and its programme included 100 paper presentations and 18 posters. There were several side events and two high level plenaries — one on the Vienna Declaration and one on insights gained from the design, construction and commissioning of advanced water cooled reactors. The number of contributions reflects the strong interest in the topic. Of particular relevance was the participants' frank and open exchange of views and experiences that will benefit the further enhancement of nuclear safety. The key insights and recommendations obtained, as summarized by the Conference President, will also shape future work on nuclear installation safety.

This publication, organized in two volumes, provides the executive summary of the conference including the key outcomes and recommendations, together with the papers presented. The IAEA officers responsible for this publication were C. Spitzer of the Division of Nuclear Installation Safety and S. Monti of the Division of Nuclear Power.

## EDITORIAL NOTE

*The contents of this publication have not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the named authors or participants. In addition, the views are not necessarily those of the governments of the nominating Member States or of the nominating organizations.*

*Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.*

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

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

*The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights. Material prepared by authors who are in contractual relation with governments is copyrighted by the IAEA, as publisher; only to the extent permitted by the appropriate national regulations.*

*Any accompanying material has been prepared from the original material as submitted by the authors.*

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

## CONTENTS OF VOLUME 2

### EXECUTIVE SUMMARY

Plenaries.....	2
Side Events.....	7
Topical Areas.....	8

### LICENSING OF ADVANCED REACTOR DESIGNS

#### Licensing Process of Advanced Reactors

Meeting the objectives of the Vienna Declaration on Nuclear Safety: Licensing of New Nuclear Power Plants in Pakistan <i>N. Mughal, F. Mansoor, J. Akhtar</i> .....	17
Lessons Learnt From the UK Generic Design Assessment Process <i>R. Moscrop, J.R. Jones, A. Tehrani, R. Exley</i> .....	22
Lessons Learned From the Preparatory Process for Licensing of the New Nuclear Units in Hungary <i>J. Krutzler</i> .....	27
Russian Regulatory Approach to Evaluation of Passive Systems Used for Specific BDBA's (SBO, Loss of UHS) During Safety Review Of NPP <i>D. Rogatov</i> .....	31

#### Digital I&C Systems

A Method for Evaluating Digital CCF Across an Integrated Plant Design <i>S. Small, I. Poppel</i> .....	41
Development of a Method for the Assessment of Modern I&C System Architectures With Regard to Failure Effects <i>C. Mueller, J. Peschke, E. Piljugin</i> .....	48
Spurious Actuations in Digital Instrumentation and Control Systems - Evaluation Framework <i>I. Garcia</i> .....	59

#### Uncertainty Qualification and Safety Margins

On Some Challenges in Defining and Using Defense In Depth and Safety Margin Concepts, as Highlighted by the Safety Improvement Process <i>D. Serbanescu</i> .....	65
BEPU and Safety Margins in Nuclear Reactor Safety <i>F. D'Auria, H. Glaeser, N. Debrecin</i> .....	70
Assessment of Base-Isolated CAP1400 Nuclear Island Design <i>Y. Jie, L. Shaoping</i> .....	74
A Scheme for Harmonization of Terminology on Safety Margins and Criteria <i>V. Mečíř, J. Macháček, R. Meca</i> .....	79

#### SMR Regulatory Perspectives

Small-sized Reactors of Different Types: Regulatory Framework to be Re-thought? <i>W. Kröger</i> .....	87
---	----

Study on Plume Emergency Planning Zone Determination for CAP200 Small Modular Reactor <i>W. Xuan, L. Liao, D. Sun</i> .....	92
Preparing for Small Modular Reactor Application Reviews: NRC Perspective <i>A. Bradford</i> .....	97

## **IAEA SMR Focused Initiatives**

SMR Regulators' Forum Pilot Project Report <i>S. Magruder, D. Jackson, K. Herviou, M. Devos, S. Cook, P. Dupuy, K. Thomas</i> .....	103
Applicability of IAEA Safety Standard SSR-2/1 to Water-Cooled Small Modular Reactors <i>K. Madden, S. Magruder, H. Subki</i> .....	108
Design Safety Considerations for Water-Cooled Small Modular Reactors - Incorporating Lessons Learned From the Fukushima Daiichi Accident <i>M. Subki, Susyadi, K.B. Park, M.E. Ricotti, C. Zeliang</i> .....	115

## **Contributions to Harmonization of Approaches and Methods by International Forums**

The European Utility Requirements for Advanced Light Water Reactors (EUR): Recent Achievements and New Challenges <i>G. Jacquard, E. Vieilletoile</i> .....	127
Multinational Design Evaluation Programme: 10 Year-Achievements <i>J. Collet, A. Lorin</i> .....	135

## **SAFETY REINFORCEMENT OF EXISTING INSTALLATIONS**

### **National Strategies to Implement International Safety Requirements**

Ensuring Safety Regulation for Sustainable Development of Nuclear Power <i>D. Bhattacharaya, J. Koley, P.R. Krishnamurthy</i> .....	145
Analyses of DEC for NPP's in the Czech Republic Andtheir Implementation into SAR <i>P. Kral, J. Krhounkova, J. Machacek</i> .....	149
Application of the Concept of Defence in Depth to the EPR Reactor Design <i>E. Courtin</i> .....	156

### **Safety Reinforcement of Operating Reactors**

WENRA Approach with Respect to Design Extension of Existing Reactors <i>H. Hirsch, B. Becker, K. Nünighoff</i> .....	165
Safety Principles and Defence-In-Depth Concept Implemented in German Regulations <i>K. Nünighoff, B. Becker, S. Eismar</i> .....	170
Review of the Upgraded Severe Accident Mitigation Strategies for the Generation II PWRS in France Foreseen in the Framework of Plant Life Extension <i>R. Cozeret, C. Debaudringhien, G. Cenerino, E. Raimond</i> .....	178

### **Periodic Safety Review and Assessment**

Recentapproaches Related to Safety Enhancement of Operating NPPs in Korea <i>T. Jin</i> .....	185
--	-----

External Event Level 1 PSA for the WWER440 Type Reactors in Slovakia <i>Z. Kovacs</i> .....	190
Addressing Fire Safety “the Right Way” <i>R. Kalantari, T. Jutras, P. Ouellette</i> .....	196
Updating of a Screening Method for Assessment of Comprehensiveness of Defence in Depth and Areas for its Applications <i>J. Misak</i> .....	202

## **Challenges in Severe Accident Management**

In Vessel Melt Retention Strategy - Status of Work for VVER 1000 Units Applications <i>J. Zdarek</i> .....	215
Enhancing Human Reliability in Severe Accident Mitigation Through Advanced Expert Systems <i>M. Gajdoš, P. Lenhard, R. Lenhard, T. Majerský</i> .....	224
BWROG – Emergency Procedures and Severe Accident Guidelines (EPG/SAG) Revision 4 Highlights <i>B. Williamson, P. Ellison, K. Klass, J. Lyter, T. Matsuo, Toshihiro, D. Roniger, L. Schulze</i> .....	229

## **Progress on Severe Accident Management**

Activities on Safety Improvement of Czech NPPs in Solution of Severe Accident Issues <i>J. Duspiva</i> .....	239
Proposal, Design, Implementation and Safety Demonstration of Severe Accident Management Measures at VVER440 in Slovakia <i>J. Baláž, M. Cvan</i> .....	246
Severe Accident Management at Paks NPP <i>G. Volent</i> .....	251
Lessons From SAMG Exercises for Existing and New Reactors <i>G. Vayssier, B. Lutz</i> .....	255

## **Cross-Cutting Analysis and Perspectives Related to Severe Accident Mitigation**

Developments for Nuclear Power Plant Safety <i>T. Yamamoto, A. Ohnuki, H. Shimizu</i> .....	265
Regulatory Aspects of the Targeted Safety Re-Assessment and the Experience Gained From the Regulatory Oversight of the TSR Related Activities <i>A. Siklosi</i> .....	271
RELAP/SCDAP Sensitivity Study on the Efficiency in Severe Core Degradation Prevention of Depressurization and Water Injection into Steam Generators Following SBO at a CANDU-6 NPP <i>E. Dinca, D. Dupleac</i> .....	275

## **System, Structure and Component (SSC) Modifications to Cope With Severe Accidents**

Safety Enhancement Technology Development with Collaborative International Activity <i>K. Arai, F. Ishibashi</i> .....	283
Bringing Safety Performance of Older Plants on Par with Advanced Reactor Designs <i>A. Viktorov, G. Frappier</i> .....	288
The Nitrogen Injection Threat in PWR Reactors <i>A. Rami</i> .....	292



Contribution of The OECD/NEA Working Group on the Analysis and Management of Accidents  
(WGAMA) in the Severe Accident Field  
*D. Jacquemain, L. Herranz, N. Sandberg*..... 297

# EXECUTIVE SUMMARY

## Outline

Over the years, the IAEA has organized a series of international conferences on topical issues in nuclear installation safety. The conferences have yielded recommendations and led to activities that have served to increase international cooperation and to promote the exchange of vital information to enhance nuclear safety.

The sixth *IAEA International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants* took place in Vienna, Austria, 6 – 9 June 2017.

The purpose of the conference was to foster the exchange of information on the latest approaches, advances and challenges in the demonstration of the safety of nuclear power plants that are planned to be licensed and constructed in the near future, in particular those using water cooled reactors, including small and medium sized or modular reactors. This conference in the series was focused on the safety demonstration of the nuclear power plants (NPPs) that have been and will be licensed and constructed in the near future, which includes, among other aspects, the establishment of, and compliance with, comprehensive and rigorous requirements for siting, design and operation; the demonstration of adequate safety margins against external hazards; and a robust and reliable design to prevent early radioactive releases or radioactive releases large enough to require long term protective measures and actions.

The introduction of passive safety systems, digital instrumentation and a number of innovative safety features in the designs, as well as the inclusion of severe accidents in the design envelope of the new plants, are some of the developments that pose crucial challenges to the safety demonstration and licensing of new reactors.

The conference aimed to provide a platform for the interchange of experiences that can provide valuable insights into how the topics covered by the conference are currently addressed in different countries for various types of stakeholder organizations in Member States. Accordingly, the conference intended to contribute to the harmonization of approaches and methods applied for the safety demonstration of nuclear power plants worldwide.

The conference covered safety assessment of advanced reactor designs, design safety principles, licensing of advanced reactor designs and safety reinforcement of existing installations. The content of the technical programme is summarised in detail below. It was comprised of presentations accompanied by discussions on the four topical areas, several side events and two plenaries - one on the Vienna Declaration and one on Insights gained from Design, Construction and Commissioning of Advanced Water Cooled Reactors.

The high-level plenary titled *Vienna Declaration on Nuclear Safety: Objectives, Challenges and Prospects* featured discussions on how to implement in practice the principles in the 2015 declaration, which aims to strengthen work to prevent accidents with radiological consequences and mitigate such consequences should they occur.

The conference participants' recommendation that the IAEA facilitate the application of the new design safety requirements by Member States would "support the harmonisation of approaches and methods applied to nuclear power plants that are planned to be licensed and constructed in the near future," said Conference President Petteri Tiippana, Director General of the Finnish Radiation and Nuclear Safety Authority.

"We now need Member States' to adopt a bottom-up approach and share their experiences and practical approaches also regarding safety improvements for existing nuclear power plants in the context of the Vienna Declaration," Mr. Tiippana continued.

The conference recommended that IAEA collect both positive and negative regulatory and industry experiences and lessons for nuclear power programmes, including new-build projects, he said adding that participants encouraged the Agency to continue to provide fora for discussions among Member States to strengthen international cooperation and knowledge transfer.

The IAEA Deputy Director General Juan Carlos Lentijo, Head of the Department of Nuclear Safety and Security, emphasized the participants' frank and open-minded exchange of views and experiences benefited the further enhancement of nuclear safety.

"The conference provided valuable insights on challenges and progress related to technical and scientific matters on topics such as innovative design features. It also enhanced the understanding of how to meet new safety requirements, for example the practical elimination of early or large radioactive releases and the need for design for potential core-melt scenarios," he said.

A final synthesis concluded that the wide variety of topics discussed at the Conference demonstrated the broad interest of the global nuclear safety community, and the strong need for discussions such as those held during the Conference.

## Plenaries

### Opening Plenary

The opening plenary, introduced by Ms. Cornelia Spitzer (IAEA) included the opening remark by the IAEA Director General Mr. Y. Amano and the opening statement by Mr. P. Tiippana, Director General of the Finnish Radiation and Nuclear Safety Authority and Conference President.

The speakers welcomed the conference participants and expressed their expectation on fruitful discussions among the large audience on the latest approach and challenges in demonstrating safety at nuclear power plants on topics such as safety assessment and licensing of advanced reactor designs, design safety principles and safety reinforcement of existing installations. The discussions had a particular focus on nuclear power plants using water cooled reactors, including small and medium sized or modular reactors.

Several considerations on the role of nuclear power in the context of increasing safety and minimizing accidents were addressed in the opening statements. A common element which can be highlighted from the opening speeches is the general belief that international collaboration, peer and safety reviews and sharing of operating experience make the nuclear infrastructure stronger as a whole. It was emphasized that the IAEA can contribute to strengthen this collaboration through the development of the IAEA safety standards by integrating current technology and best practices, and providing for their application to achieve a high level of safety.

The IAEA Director General Y. Amano delivered several important messages to the audience at the conference opening remarks as follows:

*“Good morning, Ladies and Gentlemen, Mr. Tiippana, Dear Colleagues,*

*I am pleased to welcome you to the sixth IAEA International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants. This Conference is part of a series on nuclear safety which the IAEA has organized since 1998.*

*Nuclear installation safety is of global importance as nuclear accidents can have effects across borders. This makes licensing and supervision of nuclear power plants a concern not only for operating nations, but also for countries near and far.*

*This Conference provides a platform for discussions on issues such as safety assessment and licensing of advanced reactor designs, design safety principles, and safety reinforcement of existing installations.*

*Nuclear power plants are designed with the goal of minimising the likelihood of accidents and ensuring that – if an accident should occur – its consequences can be mitigated. A comprehensive safety assessment is essential to ensure the protection of workers, the public and the environment.*

*Over the coming days, you will consider the latest advances and challenges in demonstrating the safety of nuclear power plants that are expected to be licensed and built in the near future*

*There will be a particular focus on plants using water cooled reactors, including small and medium sized or modular reactors. Another important topic will be the implications of the Vienna Declaration on Nuclear Safety for operating nuclear power plants.*

*Ladies and Gentlemen,*

*Nuclear power makes a significant contribution to reducing greenhouse gas emissions and improving energy security, while delivering energy in the growing quantities needed for development.*

*Global use of nuclear power continues to grow, despite the Fukushima Daiichi accident in 2011. At present, 30 countries are using nuclear power. About 30 others are considering building their first nuclear power plant, or have started doing so. Most of these possible newcomers are developing nations.*

*IAEA safety standards establish fundamental principles, requirements and recommendations for ensuring nuclear safety. They serve as a global reference for protecting people and the environment.*

*We have revised requirements on safety assessment and design safety, and a revision of associated safety guides is underway.*

*I encourage all countries to make full use of the many services offered by the IAEA in nuclear safety.*

*Our education and training programmes help to strengthen Member States' capacities in nuclear safety, including in design safety.*

*We offer expert peer reviews on topics such as generic and plant-specific designs, national design requirements, safety assessments and periodic safety review programmes.*

*Ladies and Gentlemen,*

*I am pleased to see so many participants here today.*

*We look forward to your insights and recommendations, which will help to shape our future work on nuclear installation safety.*

*I wish you every success with your discussions and I look forward to learning about the outcome.*

*Thank you."*

The Director General of the Finnish Radiation and Nuclear Safety Authority and Conference President Mr. P. Tiippana highlighted some rationale for this conference, and in particular why the safety demonstration of a nuclear installation remains a topical issue for the nuclear safety:

*"Demonstrating nuclear installation safety is no simple task, and it is becoming more and more difficult and challenging due to new technologies and updated safety requirements.*

*We need to make sure safety standards are applied, and to identify both good practices and areas of improvement in conducting safety demonstrations.*

*With the ever-evolving digitalization of almost everything in people's daily lives, the nuclear industry is also considering the use of novel measures to enhance operational performance of nuclear installations.*

*The industry has started exploring the possibility of using big data to enhance the reliability and safety of their nuclear installations. The nuclear community has been very good at collecting data, and if we look into the possibilities and challenges, we might be able to discover nuanced approaches in the engineering and operations of nuclear power plants to make them safer in a way we could not imagine before."*

### **The Vienna Declaration on Nuclear Safety: Objectives, Challenges and Prospects**

The first plenary, chaired by Mr. P. Tiippana, Director General of the Finnish Radiation and Nuclear Safety Authority and Conference President, focused on the objectives, challenges and prospects of the Vienna Declaration on Nuclear Safety (VDNS); moreover, it provided an opportunity to present and discuss open issues, challenges of achieving the objectives of the VDNS and possibly different understanding from technical point of view. The plenary was composed of the following esteemed panellists:

- D. Drabova, Czech Republic;
- J. C. Niel, France;
- A. Kawano, Japan;
- A. Lyubarskiy, Russian Federation;
- M. Johnson, United States of America.

The panellists were requested to provide statements on the following topics:

- Major objectives, challenges and possible shortcomings in the context of the IAEA safety standards as well as national requirements and regulations to implement the principles of the VDNS;
- Possible difference related to the terms "avoiding", "preventing", "practical elimination" used in the VDNS, the IAEA safety standards and/or national regulations; need for further discussion / clarification / harmonisation to better deal with / understand the consequences on the design and operation of different types of nuclear power plants (NPPs);
- Meaning of "early" and "large" releases in practice for the siting, design and operation of the NPPs; establishment of definitions / requirements / regulations in the respective country to meet the objective; consideration of site related factors, such as population distribution, evacuation routes, etc. in the safety assessments;
- Understanding and view of "reasonably practicable" and "achievable" safety improvements in the context of "to be implemented in a timely manner"; meaning in practise, in particular for existing NPPs; interpretation and implementation throughout the lifetime of a NPP, dependence on the life

cycle phase (for instance periodic safety review (PSR) after first ten years of operation vs. subsequent PSR after 20 years etc. or a decision on progressing to long term operation (LTO) phase); practical guidance for what would constitute as timely implementation.

In the subsequent discussion the content of the Vienna Declaration was largely discussed by the panellists and participants elaborating on the clarification of the objectives of the declaration, and the challenges of its implementation.

As general conclusion of this plenary, the panellists and participants agreed that the revised IAEA safety standards well reflect the objectives of the VDNS. Panellists and participants recognized that sharing information is one of the best ways to maintain permanent focus on improving safety. It was recommended that Member States pursue a proactive, bottom up approach in sharing experiences and practical approaches regarding safety improvements for existing NPPs in line with the objectives of the VDNS.

It was noted that similar conclusion was drawn from the Commission on Safety Standards already in 2015 and reiterated at the 7th Review Meeting on the Safety Convention on Nuclear Safety.

Extensive discussions on the concepts of practical elimination and reasonably practicable as well as on the definition of early or large releases were held. The general consensus was that it is important for each Member State to have a process in place to perform a safety assessment and determine if those concepts have been adequately and effectively implemented.

During the discussions the safety improvements to existing nuclear power plants and what is considered sufficient to meet the objectives of the VDNS were identified as a main challenge related to the backfitting of nuclear power plants in operation.

A number of Member States requested further support and assistance from the IAEA in implementing the latest design safety requirements at nuclear power plants in operation.

### **Insights Gained from Design, Construction and Commissioning of Advanced Water Cooled Reactors**

Newcomer countries and countries with established nuclear programmes are currently engaging in a number of construction projects at various stages of completion globally. These projects have encountered a diverse range of challenges, including difficulties in keeping first-of-a-kind (FOAK) realization on budget and on schedule. As such, the second plenary, chaired by Mr. A. Bychkov, Russian Federation, focused on sharing insights from the design, manufacturing, construction and commissioning of advanced water cooled reactors. The plenary was composed of the following esteemed panellists:

- M. Zheng, China;
- T. E. Jin, Korea, Republic of;
- A. Kiryukhin, Russian Federation;
- A. Bradford, United States of America;
- G. Rzentkowski, International Atomic Energy Agency;
- P. Vincze, International Atomic Energy Agency.

The plenary was intended to present specific cases of design, manufacturing, construction and commissioning of advanced water-cooled reactors, as well as to share international experience. Each of the panellists provided short presentations focused on the following topics:

- Impact of design change and/or design finalization during construction;
- Challenges related to a suitable supply chain;
- Construction and commissioning management and related risks;
- Modern construction technologies and methods: advancements vs challenges;
- Good practices and lessons learned to overcome challenges during design, construction and commissioning of advanced NPPs.

The panellists noted that while challenges exist, they are well identified, and as such, vendors, engineering, procurement and construction (EPC) companies, operators and regulators are aware of the focal areas of contention and have found effective ways to manage these challenges accordingly. Throughout the discussion, the importance of a stable and well established regulatory framework to succeed in the completion of a nuclear project was stressed. The discussion focused on the following main challenges:

- *Complexity of designs:* A mature technology should pursue simplification rather than an increasing number of systems, sub-systems and components;

- *Supply chain:* Reliable and well qualified supply chain and appropriate oversight is a must;
- *Design changes during construction:* Sometimes managed by means of licensing amendments. This suggests the need to well define the technical specifications of the plant and finalize the design prior to starting construction;
- *Complexity of the construction phase:* Integration of thousands of people from hundreds of organizations with different organizational culture;
- Some challenges have arisen from peculiar features/advantages of the advanced water cooled reactor technology like modularization and the adoption of passive safety systems.

### **Keynote – ETSON: Its Role and Activities for Harmonising Safety Assessment**

The Keynote, delivered by Mr. B. De Boeck, ETSON, and chaired by Mr U. Stoll, Germany, provided the participants with the opportunity to receive information on the background, role and main activities of the European Technical Safety Organisations Network (ETSON). Among the objectives defined for their future activities, ETSON aims at strengthening links with the IAEA, in particular in the Technical and Scientific Support Organizations (TSOs) Forum and the TSOs conference, as well as their participation in the development and revision of IAEA safety standards through their member organisations in Member States.

The need for independence between the nuclear power plant design developer and the reviewer of the safety demonstration in relation to the key role of the TSOs in this field was emphasized. Participants also stressed that expertise in safety assessment for newcomer countries is necessary and therefore encouraged new comer countries to establish relationships with competent and well experienced external organizations, to develop and implement education programmes and training courses in the early phase of a new nuclear power programme in order to build capacity for performing all the activities necessary to ensure safety in licensing, construction and operation.

### **Closing Plenary**

The closing plenary was comprised of a closing remark by the IAEA Deputy Director General of the Department of Nuclear Safety and Security J. C. Lentijo and the closing statement by Mr. P. Tiippana, Director General of the Finnish Radiation and Nuclear Safety Authority and Conference President.

In his closing remarks, the President of the Conference focused on the key outputs and recommendations. Mr. Tiippana highlighted that international collaboration, peer and safety reviews and sharing of operating experience remain essential elements to improve the nuclear safety of the installations; and he emphasized the need for international collaboration specifically as it relates to new designs and new build projects. Sharing is valuable for all the stakeholders and can make the industry stronger as a whole. The President of the Conference also reminded that the IAEA technical safety review services contribute to the enhancement of nuclear safety by providing an independent review on different subject areas; he encouraged Member States to further explore and utilize these services in a systematic approach.

The key outputs delivered during the conference summary are as follows:

- A Common approach is needed to assess the reliability of safety systems relying on passive concepts;
- Fora for discussion on approaches to demonstrate safety in core melt scenarios are recommended;
- The development and verification of safety demonstration tools represent a priority for Member States;
- The use of a quality Probabilistic Safety Assessment (PSA) is recommended to enhance safety;
- Further guidance is needed to address the concept of “practical elimination” and its demonstration;
- The importance of assessing the implementation of defence-in-depth in design is highlighted;
- The Review of the applicability of the IAEA safety standards to SMR designs is requested;
- Internationally accepted methods to evaluate new design features are desired;
- Consideration for multi-unit interactions are recommended (e.g. SMRs, but not limited to).
- The sharing of experiences in the licensing of passive systems is recommended;
- Further improvements to severe accident management programmes are recommended;
- The sharing of experiences with backfitting measures implemented at nuclear power plants in operation to meet the objective of the Vienna Declaration on Nuclear Safety to the extent practicable is recommended;



- Further clarification on the terminology of the VDNS is desired.

The conference recommendations highlighted by the Conference President are summarised as follows:

- Member States should share experiences and practical approaches (e.g. related to the VDNS and the evaluation of new design features) and the IAEA should provide fora to strengthen international cooperation and knowledge transfer;
- The IAEA should facilitate the application of new design safety principles, also related to small and medium sized or modular reactors (SMRs);
- IAEA should collect regulatory and industry experience and lessons, positive and negative ones (e.g. New build Projects);
- The IAEA should continue to support the harmonization, verification and validation and common approaches.

The closing remark by Deputy Director General Lentijo remarked on the impressive participation at the conference and the excellent quality of the scientific contributions. Closing his speech, gratitude was expressed in particular to the Conference Secretariat, who provided advice on the scope, overall objectives, structure of the conference and to the Scientific Organizing Committee, who set up the detailed conference programme, identified key speakers, and last but not least, selected and peer reviewed over 100 scientific contributions. The joint efforts of the chairpersons, the Scientific Organizing Committee and the Conference Secretariat were fundamental in making the conference a success.

The IAEA Deputy Director General of the Department of Nuclear Safety and Security J. C. Lentijo closing remarks are as follows:

*Good afternoon, ladies and gentlemen. On behalf of the IAEA Director General, I thank you for your participation in this sixth IAEA International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants. I am glad that more than 300 participants from 48 Member States and 5 International Organisations are here.*

*The conference has been intense, with 100 papers and 18 posters presented. There were several side events and two high-level plenaries - one on the Vienna Declaration and one on Insights gained from Design, Construction and Commissioning of Advanced Water Cooled Reactors. This packed programme reflects the strong interest in the topic.*

*The Conference covered topics, ranging from new reactor projects to nuclear power plants in operation addressing safety assessment and licensing of advanced reactor designs, design safety principles, and safety reinforcement of existing installations. We had fruitful, open and beneficial discussions on the experiences and challenges of demonstrating the safety of nuclear power plants that are planned to be licensed and constructed in the near future, in particular those using water cooled reactors, including small and medium sized or modular reactors.*

*Valuable insights were obtained for both, challenges and advances from technological and scientific point of view, and on the application of the new safety requirements.*

*The Conference also featured a useful discussion of the implications of the Vienna Declaration on nuclear safety for nuclear power plants in operation.*

*This wide variety of topics demonstrates the broad interests of the global nuclear safety community. The Director General in his opening remarks emphasised the global importance of nuclear installation safety along with the IAEA Safety Standards and review services available to the Member States. I invite you to take advantage of these services.*

*We welcome the interest in the Agency's safety standards in the area of safety assessment and design safety, and particularly in their ongoing revision as well as the development of supporting technical documentation. I encourage all countries to participate in these activities.*

*The key insights and recommendations obtained, as just outlined by the Conference President, will enable us to shape our future work on nuclear installation safety. We will focus on facilitating the application of the new safety requirements by building on the practical experiences from Member States in order to support the harmonisation of approaches and methods. We will also continue to provide fora for technical and scientific exchanges among Member States to strengthening international cooperation and knowledge transfer. As always, the Secretariat stands ready to assist the Member States in working to address their challenges.*

*My department – the IAEA Department of Nuclear Safety and Security - cooperated with the IAEA Department of Nuclear Energy to prepare this Conference. I recognize the instrumental role of the Scientific Secretaries: Ms. Cornelia Spitzer and Mr Stefano Monti. Ms. Julie Zellinger of Conference Services support was essential in organizing the Conference. Special thanks go at first to the President of*

*the Conference, Mr. Tiippana, as well as to the members of the Scientific Organising Committee and to all the panellist, speakers, chairpersons and poster presenters for your effort. Thanks to you, this Conference was very successful.*

*Thank you for taking part in this Conference. I wish you a safe and pleasant journey home or wherever your travels may take you.*

*I hereby declare the Conference closed.*

## **Side Events**

### **Workshop on Technical Safety Review Services**

The workshop was intended to share experiences from both the IAEA and Member States representatives about the Technical Safety Review (TSR) services. The IAEA presentation summarized the scope, intent and current status of the TSR services and was followed by presentations and discussion with each panellist. There was a consensus view amongst the panellists that the TSR services benefit Member States by providing tailored, independent evaluation of the safety assessment and design safety documentation and making recommendations for enhancements and improvements to nuclear safety. TSR services encompass six subject areas including design safety, generic reactor safety, safety requirements, probabilistic safety assessments, accident management and periodic safety reviews. The significance of these services was reinforced by the fact that they are based on IAEA safety standards which represent an international consensus view on an appropriate level of safety. Several panellists also emphasized that the benefit comes not just from the review itself, but from the review preparations and work undertaken to address observations and recommendations.

Questions from the audience primarily focused on the scope and documentation required for the TSR services. Both the panellists and the IAEA staff reinforced that the TSR service does not constitute any kind of design certification or licensing activity as this is not a function of the IAEA; rather, it is the responsibility of the Member States. It was pointed out that the TSR services are primarily intended to improve the quality of the documentation being considered by providing recommendations in areas where supplementing information or modifications are needed to adhere to the IAEA safety standards. An example of this discussion focused on the TSR review of design safety documentation. This TSR services does not constitute a review of the design itself, but, rather, a review of the quality of how the documentation demonstrates that the design adheres to the IAEA safety requirements which are utilized as the review criteria.

Clarification regarding the role of the IAEA safety guides and the involvement of design organizations was discussed for inclusion in the TSR Services Guideline document that is currently under preparation. In response to this discussion, the IAEA will circulate the draft TSR Services Guideline document for comments prior to finalising and publishing. Several panellists also encouraged Member States to request a TSR service to partake in the benefits such recommendations and observations provide.

### **Workshop on an Introduction and Further Explanation on Design Extension Conditions**

The workshop introduced and discussed the application of design extension conditions (DECs) as described in IAEA Safety Standard SSR-2/1, Nuclear Power Plants: Design. During the discussion, Member States presented their approach for implementing DEC into their safety requirements. Consensus was found in regards to categorizing accident conditions caused by multiple failures or those exceeding capability of the safety systems as DECs. Member States agreed that designing dedicated safety features for DEC with less conservatism was acceptable provided justification of sufficient margin to cover uncertainties and avoid cliff edge effects exist.

Further engagement on the effectiveness of provisions credited in the safety analysis of DEC was discussed and it was determined that this may be demonstrated by the application of rules that are less penalizing than those applied to design basis accident (DBA) analyses. Further discussion concluded that a comprehensive safety demonstration of the DEC analyses must be included in the safety analysis report (SAR) regardless of whether or not the consequences are mitigated by the operation of safety systems unaffected by the DEC sequence.

To conclude, it was determined that most of the DEC without significant fuel damage are dependent on the reactor technology and design. As such, a systematic and comprehensive approach should be implemented and documented to justify the postulated DECs for the design of a nuclear power plant with the objective to reinforce

the plant capabilities to prevent accident with core melting and to meet the total core damage frequency target with a reliable confidence.

### **Roundtable on SMR Deployment: Technical, Construction and Licensing Challenges**

A roundtable was held to discuss the technical, construction and licensing challenges facing the deployment of SMRs. The IAEA provided a short presentation to introduce small modular reactor (SMR) technology and provide a comprehensive overview of the designs being pursued and Member State involvement. Following which, each of the five panellists provided an overview of their countries SMR programme, including those in the Russian Federation, United Kingdom, United States of America, People's Republic of China, France and Switzerland.

The panellists discussed the challenges and opportunities SMRs face as a first-of-a-kind technology. One such challenge lies in the manufacturing of SMRs, as SMRs tend to shift the terrain from on-site stick-built to factory built nuclear power plants. The importance of economies of scale was also discussed given the reduced power output of SMRs and the optimization of passive safety systems results in lower maintenance and staffing costs.

Challenges and opportunities facing the regulatory scope specifically related to the use of non-conventional reactor types, like modular high temperature gas and molten salt reactors, were largely. For instance, uncertainty associated with accident progression and their types was emphasized. An opportunity to streamline the harmonization of safety standards was recognized taking into account that the design safety requirements established for the nuclear power plants will need to be adapted to consider specificities of SMR designs. The need to harmonize design safety requirements on an international scale to improve economic viability was also highlighted as challenge but considered by the participants as highly desirable. The participants agreed that SMRs could be designed so that the implementation of protective actions for the people and the environment would not be necessary in accident conditions. The panel also discussed the importance of assisting newcomer countries through IAEA services and partnerships with developed nuclear power plant programmes.

Many SMR designs are proposed to be used for applications other than electricity generation like desalination, district heating, etc. As such, the need to understand and minimize the possibility of cascading effects during accidents for multi-unit plants and those in close proximity to chemical plants were discussed. As was the need to investigate the introduction of non-radioactive hazards, such as chemical and biological hazards that these applications and innovative designs may present.

In regards to floating reactors, it was emphasized by the panellists that proven reactor designs will be utilized. However, it was stated that much emphasis needs to be placed of resolving legal aspects related to transporting a reactor in international and domestic waters and the liability associated with doing so. Further accident analysis must also be considered as it relates to capsizing, terrorist attacks, etc.

## **Topical Areas**

### **Safety Assessment of Advanced Reactor Designs**

A wide range of aspects was covered by the papers presented, including atmospheric dispersion of radioactive materials, dynamic assessment of facilities' contamination and failure in accidental conditions, single-phase direct numerical simulation, reactor pressure vessel (RPV) neutron fluence assessment and severe accident sequences analysis. Relevant efforts are being made in advanced modelling of physical phenomena focused on closing the gaps introduced by the unavailability of modelling tools, such as those related to atmospheric dispersion of radionuclides and dynamic probabilistic safety assessment (PSA). Evidence related to international efforts to enhance codes, such as those for multiscale simulation and safety demonstration of advanced water-cooled reactors, was provided. Relevant activities are being implemented at the experimental level to provide new sets of data for severe accident codes benchmarking. The IAEA's role in contributing to identification of mechanisms for facilitating the selection and sharing of good quality data for code validation (most of them protected by proprietary rights) was emphasized. Data for severe accident analysis was one of the specific aspects highlighted, which included both plant data (e.g. Fukushima Daiichi NPP) and data from experimental installations. Relevance of the need to further develop full parallel deterministic transport codes was also

specifically identified. In summary, continuing development and corresponding verification of safety demonstration tools was considered as still needed.

Safety systems relying on passive phenomena to accomplish their safety functions are being introduced with innovative design safety features, and thus, there is a high interest from Member States to develop methods to evaluate the reliability of these passive systems. During the discussions, the critical role passive systems play in ensuring nuclear safety, especially in advanced reactor designs, was noted and the need for thorough assessment of passive systems reliability was highlighted. In spite of the potential advantages of passive systems, they imply several challenges in the demonstration of their reliability. In particular, evaluation of passive systems performance could challenge computer codes by phenomena that could be beyond their validation domain; therefore, the need for validating the computer codes against phenomena involved in passive systems was underlined. It was specifically noted that the validation of computer codes needs to be done on the basis of both separate effect tests and integral effect tests considering any scaling effects. Another challenge that caused concerns among participants is related to the interactions between passive systems and necessity of their investigation. It was concluded that integral experimental facilities including different types of passive systems are required for proper investigation of interactions between passive systems. Several sessions of the conference touched upon this issue and eventually the conclusion made was that there is a need for a common approach to assess the reliability of passive systems. The participants further agreed that the use of innovative technology and components should necessitate specific qualification tests and analyses to demonstrate efficacy and reliability of those components and systems.

Another topic that raised a large interest among various Member States representatives was the in-vessel melt retention (IVMR) strategy. In general, it was noted that the robust safety demonstration of effectiveness of IVMR strategy should include margins and consider a large spectrum of influencing factors and account for uncertainties (especially for high power reactors). During the discussions, it was revealed that in addition to the national, regional and international programmes that are underway to reduce the uncertainties related in particular to IVMR, there is a need for a sound technical basis to support a robust safety demonstration of corium stabilization and cooling in case of an accident with core melting. The IAEA is supporting this effort by providing platforms for discussion and fostering information sharing and dissemination.

The safety assessment of SMRs was discussed in regards to the need to develop an understanding of how to demonstrate the safety of these designs, and moreover, how to determine an appropriate level of uncertainty where unproven methods are utilized. The need to develop validation codes for modelling was discussed in great detail. Third party validation and international collaboration was deemed vital to ensuring a high level of effectiveness in this regard. Further understanding and development regarding design basis accident and severe accident management were discussed, as well as the possibility to investigate decreasing the required emergency planning zone size.

A deterministic approach supplemented by probabilistic insights and feedback from operation remains a good practice widely used for the identification of postulated initiating events (PIEs). The safety demonstration proving the compliance of the design with the regulatory requirements is performed on the basis of a set of deterministic analyses and PSAs, they represent complementary means to provide a comprehensive view of the overall safety of the plant.

Several papers and associated intensive discussions were specifically devoted to the use of PSA to support the design process of advanced NPPs. It was noted that the approaches for PSA modelling have grown and changed in parallel with the evolution of NPP designs; however, the direction of PSA applications has not changed significantly. While the main technological solutions are provided based on the deterministic considerations, the PSA is mainly used to balance the design, reveal hidden vulnerabilities, optimize and justify Limiting Conditions for Operation (LCOs), verify compliance with system reliability targets and other applications. In general, it was mentioned that enhanced designs have been achieved by continuous consultations between design and system engineers and PSA teams, concluding that the use of PSA in design is a highly interactive process.

In the meantime, participants highlighted the critical importance of the quality of the PSA models used in the process of plant design and operation. It was specifically noted that current PSA models have to deal with new modelling challenges such as modelling of passive systems, the assessment of reliability of passive systems and digital I&C systems and others. In addition, it was underlined that high quality PSAs are achievable only through the comprehensive and independent review process. In this context, Member States were recommended to request

the IAEA Technical Safety Review – Probabilistic Safety Assessment (TSR-PSA) service in order to receive independent PSA review based on the IAEA safety standards.

The need for consideration of multi-unit interactions in safety assessment, both by probabilistic and deterministic means, was specifically highlighted.

### **Design Safety Principles**

The identification of design extension conditions (DEC), rules and criteria used in the design of safety features for DEC was addressed and discussed in several presentations. The presentations showed that the identification and assessment of DEC differ from one country to another for the same basic design.

Uncertainty and safety margin evaluation including cliff edge effects were discussed in terms of their better and common understanding and definitions with the aim of soundly including them in the best-estimate plus uncertainty analysis also recommended by the IAEA. Although this topic was discussed for power reactors, it also applies to SMRs.

The interpretation and demonstration of practical elimination of large or early releases was addressed in a specific session of the conference and the presentations led to intensive discussions. The origins of the concept and its evolution were highlighted in the presentations. The concept of practical elimination could be considered as a relevant part of the application of defence-in-depth principle in order to ensure that the likelihood of accident conditions that could lead to early or large radioactive releases is extremely low. There is a need to develop further clarification in the practical application of the concept and demonstrating for the different cases the effectiveness of the safety provisions for meeting the objective of practical elimination with a high level of confidence.

Nevertheless, the participants agreed that appropriate engineering provisions and guidance should be required to be implemented to mitigate the consequences of severe accident scenarios which might still occur due to unexpected further failures.

Related to the implementation of defence-in-depth, also specific aspects such as the safety classification or equipment qualification for equipment required for different plant states, their diversity and independence were addressed. The discussion showed that the issue is more on the application of the defence-in-depth concept rather than on harmonization of requirements and/or recommendations. Further clarification of current practices for new builds as well as nuclear power plants in operation was regarded useful.

Enhancement of defence-in-depth at operating nuclear power plants is usually investigated considering the feasibility of the installation of new systems and components for mitigating the consequences of accidents with core melting, and to improve the independence between the systems designed for different plant states. Regarding the mitigation of accidents with core melting, a majority of the safety improvements already implemented or planned aim at preventing dispersion of the molten fuel caused by the rupture of the reactor vessel at high pressure, and at ensuring the corium debris retention inside the reactor vessel by the implementation of an adequate ex vessel cooling system. In some Member States, an ex-vessel retention strategy is envisaged. Recognizing that full independence of the different levels of defence-in-depth is not practically achievable raises the question to what extent independence between the levels of defence is achievable. A comprehensive analysis to determine weaknesses in the implementation of defence-in-depth is largely regarded to be necessary.

The application of design principles is also linked to requirements developed internationally or by regulatory bodies. In this context, the IAEA safety standards, the new revision of the European Utility Requirements (EUR) and applicable regulations in some countries such as France, China, Finland or the UK were considered. A specific session was dedicated to the challenges in the implementation of design safety principles due to different regulatory frameworks.

High level nuclear safety objectives have reached a certain level of harmonization and are comparable between countries but some safety principles and aspects are not evaluated with the same criteria between countries having the same overall safety requirements. Therefore, the organization of exchanges between regulatory bodies and nuclear industry sector actors was recommended to get a better mutual understanding of the rationale for their application. Efforts of harmonization between countries need to be carried on for the benefit of consistency between country regulatory requirements, the predictability of the licensing of a reactor design, and the cost to completion for new nuclear projects.

## **Licensing of Advanced Reactor Designs**

In regards to meeting the objectives of the Vienna Declaration on Nuclear Safety a majority of the Contracting Parties had reported at the 7th Review Meeting on Convention on Nuclear safety that the objectives of the Declaration were included in the latest revision of their regulatory requirements.

Issues related to consideration of vendor country regulations, safety requirements relevant to passive safety features, legal implications of the generic design assessment process, approaches to respond to the Vienna Declaration, independent verification of a safety case, design extension conditions applied to the spent fuel pool were addressed.

The participants recognized that the safety objectives and the high level regulatory requirements reflected in the national regulations are often identical or similar, but the guidelines published by regulatory bodies may differ in the application or safety demonstration. For the industry, efforts of harmonization between countries are desirable for the benefit of consistency between country regulatory requirements, the predictability of the licensing of a reactor design, and the costs to completion for new nuclear projects.

Harmonization of technical specifications for advanced light water reactors is very important for all stakeholders. For example, the EUR includes 4500 requirements that cover many aspects such as safety, performance, and competitiveness, and can be used by the utilities for design assessment and technical reference in call for bids.

From all sides, the importance of harmonization of codes and standards was emphasized because it has impacts on the time of the project, costs, supplies of equipment and safety. There is a need to harmonize regulatory requirements (e.g., within the Multinational Design Evaluation Programme (MDEP)) and industrial standards and codes as well. The differences are being analysed and harmonisation aims at either convergence (same or similar requirements) or reconciliation (differences are accepted but justified), as designs are associated to codes and some vendors cannot always adapt to different codes.

Digital instrumentation and control (I&C) remains an important topic of discussion. It was concluded that there is a need for developing an internationally recognized method to evaluate common cause failures in digital I&C control and protection systems and support systems including emergency diesel generator using embedded digital devices that will be fundamentally structured around the defence-in-depth concept.

There are more than fifty SMR designs under various stages of development comprising a broad spectrum of reactor technologies; each having its own advantages and disadvantages. Selecting the appropriate SMR design depends on the intended application and timeline for deployment. Standardization and/or harmonization of safety standards and international collaboration are very desirable and most countries pursuing SMRs are already engaged internationally in this discussion. There is a strong interest in the industry in trying to harmonize safety and licensing requirements for SMRs because much of the plant will be built in a factory and standardization is important. According to the discussion, emergency planning zones (EPZ) for SMRs should be revisited and refined to account for advantages in SMR designs. Moreover, multi-modular issues need to be researched further to account for multiple failures or possible mass failures' effects on all units/modules.

The interests and statuses of the development of SMRs in Member States were discussed during the roundtable. In China, the national safety authority has issued a guide for an SMR review plan and started the preparation of design requirements; in the Russian Federation, three SMRs are being licensed. In other Member States, there is no real development work but there is a clear interest in international cooperation. Economics in a competitive market seem to be the most important hurdle, in a context where now-a-days renewable energies are highly subsidized. In addition, first-of-a-kind issues could be important regardless of the technology of the SMRs.

## **Safety Reinforcement of Existing Installations**

The Vienna Declaration on Nuclear Safety (VDNS) stresses the importance of improving the nuclear safety of nuclear power plants in operation in order to prevent long term off-site contamination should an accident occur. It was recognized that implementing the VDNS will influence the nature of the provisions to be implemented and the priorities for their implementation. Additionally, the EU Nuclear Safety Directive and the reference levels established by the Western European Nuclear Regulators' Association (WENRA) must also be considered by the EU Members.

The practical implementation of the VDNS at existing nuclear power plants is still a challenge for the operating organisations and a clarification of the terminology is highly desirable.



Maintaining a high level of nuclear safety at nuclear power plants in operation throughout their entire lifetime is required by the national regulations, but meeting this requirement remains a challenge to operating organization resources beyond the obligation of performing periodic testing, inspection and maintenance. Considering Member States' practices different means to identify, design and implement safety improvements have been reported. The majority of the participants recognized that the stress tests or the safety re-assessments and the peer reviews required by the regulatory bodies and implemented in the light of the Fukushima Daiichi accident have largely identified safety improvements already implemented or that are in the process of being implemented. However, as the regulatory framework is not the same in all Member States, the self-assessments completed by Member States in the light of the Fukushima Daiichi accident have revealed differences in the objectives, priorities and implementation schedule for safety improvements due to different regulatory approaches. Other means of identifying safety improvements were discussed among them license renewal, authorizations for continued operation or the use of operating experience.

The presentations outlined a set of technology independent common areas where the operating organisations have planned or already implemented some modifications aimed at improving nuclear safety including:

- Reinforcement of the defence-in-depth concept by strengthening the independence among the systems and components designed to mitigate different plant states;
- Definition of strategies to mitigate the consequences of accidents with core melting and development of the associated severe accident management guidelines (SAMG);
- Introduction of safety features to cope with potential failures of the safety systems;
- Prevention and limitation of the effects of the external and internal hazards.

The discussions highlighted some difficulties in the application of the latest design safety requirements primarily established for new builds to operating nuclear power plants and recommended to share experiences with backfitting measures implemented at nuclear power plants in operation to meet the objective of the Vienna Declaration on Nuclear Safety to the extent practicable.

All participants agreed that sharing approaches, practices and design solutions at an international level as well as dissemination of research and development (R&D) achievements contribute to saving time and resources in the identification and implementation of the safety improvements. IAEA conferences and technical meetings, the World Association of Nuclear Operators (WANO) inspections and owner group events provide good opportunities for cooperation and sharing of good and best practices and lessons learned.

The effective implementation of severe accident management guidance remains a priority for operating reactors. Severe accident management has been strengthened following the Fukushima Daiichi nuclear power accident and most operating nuclear power plants have completed or have planned to complete the process of implementing these improvements. Questions remain regarding the proper usage and control of portable equipment which is used during accident management and the appropriate level of regulatory oversight.

Multiple failures are widely recognized as the major contributing factor to accidents with core melting. For nuclear power plants in operation a strategy widely applied to reinforce prevention of core melting relies on the installation of additional equipment in case of failure of the systems designed to respond to in such an event. Another issue discussed was that site hazards have to be considered on the basis of their causation and likelihood including a realistic set of combinations of natural hazards when natural causes for their combination exist.

The role of the off-site support services was discussed in the context of the accident management in conditions not initially considered by the design of the nuclear power plant and in the event of natural hazards of a magnitude higher than the one considered for the design of the structures and components. The participants discussed that the use of non-permanent equipment should be investigated with due account taken of the coping time available before unacceptable consequences occur.

## **LICENSING OF ADVANCED REACTOR DESIGNS**





# LICENSING PROCESS OF ADVANCED REACTORS

**Chairperson**

**A. JULIN**  
Finland





## MEETING THE OBJECTIVES OF THE VIENNADECLARATION ON NUCLEAR SAFETY: LICENSING OF NEW NUCLEAR POWER PLANTS IN PAKISTAN

N. MUGHAL  
Pakistan Nuclear Regulatory Authority (PNRA)  
Islamabad, Pakistan  
Email: nasir.mughal@pnra.org

F. MANSOOR, J. AKHTAR  
Pakistan Nuclear Regulatory Authority (PNRA)  
Islamabad, Pakistan

### Abstract

In the aftermath of Fukushima Daiichi Nuclear Power Plants accident, nuclear think tanks sat together to draw lessons learnt and to devise new requirements to be incorporated in the standards to minimize the possibility of re-occurrence of such accidents and to reduce the consequences of such events in future. International fora encouraged policy makers and think tanks to evaluate the existing domains of regulatory regime as well as the prevailing designs of Nuclear Power Plants (NPPs) for ensuring protection of the public and environment; enhancing accident mitigation; strengthening emergency preparedness and improving regulatory performance. In light of Fukushima event, member states not only conducted different analysis (also named as stress tests) to demonstrate the adequacy of existing plants but also re-visited the regulatory framework and the governing processes to identify any area for further enhancement. In unanimity, 'Vienna Declaration on Nuclear Safety' has been endorsed by all the contracting parties of 'CNS' which highlighted the key principles to be considered by the nuclear world. The paper will focus on the areas considered during the licensing of two new design NPPs (Karachi Nuclear Power Plant Unit-2 (K-2) and Unit-3 (K-3)) as a consequence of the 'Vienna Declaration', the new aspects that have been considered in the regulatory processes to conform to the 'Vienna Declaration' and the process followed during the licensing of the new nuclear reactors.

### 1. VIENNA DECLARATION ON NUCLEAR SAFETY

The Vienna Declaration on Nuclear Safety (VDNS) [1] was issued as a result of the diplomatic conference on Convention on Nuclear Safety (CNS) held in February 2015, which indicated to the international community the concerns and efforts of all Contracting Parties to improve nuclear safety. The Vienna Declaration on Nuclear Safety requires all the Contracting Parties to act for implementation of the principles of VDNS to prevent accidents with radiological consequences and to mitigate consequences should these occur. The main obligations of the VDNS can be summarized as:

- a) According to principle-1 of VDNS; new NPPs are to be designed, sited, and constructed, consistent with the objective of preventing accidents in the commissioning and operation and, mitigating possible releases of radionuclides causing long-term off site consequences. Should an accident occur, the large and early radioactive releases, which require long-term protective measures and actions, are required to be practically eliminated.
- b) The principle-2 of VDNS requires the Contracting Parties to carry out comprehensive and systematic safety assessments periodically and regularly for existing nuclear installations throughout their lifetime in order to identify safety improvements.
- c) The principle-3 of VDNS requires the national regulations to take into account the relevant IAEA Safety Standards and other international practices and experience.
- d) Pakistan, along with other Contracting Parties, agreed to uphold and implement the Vienna Declaration. Pakistan took a series of actions to implement the objectives of the Vienna Declaration on Nuclear Safety [2].



## 2. SAFETY IMPROVEMENT AT NPPS OF PAKISTAN THROUGH DIRECTIVE AFTER FUKUSHIMA ACCIDENT

As a matter of principle, PNRA issued directive to its licensee and applicant, which intuitively provided the legal basis to carryout regulatory oversight of existing and future NPPs beyond the scope/requirements delineated in the existing regulatory framework. PNRA required the applicant that lessons learnt from Fukushima accident should be an integral part of design for new NPPs rather than incorporating them as back fitting measures. This directive was the need of the day as revision of regulations /regulatory framework is a lengthy process which takes time.

## 3. LICENSING PROCESS

PNRA has a well-defined regulatory framework which ensures comprehensive safety assessment and verification before the commencement of operation of nuclear installations. PNRA Regulations PAK/909 [3] prescribe a mechanism for licensing of nuclear installations according to which authorizations are granted for following stages which are in accordance with IAEA SSG-12:

- a) Site Registration
- b) Construction License
- c) Permission for Commissioning
- d) Permission to Introduce Nuclear Material into the Facility
- e) Operating License
- f) Revalidation of Operating License
- g) Licensing Beyond Design Life
- h) Authorization for Decommissioning/Closure
- i) Removal from Regulatory Control

PNRA Regulations PAK/910 [4] prescribes detailed site assessment requirements for site registration. PNRA Regulations PAK/911 [5] require that at the design stage of a nuclear installation, a comprehensive safety analysis shall be carried out to identify all sources of exposure and to evaluate radiation doses which could be received by workers and the public, as well as potential effects on the environment. The safety analysis shall take following into consideration:

- 1) All planned normal operation modes of the plant
- 2) Plant performance in anticipated operational occurrences
- 3) Design Basis Accidents
- 4) Event sequences that may lead to a severe accident

Thorough assessment of the above mentioned safety analysis, robustness of the engineering design to withstand postulated initiating events and accidents are established, effectiveness of safety systems and safety related items or systems is demonstrated, and requirements for emergency response are established. Regulations PAK/911 [5] require that measures should be taken to ensure that radiological consequences are mitigated. Such measures include: engineered safety features; onsite accident management procedures established by the operating organization; and on-site and off-site emergency planning and preparedness measures to mitigate radiation exposure if an accident occurs. A safety analysis of the plant needs to be conducted in which methods of both deterministic and probabilistic analyses are applied. These analyses establish and confirm the design basis for items important to safety. In addition, the safety analysis also included the demonstration of the adequacy of additional systems which were provided to cope with events beyond the design bases including severe accidents. Applicant is required to demonstrate that the plant as designed is capable of meeting prescribed limits for radioactive releases and acceptable limits for potential radiation doses for each category of plant states. The safety assessment is based on the results derived from the safety analysis, operating experience, results of supporting research and proven engineering practices. The applicant needs to ensure that an independent verification of the safety assessment is performed before the design is submitted for regulatory review and approval.

#### 4. REGULATORY REQUIREMENTS RELATED TO SITE REGISTRATION

Requirements for site registration/siting of a nuclear power plant are provided in Regulations PAK/910 [4] which is mainly based on IAEA Safety Standards No. NS-R-3 titled Site Evaluation for Nuclear Installations and USNRC 10 CFR Part 100. Before site registration, the applicant has to obtain approval from the Environmental Protection Agency. Subsequently, a Site Evaluation Report (SER) is submitted to PNRA for site registration in order to ensure that the plant complies with the national laws and regulations regarding environment protection, land and water use, marine life, etc. In the evaluation of suitability of a site for a nuclear installation, various aspects are considered such as external events (natural origin or human induced), characteristics of the site and its environment that could influence the transfer to persons and the environment of radioactive material to be released, population density, population distribution and other characteristics of the external zone, as they may affect the possibility of implementing emergency measures and the need to evaluate the risks to individuals and the population.

Regulations PAK/910 [4] are currently under consideration for revision to incorporate requirements for periodic re-evaluation and re-assessment of all hazards (natural or man-made) in line with the current revision of IAEA safety requirements on siting and the principles of the Vienna Declaration on Nuclear Safety.

In addition, Regulations PAK/909 [3] also require provision of clearance/approvals from local, provincial and other federal agencies.

#### 5. NEW ASPECTS COVERED IN THE EXISTING SITE REGISTRATION PROCESS

For site registration, licensee submitted the Site Evaluation Report (SER) to PNRA which included details/information mainly on geography, demography, meteorology, geology, seismology and geotechnical engineering of the site. In-line with Vienna Declaration and based on lessons learnt from Fukushima Daiichi accident, PNRA included new aspects in its existing site registration process. Accordingly, PNRA took on-board other government organizations, held/arranged discussions, acquired technical data, utilized their knowledge/expertise and updated assessment in the site registration process. The government organizations which were consulted during the technical review of the site evaluation to facilitate decision making are listed below:

- a) National Institute of Oceanography (NIO);
- b) NED University (Civil Engineering Department);
- c) Pakistan Meteorological Department (PMD);
- d) Geological Survey of Pakistan (GSP);
- e) Pakistan Coast Guards (PCG).

#### 6. IMPLEMENTATION OF VIENNA DECLARATION DURING SITE REGISTRATION OF K-2/K-3

K-2/K-3 is located on the coastline of the Arabian Sea, near Karachi city in the Sind Province of Pakistan. The site of K-2/K-3 is about 1.5km in the North-West of existing Karachi Nuclear Power Plant Unit-1 (K-1). In-line with Vienna Declaration and based on lessons learned from Fukushima Daiichi accident, amidst other, following aspects were specially focused by PNRA during the review of site evaluation report:

- a) Licensee was required to perform Probabilistic Seismic Hazard Analysis (PSHA) for the site.
- b) K-2/K-3 site was investigated for any earthquake potential up to 300km and potential fault sources were evaluated for peak ground acceleration.
- c) PNRA also directed the licensee to re-evaluate the seismic potential of Murray Ridge situated about 75km from the site with the perspective of tsunami potential. The tsunami analysis of Murray Ridge and historic instrumental seismicity along with other geophysical and drilling data indicated that no tsunami event occurred along Murray ridge in recent and distant past. Whereas, other potential sources related to Karachi site i.e. Makran subduction zone and triple junction are identified and also evaluated with special emphasis.
- d) Based on PNRA requirements, licensee performed studies by using next generation attenuation (NGA-2008) relationships to determine PGA values for K-2/K-3 site. The Safe Shutdown Earthquake (SSE) for site was re-assessed as 0.2g.

- e) Study has been performed for site to analyse the Seismic Hazard along with tsunami potential as per new IAEA guidelines. According to this study, in the worst case scenario, flooding height as a result of expected tsunami would be 2.8m. Moreover, site has been enlisted with Tsunami Early Warning System (TEWS) of Pakistan Meteorological Department (PMD) for dissemination of tsunami warnings.

## 7. NEW ASPECTS COVERED IN THE EXISTING PROCESS FOR ISSUANCE OF CONSTRUCTION LICENCE

In accordance with Regulations PAK/909, after site registration, the licensee applied for construction licence of K-2/K-3 along with applicable submissions which includes Preliminary Safety Analysis Report (PSAR), Quality Assurance Program (QAP) and Probabilistic Safety Analysis (PSA) Report. Verification of safety of nuclear installations was carried out at this stage through review & assessment, analysis & audit calculations and site surveys. Safety analysis, carried out by the licensee to support the design was reviewed and audit calculations were conducted by PNRA on sampling basis using analytical computer codes. The underlying assumptions, modelling techniques, accident sequence quantification, results and uncertainties were verified against the acceptance criteria.

PNRA included the following new aspects in the existing licensing process in-line with the lessons learned from Fukushima Daiichi accident and Vienna Declaration, in evaluation of application for issuance of construction licence to K-2/K-3.

- a) Although, the review and assessment process implicitly covered the feedback from operating experience, a new phase has been introduced in the review and assessment process following Fukushima accident which explicitly covers the operating experience feedback (OEF). The duration of phase is about 04 months.
- b) PNRA required submission of scale model testing reports which mainly included: tests of passive core cooling system in Station Blackout condition and passive residual heat removal system, secondary piping rupture upstream or downstream the isolating valve, passive containment cooling system, heat conducting capacity margin test and test on effect of flow pass change of in-vessel retention on heat exchange characteristics of pressure vessel.
- c) Based on regulatory review, PNRA required the licensee to submit detailed design report of secondary or outer containment and shield building which are new design features against impact of large commercial aircraft.
- d) As per existing regulatory framework, the design shall be independently verified by persons or groups separate from those carrying out the design before the submission to PNRA. Accordingly, PNRA required the licensee to submit the report describing the results of this independent verification.
- e) PNRA participated as an observer in IAEA Generic Safety Review of ACP-1000 (K-2 & K-3) and used the feedback of this review in licensing process.
- f) A number of additional supporting analyses were also required for regulatory review such as; the evaluation of steam generator components against cold emergency feed water, fatigue monitoring program, the stability and settlement analysis for foundations of seismic category-I structures etc.

## 8. IMPROVEMENT IN NUCLEAR SAFETY REGULATIONS

In light of the overriding concept of priority for safety, PNRA has proposed that design objective of NPPs be modified in the revision of Regulations PAK/911 to include the principle of practical elimination of event sequences which may result in significant radiation release. This necessitates that the design should ensure that off-site intervention measures to mitigate radiological consequences be limited or even eliminated in technical terms (VDNS Principle-1). National regulations already require the Periodic Safety Review of the operating nuclear power plants at least every 10 years. This includes re-evaluation of the site related aspects along with other factors (VDNS Principle-2). Keeping in view the lessons learnt from the Fukushima Daiichi accident and in line with Vienna Declaration, the following changes have been proposed in PNRA Regulations PAK/911 in accordance with the international practices and experience (VDNS Principle-3):

- a) Consideration of reliable filtered venting system independent of any AC power with limited operator action for operation;
  - b) Consideration of low probability independent events to occur simultaneously;
  - c) Consideration to control hydrogen within the spent fuel storage building in the event of loss of spent fuel cooling and to maintain integrity and functionality of fuel building;
  - d) Availability or provision of combined means to provide emergency power having reliability and form consistent with the safety requirements of the systems to be supplied, and performing their safety functions for longer durations on the assumption of a single failure;
  - e) Consideration of passive design features in the plant systems specially the emergency core cooling systems, Hydrogen recombining systems and spent fuel pool cooling systems.
- (Note: These regulations are currently being revised.)

## 9. CONCLUSION

The existing process of licensing of NPPs along with new aspects that has been considered in recent applications covered the objectives set out in the Vienna Declaration and Fukushima experience feedback. The objectives set out in the Vienna Declaration are now being implemented in all the new licensing applications and are also considered in the revision of regulations on siting and design of nuclear installations.

## REFERENCES

- [1] Vienna Declaration on Nuclear Safety, CNS/DC/2015/2/Rev.1, Vienna (2015).
- [2] PAKISTAN NUCLEAR REGULATORY AUTHORITY, Seventh Convention Report of Pakistan on Convention on Nuclear Safety, PANRA, Islamabad (2016).
- [3] PAKISTAN NUCLEAR REGULATORY AUTHORITY, PNRA Regulation for Licensing of Nuclear Installation(s) in Pakistan (PAK/909), PANRA, Islamabad (2012).
- [4] PAKISTAN NUCLEAR REGULATORY AUTHORITY, PNRA Regulations on the Safety of Nuclear Installations – Site Evaluation (PAK/910), PANRA, Islamabad (2008).
- [5] PAKISTAN NUCLEAR REGULATORY AUTHORITY, PNRA Regulation on the Safety of Nuclear Power Plant Design (PAK/911), PANRA, Islamabad (2014).

## LESSONS LEARNT FROM THE UK GENERIC DESIGN ASSESSMENT PROCESS

*IAEA International Conference – Vienna – June 2017*

DR R. MOSCROP, DR J. R. JONES, PROF A. TEHRANI, & R. EXLEY

Office for Nuclear Regulation

United Kingdom

Email: robert.moscrop@onr.gov.uk

### Abstract

UK government policy recognises that the construction of new nuclear power plants in the UK will play a vitally important role in providing reliable electricity supplies and a secure and diverse energy mix as the UK makes the transition to a low carbon economy. As an enabler to this construction programme, it is necessary to ensure that adequate levels of safety are guaranteed by design. The Office for Nuclear Regulation (ONR), the UK national body responsible for the regulation of nuclear safety and security, together with the Environment Agency (EA), the national body responsible for the relevant regulation in England and Wales, have developed a design acceptance process for the preliminary assessment of new reactor designs called the Generic Design Assessment (GDA). The process allows ONR and EA to interact with reactor designers at an early stage to maximise their influence. It also allows designers to understand and address regulatory concerns while the design is still on paper, which reduces the financial and regulatory risks for power station developers. The lessons learnt to date from application of the GDA process are presented in terms of the common regulatory issues that have been identified with international designs and the changes needed in order to meet UK safety expectations. ONR expects a safety case which demonstrates defence in depth in the design process as well as in the operation of the plant. Requirements include the need for comprehensive fault and hazard identification and a graded approach to safety analysis, including consideration of design basis analysis and beyond design basis analysis (design extension conditions) integrated with probabilistic safety analysis to reduce assessed risk as far as reasonably practical. ONR's expectations also include addressing the Vienna declaration for new designs.

### 1. INTRODUCTION

UK government policy [1] recognises that the construction of new nuclear power plants in the UK will play a vitally important role in providing reliable electricity supplies and a secure and diverse energy mix as the UK makes the transition to a low carbon economy. As an enabler to this construction programme, the Office for Nuclear Regulation (ONR), the UK national body responsible for the regulation of nuclear safety and security, together with the Environment Agency (EA), the national body responsible for the relevant regulation in England and Wales, have developed a design acceptance process for the preliminary assessment of new reactor designs called the Generic Design Assessment (GDA) [2].

The process allows ONR and EA to interact with reactor designers at an early stage to maximise their influence. It also allows designers to understand and address regulatory concerns while the design is still on paper, which reduces the financial and regulatory risks for power station developers. In this context, ONR and EA are not exercising their regulatory powers, but rather providing technical advice to the vendors on the licensing of the designs. The process has been in place since 2007 and is now well established and mature with two reactor designs (AREVA/EDF UK EPR™ [3] and Westinghouse AP1000® [4]) already having received a design acceptance certificate and one further design (Hitachi-GE ABWR) well into the later stages of the process.

The purpose of this paper is to use these previous GDA assessments as a way of illustrating UK regulatory requirements. The lessons learnt to date from application of the GDA process are presented in terms of the common regulatory issues that have been identified with international designs and the changes needed in order to meet UK safety expectations.

The licensing arrangements in the United Kingdom were introduced in the late 1950s in response to an accident at a military facility in west Cumbria. Legislation was introduced which required plant operators who handle nuclear material to apply for a site licence. The government established a Nuclear Installations Inspectorate (the predecessor organisation to ONR) to enforce compliance with the licence conditions and the ONR remains responsible for enforcement of the legislation to date. The licence conditions relevant to the design of new reactor require an adequate safety case justifying operations and operating rules defining the boundary of safe operation

[5]. These requirements were originally addressed by performing Deterministic safety analysis to demonstrate safety margins between operation and plant damage. This includes transient analysis of Design-Basis faults against Fuel Design Criteria. In subsequent years, a number of incidents outside the nuclear industry caused the UK government to revise health and safety legislation generally. The associated legislation extended the duties of licensees; requiring them to consider whether additional measures to mitigate the risk inherent in their operations were reasonably practicable [6]. This requirement has been reinforced by recent events such as TMI, Chernobyl and Fukushima.

The principles behind this approach are not unique to the UK and their impact on the design and licensing of new reactor designs is to some extent universal. This paper considers first the issue of Reasonably Practicable safety enhancements and then discusses the application of Deterministic Analysis. In making the decision on whether to sample a particular topic in detail and potentially to intervene, the regulator is required to follow the ONR enforcement principles [7]. These require regulatory action be proportion to the risk, consistency with other regulatory decisions, targeted, transparent and accountable. These principles are designed to ensure that assessment resources are appropriately targeted and that licensees can have predictable interaction with the regulator. In order to comply with these requirements, the inspectorate has issued guidance to its staff in the form of safety assessment principles [8] and technical assessment guides (for example [9]). The following discussion is based on this guidance.

## 2. THE TEST OF AS LOW AS REASONABLY PRACTICABLE

The UK law requires that the licensee consider measures that can be taken to eliminate or protect against a risk and to apply the test of whether the cost and trouble incurred is grossly disproportional to the incremental reduction in risk. Explanation of the thinking behind this approach is found in [10]. The framework is illustrated in Fig. 1.

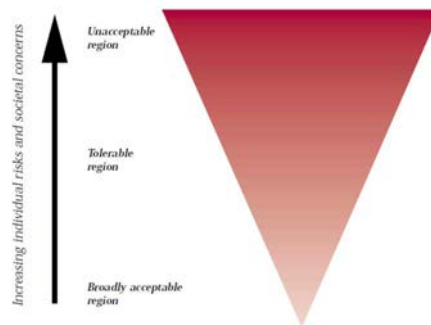


FIG. 1. The Tolerability of Risk framework [10].

In Fig. 1, the triangle represents increasing level of ‘risk’ for a particular hazardous activity (measured by the individual risk and societal concerns it engenders). As we move from the bottom of the triangle towards the top the need for mitigation is increased. The dark zone at the top represents an unacceptable region. For practical purposes, a particular risk falling into that region is regarded as unacceptable whatever the level of benefits associated with the activity. Any activity or practice giving rise to risks falling in that region would, as a matter of principle, be ruled out unless the activity or practice can be modified to reduce the degree of risk so that it falls in one of the regions below, or there are exceptional reasons for the activity or practice to be retained.

The lighter region represents an area where the risk could be accepted but mitigation measures should be taken unless analysis of the balance between benefit and risk shows that it is not reasonably practicable.

In developing a safety case, it is tempting to assign a value to the tolerable risk associated with a radiation dose; based on the risk of widely accepted in similar activities. However, ONR is likely to take a wider view. Risk can include consideration of the consequences of damage to trade and reputation. In a number of cases this has been the dominant risk [9]. The Three-mile Island Accident is one illustration: The individual risk to members of the public was low, but the impact on the development of nuclear power within the USA was severe.

The assessment of what is reasonably practical therefore becomes a qualitative rather than a quantitative process and the law regards relevant good practice as an illustration of an accepted balance.

### 3. SCOPE OF DETERMINISTIC DESIGN BASIS ANALYSIS

In the UK, identification of reasonably foreseeable Design Basis faults is the responsibility of the licence holder. However, ONR does provide guidance to help limit the scope of the task [8]: The licensee is required to consider the likelihood of the fault and the magnitude of the hazard.

Faults with a return frequency of less than once in 100,000 years, and faults where the unmitigated dose would be insignificant, can be excluded. Quantitative guidance is provided [8] and this is illustrated for off-site dose in Fig. 2. The criterion for tolerability varies with the frequency of the fault; increasing as the fault frequency is reduced.

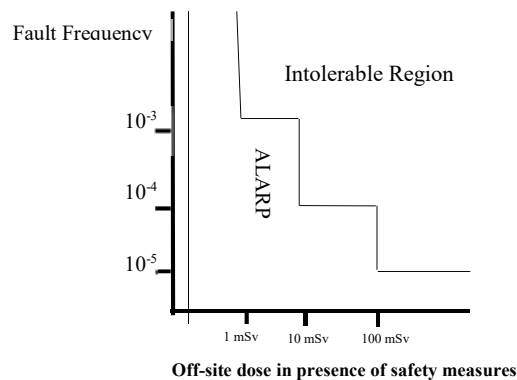


FIG. 2. ONR Target Levels of Off-site Exposure from Postulated Accidents.

From application of the GDA process to the assessment of international designs [3, 4] it is clear that a first lesson to be learnt from GDA is that the derivation of the list of design basis faults (generally called the Fault Schedule in the UK) based on the most extreme failure of each plant system, tends not to be sufficiently comprehensive to meet UK requirements. Faults often omitted from the design basis analysis of safety analysis report [3, 4] include:

- Faults initiated by common mode failure of essential support systems;
- Faults during shutdown and part-power operations;
- Faults involving the spent fuel pool and fuel handling;
- Faults involving heterogeneous boron dilution (on PWRs);
- Faults involving spurious computer software failure on C&I platforms including the primary protection system and where the fault is assumed to affect multiple redundant trains, and;
- Internal and external hazards.

The faults initiated by common mode failure of essential support system should include consideration of the essential electrical system, HVAC system or the cooling chain including loss of ultimate heat sink as well as long term loss of off-site power since it is difficult to conclude that the common mode failure rate for any of these faults is less than  $10^{-5}$  per year target given in Fig 2. While it is recognised that design provision for internal and external hazards are often considered within the safety analysis report there is often a lack of rigour in how the adequacy of the provision is substantiated sufficient to meet the requirements expected for a UK safety case.

In summary, the UK expectation [8] is that the process for fault identification should be systematic, auditable and comprehensive covering:

- significant inventories of radioactive material;
- planned operating modes and configurations including shutdown states and decommissioning operations and any other activities that could present a radiological risk, and;
- chemical and other internal hazards, man-made and natural external hazards, internal faults from plant failures and human error, and faults resulting from interactions with other activities on the site.

#### 4. DEFENCE IN DEPTH AND DESIGN EXTENSION CONDITIONS

International guidance [11-13] has recently been revised and developed to take account the lessons learnt from Fukushima. These new requirements include the need to enhance the defence in depth concept covering Design Extension Conditions (DEC), consideration of practical elimination, avoidance of cliff edges just beyond the design basis for external hazards and combinations of credible initiating events including internal and external hazards. The aim of these objectives is to avoid large early releases or releases that can result in the long-term contamination of land. There are two categories of DEC:

- DEC-A sequences for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved;
- DEC-B sequences associated with postulated severe fuel damage.

The selection process for DEC-A sequences starts with the consideration of those events and combinations of events which cannot be considered with a high degree of confidence to be extremely unlikely to occur and which may lead to severe fuel damage in the core or in the spent fuel storage and covers:

- Events occurring during the defined operational states of the plant;
- Events resulting from internal or external hazards;
- Common cause failures.

The set of category DEC-B events are postulated and justified to cover situations, where the capability of the plant to prevent severe fuel damage is exceeded or where measures provided are assumed not to function as intended, leading to severe fuel damage.

Many of these developments were already established as relevant good practice [8] in the UK although ONR guidance undergoes regular review to maintain compliance with relevant international practice. In particular, it has been a long standing practice in the UK to consider fault sequences with frequencies greater than  $10^{-7}$  per year to be within the design basis. In practice this drives for the inclusion of functional diversity within a design for each major safety function consistent with DEC-A approach, although in the UK there is the additional expectation that the safety classification for such equipment will be designed to meet nuclear design codes and standards (associated with a system safety classification of at least Class 2 as discussed in Section 6 below) rather than industrial codes and standards.

From application of the GDA process to the assessment of international designs [3, 4] a second lesson to be learnt from GDA is that generally the new designs have through the use of level 1 and 2 Probabilistic Safety Analysis (PSA) included design provisions to meet the DEC-A and DEC-B requirements. However, the UK requirement to systematically demonstrate functional diversity for each safety function has often identified the need for significant additional transient analysis studies covering sequences such as anticipated transients without scram (ATWS) events and this analysis has sometimes identified the need for additional design modifications. Specifically, these design changes have included:

- Upgrading of the diverse safety systems [3, 4] to meet Class 2 design requirements;
- Provision of a hard-wired diverse protection system [3] to provide functional diversity for failures in the computer based primary protection system;
- Provision of additional actuation signals on the diverse protection systems [3, 4].

Other lessons to be learnt [3, 4] from GDA are that in developing design basis fault sequences explicit accident analysis and ALARP justification is needed to justify:

- Passive single failures including accumulator non-return (check) valves;
- Interface loss of coolant accidents (LOCA) with the potential for containment by-pass;
- Consequential steam generator tube rupture (SGTR) failures following steamline faults;
- Consequential LOCA faults following Safety Relief Valve (SRV) lift, and;
- The transition from the controlled state to the safe shutdown state.

In summary, the UK expectation [8] is that correct performance of safety-related and non-safety equipment should not be assumed where this would alleviate the consequences. Where failures or unintended operation of equipment not qualified for specific accident conditions could exacerbate the consequences, or otherwise make the fault more severe, this should be assumed within the DBA.

Each design basis fault sequence should include as appropriate:

- Failures consequential upon the initiating fault, and failures expected to occur in combination with that initiating fault arising from a common cause;



- Single failures in the safety measures in accordance with the single failure criterion;
- The worst normally permitted configuration of equipment outages for maintenance, test or repair, and;
- The most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.

Sequences with very low expected frequencies need not be included in the DBA. Judgement should be exercised in this regard, but for high hazard facilities, a fault sequence frequency of  $10^{-7}$  per year would be a typical cut-off when applying design basis techniques.

## 5. CONCLUSIONS

The intention of the system of regulation set out above is not to provide a prescriptive set of steps by which utilities can meet regulatory requirements, but a set of flexible guidelines which allow utilities to design, construct, commission and operate safely and to engage constructively with the regulatory body. The aim is to provide a robust demonstration that the plant can meet the challenges presented by anticipated faults and that all reasonably practical measures have been taken to reduce the risk to a broadly acceptable level.

## REFERENCES

- [1] DEPARTMENT OF ENERGY AND CLIMATE CHANGE, National Policy Statement for Nuclear Power Generation (EN-6), Vol I of II, DECC, July 2011.
- [2] OFFICE FOR NUCLEAR REGULATION, New Nuclear Reactors: Generic Design Assessment Guidance to Requesting Parties, ONR guidance ONR-GDA-GD-001, Rev. 3, 2016.
- [3] OFFICE FOR NUCLEAR REGULATION, Generic Design Assessment – Step 4 Fault Studies – Design Basis Fault Assessment of the EDF and AREVA UK EPR™ Reactor, ONR-GDA-AR-11-020a, November 2011.
- [4] OFFICE FOR NUCLEAR REGULATION, Generic Design Assessment – Step 4 Fault Studies – Design Basis Fault Assessment of the Westinghouse AP1000® Reactor, ONR-GDA-AR-11-004a, November 2011.
- [5] Office for Nuclear Regulation Licence condition handbook, October 2011.
- [6] Health and Safety at Work Act 1974.
- [7] OFFICE FOR NUCLEAR REGULATION, ONR Enforcement Policy Statement, 2014.
- [8] OFFICE FOR NUCLEAR REGULATION, ONR Safety Assessment Principles for Nuclear Facilities, 2014.
- [9] OFFICE FOR NUCLEAR REGULATION, ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), T/AST/005 – Rev. 7, 2015.
- [10] HEALTH AND SAFETY EXECUTIVE, Reducing Risks, Protecting People, HSE's decision-making process, ISBN 0 7176 2151 0, UK (2001).
- [11] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Specific Safety Requirement, No. SSR-1/2 (Rev. 1), IAEA, Vienna (2016).
- [12] VIENNA DECLARATION ON NUCLEAR SAFETY, On principles for the implementation of the objective of the Convention on Nuclear Safety to prevent accidents and mitigate radiological consequences, CNS/DC/2015/2 Rev. 1, Vienna (2015).
- [13] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Safety Reference Levels for Existing Reactors, WENRA, September 2014.

## **LESSONS LEARNED FROM THE PREPARATORY PROCESS FOR LICENSING OF THE NEW NUCLEAR UNITS IN HUNGARY**

J. KRUTZLER

Hungarian Atomic Energy Authority

Budapest, Hungary

Email: krutzler@haea.gov.hu

### **Abstract**

In 2014 the Hungarian Government signed an Intergovernmental Agreement with the Russian Federation, for the construction of two VVER-1200 units at the Paks NPP site. The Hungarian Atomic Energy Authority (HAEA) is responsible for the supervision and licensing of nuclear facilities in Hungary. In preparation for the licensing of the new NPP, significant efforts were invested to meet the challenges of such a complex task. Goal of this paper is to summarize the results and lessons learned of this preparatory process from the view of the licensing authority.

### **1. INTRODUCTION**

In January 2014, Hungary signed an Inter-Governmental Agreement with the Russian Federation for the construction of two VVER-1200 units at the Paks site, which currently has four operating units of the VVER-440 type reactor. The new units are expected to start operation around 2026. The agreements have been approved by the Parliament in two consecutive parliamentary terms. Based on the intergovernmental agreements (IGA), three contractual implementation agreements were signed in December 2014, between MVM Paks II Ltd. on the Hungarian side, and JSC NIAEP on the Russian side: the engineering, procurement and construction agreement (EPC), the fuel supply agreement, and the operation and maintenance support agreement.

Before the start of the construction, several permits and licenses must be issued. Hungary has a decentralized regulatory system, where the Hungarian Atomic Energy Authority (HAEA) is responsible for the oversight of nuclear safety, security and safeguards, whilst the Government Office of Baranya County is responsible for environmental issues.

Authorisation for site investigation and evaluation for the Paks II project company was given by HAEA in 2014. Execution of the site investigation program started in 2015. A site license application was submitted in October 2016, which was approved in March 2017 by HAEA. The construction license application is expected to be submitted in 2018.

Regarding the environmental permitting several forums were held in the region of the site, and – in line with the Espoo Convention – nine international hearings in seven neighbouring countries were conducted in September-November 2015. The Environmental Authority has issued the environmental permit in 2016, which was appealed by NGOs. Second-degree permit review concluded in April 2017 and reaffirmed the earlier environmental permit.

### **2. CHALLENGES AND LESSONS LEARNED**

The construction of a nuclear power plant is a major, long-lasting project, which represents a challenge for all involved parties. The early phases of Hungary's NPP construction project have been running for several years now, and it focused on preparations. During these efforts HAEA initiated the review of the Hungarian legislation regarding nuclear power plants. Because of this review, significant changes to the legislation have been implemented.

After the Fukushima-Daiichi accident international safety standards have been improved. This introduced several new elements into already existing concepts (e.g. practical elimination). To incorporate these new elements into the national legislations, they had to be interpreted, and detailed into safety requirements – including quantitative engineering criteria – whilst maintaining the “technological neutrality” of the legislations. The following chapters summarizes some of the experiences and results of this process.

## 2.1. Differentiation of requirements for existing and new units

The Hungarian Act on Atomic Energy states that regulatory requirements should be reviewed every 5 year, and in cases where significant new safety issues arise. A periodic review was performed in 2011, and an extraordinary post-Fukushima review was conducted in 2013-2014. During these reviews HAEA faced several challenges. First, based on lesson learned from recent construction projects (e.g. Olkiluoto 3) it was deemed necessary to prepare detailed QA/QC/QM and specific management system requirements for the design and construction processes, and for the organisational capabilities of the licensee (e.g. *intelligent customer*<sup>1</sup> capability). Second, the lessons learned from the Fukushima accident had to be incorporated into the legal requirements.

As a result of the above-mentioned reviews, the detailed and technical level requirements were implemented into the Nuclear Safety Codes (NSC). Design and construction process specific management system requirements were incorporated into Vol. 9 of the NSC (see Fig. 1.).

Incorporation of the lessons learned from the Fukushima-accident was a difficult task, because at the time of the review (2013-2014), only high-level recommendation existed (e.g. ‘large releases should be practically eliminated’, etc.). HAEA’s challenge, together with other stakeholders, was to ‘interpret’ these high-level recommendations, and create detailed engineering and acceptance criteria for them.

After careful analysis it was determined, that it is not beneficial to create universal safety requirements that are applicable for both existing (Gen II) and newly constructed (Gen III+) units. Based on this, it was decided, to separately create and/or update requirements for existing and new units (show as Vol 3. and Vol 3A. on Fig. 1.). This separation allowed to implement new concepts and stricter requirements for the new units. For instance, the updated Defence-in-Depth principle as shown in Ref. [1] was implemented in Vol. 3A. of the NSC. Also, the exceedance frequency values for natural hazards to be considered in design basis is stricter;  $10^{-4}/a$  for existing units (in line with Reference Level T4.2 of Ref [2]),  $10^{-5}/a$  for new units.

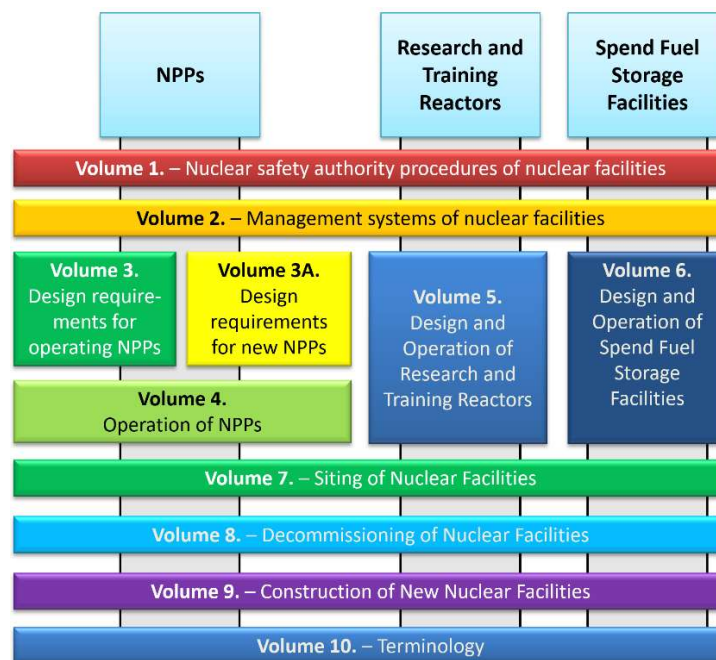


FIG. 1. Structure of the Nuclear Safety Codes (NSC).

<sup>1</sup>As an intelligent customer, in the context of nuclear safety, the management of the facility should know what is required, should fully understand the need for a contractor's services, should specify requirements, should supervise the work and should technically review the output before, during and after implementation. The concept of intelligent customer relates to the attributes of an organisation rather than the capabilities of individual post holders.

Based on HAEA's experience, and feedback from the stakeholders the decision to separate requirements for existing and new units is considered beneficial, because it allows easier interpretation of requirements for the licensees, and it also helps HAEA to take greater advantage of the graded approach during its oversight activities.

## **2.2. Specific requirements and guidance for the design and construction phase**

As mentioned in the previous chapters, the need for more detailed requirements and guidance regarding the design and construction phases of the project was identified. Besides the incorporation of lessons learned for nuclear power plant projects (e.g. Olkiluoto 3), several other areas required attention. A few examples:

*Design adaptation:* nuclear powerplant vendors generally use the codes and standards of their country of origin, but within the EU some areas have mandatory codes and standards as well (e.g. civil construction code). To harmonize and/or unify design requirements, as well as codes and standards, a design adaptation process has to be developed and implemented by the licensee. The rules of this process have been established in Vol. 9 of the NSC, and in the corresponding regulatory guide.

*Supply chain management:* based on lessons learned from other projects, it was deemed necessary to enhance supply chain management requirement for the design and construction phases. For instance, the licensee is required to oversee the whole supply chain, down to the lowest tiers, and they must ensure that every supplier doing a safety related activity has a task-specific nuclear qualification.

*Safety of neighbouring nuclear facilities:* the new units will be constructed next to the operating units. To ensure the safety of the operating units, several design (e.g. crane placement) and construction (e.g. mandatory risk assessment of on-site construction activities before their commencement) requirements have been established. One in particularly interesting challenge is the emergency preparedness of the construction site, because in case of a nuclear emergency at the operating units, a peak number of c.a. 7000 workers must be evacuated from the construction site.

To solve issue like the one mentioned above, a continuous cooperation with all involved parties is necessary, both on management and expert level. Based on HAEA experience, this process is easier if the requirements and the associated regulatory guides are sufficiently detailed.

## **2.3. Requirement management**

As a result of the requirement review shown in the previous chapters, the number of legally binding requirements and the areas covered by regulatory guidelines has significantly increased. Currently legal requirements relevant for HAEA's scope of work contains more than 10000 paragraphs, ranging from high-level requirements to specific technical requirements. Managing such a large amount of information, especially in terms of connections and interfaces represents a great challenge.

To increase efficiency of information handling, and to ensure a common understanding of requirements by staff members a project has been established within HAEA to implement a special software tool for requirement management. It was determined that there are suitable commercial software products (e.g. used by the aerospace industry) available on the market which could be customized for HAEA's specific needs.

One of the main expectations is, that the software tool should have specific features for benchmark and gap-analysis activities. This feature is necessary, firstly because the number of international recommendation and legally binding requirements significantly increased after the Fukushima accident, secondly it represents a challenge to ensure consistency with both the original text, but also with other parts of the Hungarian legal document under assessment.

The need for requirement management was also established by the licensee of the new units. Although the scope of requirements is different in some elements, the fundamental issue is the same. With that in mind, HAEA works together with the licensee to coordinate the development, and to ensure that the requirement management system of the licensee and HAEA could interface with each other.

## **2.4. Number of licensing steps**

During the review process mentioned in the previous chapters, the licensing model was also evaluated. Several aspects were considered, such as: administrative workload; possibilities to oversee and enforce nuclear

safety requirements during the design and construction phases; safety considerations for nuclear facilities affected by the construction activities; etc.

After consulting with stakeholders, in terms of facility level major licencing, a multi-step licensing model has been established as shown in Fig. 2. The first two step have already been taken (see Introduction).

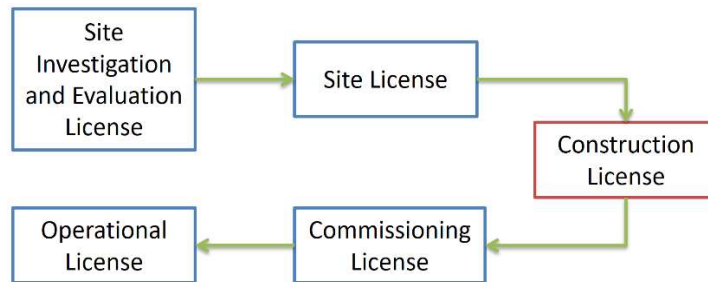


FIG. 2. Major licensing milestones (nuclear safety related).

Although the multi-step licensing model shown in Fig. 2. has certain disadvantage, like putting extra administrative workload on the licensee and the regulator, it also has advantages in terms of safety, for example:

- It ensures the early involvement of the regulator in the construction project, and safety related issue can be identified by them in a timely manner.
- The licensee gets certain assurances by receiving a licence at major milestones; it reaffirms that regulatory requirements are met. With this multi-level licensing model, the risks associated with regulatory approval processes are distributed over several phases of the project, which enables easier management of these risk, and allows a better use of the graded approach.
- When the very first licence is granted, the applicant becomes a nuclear licence holder, which means they have to meet legally binding nuclear safety requirements relevant for that phase of the project. For instance, relevant management system and leadership requirements based on Ref. [3] should be met even before the start of the site investigation and evaluation. This ensures that the nuclear safety is paramount early on.
- As a result of point (c), HAEA has the legal right to supervise the licensees' activities, and enforce nuclear safety requirements.
- At every facility level licensing step, HAEA is required by law to make a public hearing, where citizens and NGOs can express their opinions and concerns. With the multi-step model show in FIG. 2. a public hearing is held at each major project milestone, which enables enhanced public involvement in the regulatory decision-making process.

Based on HAEA experience so far, the positive effects of such a multi-step licensing outweighs the disadvantages.

## REFERENCES

- [1] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Report: Safety of new NPP designs, WENRA Reactor Harmonization Working Group, WENRA (2013), [http://www.wenra.org/media/filer\\_public/2013/04/30/rhwg\\_safety\\_of\\_new\\_npp\\_designs.pdf](http://www.wenra.org/media/filer_public/2013/04/30/rhwg_safety_of_new_npp_designs.pdf)
- [2] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Report: WENRA Safety Reference Levels for Existing Reactors (Update In Relation To Lessons Learned From Tepco Fukushima Dai-Ichi Accident), WENRA (2014), [http://www.wenra.org/media/filer\\_public/2014/09/19/wenra\\_safety\\_reference\\_level\\_for\\_existing\\_reactors\\_september\\_2014.pdf](http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf)
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and management for safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

## **RUSSIAN REGULATORY APPROACH TO EVALUATION OF PASSIVE SYSTEMS USED FOR SPECIFIC BDBA'S (SBO, LOSS OF UHS) DURING SAFETY REVIEW OF NPP**

D. ROGATOV

Scientific and Engineering Centre for Nuclear and Radiation Safety

Moscow, Russia

E-mail: rogatov@secnrs.ru

### **Abstract**

New designs of Russian VVER NPPs that obtain license for siting or construction initially includes a set of passive systems, which are used for the management of BDBAs (including severe ones) associated with SBO and/or loss of UHS. The following technical solutions to overcome SBO (loss of UHS) scenarios are used in different NPP designs:

- passive heat removal system from SG and containment;
- hydroaccumulator tanks (different groups are used at different stages of the accident).

One of the significant issues assessed during safety review of NPP with regard to the passive systems is the requirement that innovative technical means can be used in plant design on the basis of sufficient substantiation by necessary calculations, experimental studies and operational experience.

The purpose of this paper is to describe:

- different design solutions of passive safety systems used in modern VVER NPP design;
- Russian regulatory requirements used for evaluation of this systems;
- key safety review findings regarding passive safety systems.

This paper describes passive systems and approaches to their assessment, that mostly operate in BDBA with SBO and/or loss of UHS, when active systems are failed (as an example, the systems envisaged in Novovoronezh NPP-2 and Leningrad NPP-2). Passive systems used in case of a severe accident (for example core catcher, containment hydrogen removal system) are out of the scope of this paper.

### **1. INTRODUCTION**

In accordance with the requirements of the Russian safety regulation NP-001-15 [1] («in the design of NPP systems (elements) priority shall be given to systems (elements) the design of which is based on the passive principle of action, including natural processes such as natural circulation») the set of passive systems was introduced into Russian NPP designs. There are new modern systems that were introduced recently only in modern VVER designs. These systems include passive heat removal system from steam generator (PHRS SG), passive heat removal system from containment (Containment PHRS), hydro accumulators of 2nd stage (HA-2). The main aim of introduction of such systems is providing reliable implementation of one of the major safety functions [1], [2] - removal of heat from the reactor in accident scenarios with total station blackout (loss of all on-site and off-site power supplies including emergency power supply from diesel generators – SBO) along with emergency scenario with loss of nuclear fuel residual heat removal systems to the ultimate heat sink (UHS). There are also potential benefits to reduce the number of active components and (or) support systems which would further reduce maintenance and testing efforts. Therefore, sources for failures may be reduced.

However, there are many questions raised for new passive system, for example: the proof of their efficiency, the possibility of their testing during operation of NPP and representability of obtained test results, applicability of the safety principles that apply to active systems (single failure concept, etc).

It is needed to mention that the severe accident took place in Japan at the Fukushima Daiichi NPP in March 2011 highlighted the importance of passive systems that can cope to accident involving SBO and UHS and the proper fulfillment of their functions. So, the comprehensive assessment of this systems is a big challenge for experts.

### **2. DESIGN SOLUTIONS OF PASSIVE SAFETY SYSTEMS USED IN MODERN VVER NPP DESIGN**

The result of the evolution of the NPP-2006 design delivered two different options of modern NPP VVER design:

- VVER-1200/AES-2006-M design (developed by the power plant design organizations within ROSATOM: Moscow Atomenergoproekt) – the example of the design is Novovoronezh NPP-2 [3];
- VVER-1200/AES-2006-P design (developed by the power plant design organizations within ROSATOM: Saint-Petersburg Atomenergoproekt) – the example of the design is Leningrad NPP-2 [4].

The main distinctive features of these designs are that safety functions can be provided both by active systems and passive systems independently from each other.

Main difference between two approaches for configuration of safety systems is that in VVER-1200/AES-2006-M the active safety systems are of 2-train configuration (some - with redundancy of separate elements inside train) with passive safety systems as air-cooled PHRS SG and HA-1, HA-2 whereas in VVER-1200/AES-2006-P the active safety systems are of 4-train configuration (“typical” structure of safety systems) with passive safety systems as water-cooled PHRS SG, Containment PHRS and HA-1.

In both cases regardless of passive system existence, mobile equipment is used to fulfill the safety functions on later accident stages.

The scheme of construction of these systems is shown in Figures 1 and 2.

## **2.1. VVER-1200/AES-2006-M design solutions**

### **2.1.1. Air-cooled PHRS**

PHRS is intended for removal of heat residuals from the reactor core at the accidents with the loss of all alternating electric power supply sources both at the tight primary circuit and at the occurrence of leaks either in the Primary or in the Secondary Circuit. If primary circuit is intact, the heat can be removed for considerable time without external water makeup. In case of leaky primary circuit, the heat removal is secured by joint operation of PHRS and HA-1, HA-2. The system consists of four independent circuits of natural circulation: one per each circulation loop. Each circuit includes two heat-exchanging modules, pipelines of steam-condensate path with valves, path of air ducts which supply and remove air, air valves and regulative devices. Each heat exchanger is equipped with air valves allocated upstream and downstream along the motion of air flow. A regulative device is located between the heat exchanger and the upper air valve. A signal for actuation of PHRS is the signal of the NPP de-energizing and consequent non-start-up of diesel generators.

The reactor residual heat is transferred through steam generators to steam-external air heat exchangers of the PHRS where the steam is condensed and returned to the steam generators. Cold air intake is in the lower part of the reactor building. Heated air conveys through air ducts on the dome of the containment to discharge deflector.

### **2.1.2. Hydro accumulators of 2nd stage**

The HA-2 is intended for the performance of the following functions passive supply of boric solution into reactor core with the purpose of heat residuals removal under BDBA with total loss of alternating electric power supply sources including diesel generators, and leaks due to the primary circuit pipeline rupture during maximum possible period of time (no less than 24 hours taking into account the PHRS operation).

The system consists of four groups. Each group comprises two hydraulic capacities of the 2nd stage (which stay under atmospheric pressure in the modes of normal operation and contain boric acid solution), pipelines and valves. The entire stock of boric acid solution provides the required volume, which is supplied in the reactor core at the failure of one group.

On the discharge line, the HA-2 is connected to pipelines of the reactor connection of the HA-1 in non-connected from the reactor part. The boric solution is supplied from the hydraulic capacities to the head and discharge chamber of the reactor. On the discharge pipeline, shut-off gates are installed, which are necessary to disconnect hydraulic capacities from the primary circuit (at the necessity of repair, when the reactor is stopped) and check valves intended to exclude pressure increase in hydraulic capacities in the condition of expectation and automatic passive opening of discharge line in the emergency situation after decrease of pressure in the primary circuit.

## 2.2. VVER-1200/AES-2006-P design solutions

### 2.2.1. *Water-cooled PHRS from SG*

The water-cooled PHRS SG in AES-2006-P design uses water stored in tanks on the top part of the containment. The system is intended to provide long-term heat removal from core into the atmosphere in case of BDBA (for at least 24 hours). PHRS SG has four independent trains, each incorporating: emergency heat removal tank; emergency cooling heat exchanger; large and small cut-off valves; pipelines and other valves. In case of SBO, total loss of feedwater, or impossibility to remove heat from secondary circuit by other systems, the cut-off valve will be open to initiate secondary coolant circulation through emergency cooling heat exchanger (in case of accident with SBO, a passive opening of the cut-off valve is carried out due to the fact of loss of all onsite and offsite power supplies including emergency power supply from diesel generators). With that, water in emergency heat removal tank will be heat up to boiling, and will begin to evaporate, giving heat to atmosphere. The tank water level will decrease.

According to Licensee calculations tank water inventory in three trains of PHRS SG is sufficient to cool the reactor for 24 hours in case of a SBO or total loss of feedwater flow.

### 2.2.2. *Water-cooled PHRS from containment*

The system is intended to provide long-term heat removal from containment into the atmosphere in case of beyond-design-basis accidents. The system is designed to provide long-term heat removal from containment to ultimate sink in case of beyond-design-basis accidents, during at least 24 hours. Containment PHRS has four independent trains (4x33%), each incorporating 4 condenser heat exchangers, isolation valves and pipelines. Heat is removed from containment owing to vapour condensation in condenser heat exchangers, from which it is transferred to emergency heat removal tanks under natural circulation of coolant, and then to the atmosphere, owing to water evaporation in emergency heat removal tanks which are part of the water-cooled PHRS SG. Containment PHRS heat capacity was chosen to keep containment pressure in BDBA conditions (including severe accidents with fuel meltdown) within the design-bases limits.

## 3. RUSSIAN REGULATORY APPROACH TO EVALUATION OF PASSIVE SYSTEMS

In accordance with the Russian regulatory approach, the same regulatory requirements used for evaluation of the passive safety systems that are used for the active safety systems. For example, requirements for safety valves, hydraulic test, materials used to manufacture of passive system components NP-089-15 [10] (elements under pressure of the working medium) as well as requirements for monitoring the level and concentration of the boron solution [6], without any difference from active systems, are applied for elements of passive systems. Current regulations adopted in the nuclear power industry contain almost no specifications to principles of design passive safety systems used for removal heat from reactor. According to NP-006-98 [7] (and draft NP-006-16 [8]) the passive safety systems should be described in Safety Analysis Reports (SAR) at the same level of detail as the other safety systems.

First of all, as all mentioned above passive systems are innovative technical means ("first of a kind"), one of the important issues assessed in the course of review is the fulfillment of requirement para 1.2.7 NP-001-15 [1]: "Technical and administrative decisions made for NPP safety ensuring shall be well proven by the previous experience or tests, investigations, operating experience of prototypes". Existence of sufficient approbation of these systems which implies of sufficient substantiation of their operability by calculations, experimental studies and (or) operational experience shall be carefully checked. Applicability of thermo-hydraulic codes for calculation (the codes and methodologies used for safety justification shall be verified and certified in accordance with the established procedures NP-082-07 [6]) shall be shown by the Licensee (generally in SAR or in some topical reports referenced in the SAR). If the experiments to justify the efficiency of the system were conducted, SAR should describe the experimental conditions, an analysis of the compliance of these conditions with the actual conditions of the system, describe the experimental base, metrological support of experiments, provide the main results of the experiments [7], [8].



When the calculations and experimental studies of passive safety systems are implemented, the next issues also should be considered [13]:

- sufficiency of providing for the function of heat removal from reactor with no time limitation or the providing some explanation for time limitation (24, 72 or more hours) - (for water consuming systems – such as watery PHRS – the measures on inventory make-up are to be envisaged) in any weather condition (for air-cooled PHRS – minus temperatures or wind);

- potential negative interactions of active and passive systems or/and different passive systems (i.e. interactions worsening their reliability) foreseen to operate simultaneously;

- possible delays in systems operation caused by various reasons (such time interval shall not exceed time period when the accidents' evolving into the severe condition is being prevented because of natural processes related to coolant heating and boiling-off (in SGs, in primary circuit);

- analyses of the effects of non-condensable gases and a strategy to prevent collection of them into the heat exchangers.

According to para 3.1.9 NP-001-15 [1] all safety systems shall be designed and protected to tolerate common cause failures by applying the principles of diversity, redundancy and independence. However, for passive systems the existing of active systems shall be taken into account that fulfill the same safety function. So, these principles applied to combination of active and passive systems.

Failure criteria is also applied to combination of active and passive systems according to Para 1.2.12 NP-001-05 [1] that states: *“The established limits for design basis accidents shall not be exceeded at any initiating event considered by the NPP design with a coincidental independent failure of one of the following safety system elements according to the single failure principle: an active element or a passive element with mechanical movable parts, or a passive element without movable parts whose probability of safety function performance failure is equal to  $10^{-3}$  or higher or one human error independent of the initiating event. ... Failures of elements (systems which they make part of) may not be considered if high level of their reliability is demonstrated or when the element (system) is in outage for a determined period of time for maintenance and repair. The reliability level is considered to be high if indicators of reliability of elements (systems) are not lower than appropriate indicators of the most reliable passive elements of safety systems without movable parts. ...”*. The above-mentioned requirement reflects some differences in approaches to the consideration of failures of passive and active systems.

According to Para 3.1.8 NP-001-05 [1] passive safety systems (as the active systems) and elements shall be capable of performing their functions within the NPP designs cope and with due consideration of the natural effects, external human induced events typical for the NPP site and (or) under possible hydraulic, mechanical, thermal, chemical and other impacts occurred as a result of accidents at which work of the considered systems and elements is required. Passive systems mainly designed to fulfill their function in case of SBO or/and loss of UHS (when the operation of active systems is failed) consequently the special attention should be directed to the hazards which can lead to SBO and loss of UHS. The protection from these hazards shall be performed by SAR. Passive safety systems should be independent from active safety systems with the purpose to ensure that failure of the active ones never results in failure of passive ones applied for management of accidents with SBO or loss of UHS.

Reliability analyses of fulfillment of functions by the passive safety systems shall be presented in SAR according para 3.1.17 NP-001-05 [1]. The general approaches of fulfillment qualitative and quantitative reliability analysis of safety important systems described in RB-100-15 [5] in which one of the last chapters is devoted the features of the analysis of the reliability of systems with passive elements.

According to para 3.1.14 NP-001-15 [1] passive safety systems, as any safety systems, should be tested, including their active components, during commissioning and in operating plants to the extent feasible to assure their compliance with the design parameters. Direct and full checks are preferable but if performance of direct and/or full checks not be possible indirect and/or partial checks shall be carried out. Adequacy of indirect and/or partial checks shall be validated in the NPP design.

When safety function can be fulfilled by either active or passive safety system the SAR (Chapter 15) should contain substantiation for both cases: a) when only active systems are in operation and b) when only passive systems are in operation.

According to the draft NP-006-16 [8] false actuation (starting) of passive system should be evaluated as one of initiating event (as a rule the false actuation of PHRS SG is considered).

Finally, it should be noted that in case of passive systems (their pipelines) penetrating the containment and communicating with the reactor coolant or containment atmosphere the requirements of the NP-010-16 [9] apply (same as the requirements applicable to the active systems).

According to para 4.2.4 NP-001-05 [1] confirmation of the actual characteristics of passive systems is performed during the commissioning of the NPP unit, while the characteristics of equipment and systems, design limits and conditions will be specified. Based on the results of commissioning, a final version of the FSAR should be developed (para 4.2.6 NP-001-05 [1]), that contains information on the results of the carried out tests, including the refined information of the systems. The Licensee should justify in the FSAR that the passive systems, according to the results of commissioning, correspond to the initially presented data, and the characteristics of the systems obtained from the results of calculations and experiments are confirmed.

#### 4. KEY FINDINGS OF SAFETY REVIEW OF NPP IN REGARD TO PASSIVE SYSTEMS

This section presents the example of key findings regarding passive systems, found during the fulfilment of safety review of Novovoronezh NPP-2 and Leningrad NPP-2 based on regulatory approach described in Section 3.

Today the safety review of Novovoronezh NPP-2 and Leningrad NPP-2 are in different stage of implementation. For Novovoronezh NPP-2 review of preliminary version of Final SAR [11] is finished – the unit got a license for operation. For Leningrad NPP-2 review of preliminary safety analysis report (PSAR) is finished [12] and review of preliminary version of final SAR is just started. According to this the different level of issues were revealed in the course of safety review.

##### 4.1. Novovoronezh NPP-2

###### 4.1.1. *Findings about aerial PHRS SG*

evaluation of the impact of non-condensable gases inside PHRS's steam condensate tract on the efficiency of system heat exchangers;

PHRS efficiency in case of considerable coolant loss, active ECCS failure, and non-condensable gases entering heat exchange area of the steam generator;

PHRS efficiency in case of on-site fire (multifactor impact of the fire including high temperature and air humidity decrease on the entrance of the PHRS air intake, possible downflow air movement streaming around the containment, reverse flow in the PHRS air ducts on the outer side of the compartment opposite the fire can deteriorate performance of a PHRS heat exchangers);

PHRS efficiency in case of external impacts (e.g. wind impacts);

substantiation of the PHRS start-up characteristic. Substantiation of the PHRS start-up time under the minimum and maximum external temperatures. Substantiation of reliability of the PHRS lock valve and air controller.

###### 4.1.2. *Findings about HA-2:*

substantiation of the efficiency of the HA-2 system, taking into account joint operation of HA-2 and PHRS (calculated and experimental substantiations of the efficiency of passive safety systems operation in case of LOCA, taking into account the interaction of primary circuit, passive systems (HA-2 and PHRS), containment and the impact of non-condensable gases. Substantiations should prove the effectiveness of the passive safety systems, as well as show the available reserves of time before drying of the reactor core);

substantiation of the HA-2 flowrate characteristic, taking into account the possible range of places and size of the primary circuit pipe rupture, and the impact of other systems (e.g. HA-1, active ECCS).

#### 4.1.3. *Current state*

As a result of the large scale complex of the calculated and experimental substantiations of the HA-2 and PHRS performance efficiency fulfilled by the Licensee significant part of issues was eliminated or significance of issue to safety was reduced to level of recommendations.

Positive conclusions of the final review were based on assessment of the topical reports which contained results of background calculations, tests and experimental justification based on specially constructed experimental stands that were submitted by the Licensee to the Regulatory Body, along with additional information as provided in Chapter “Accident analysis” of SAR.

### 4.2. **Leningrad NPP-2**

#### 4.2.1. *Findings about PHRS SG*

experimental validation or calculations of PHRS SG capacity (test rig /mockup experiments data).

computational analysis does not include information about closing relations, drag coefficients, etc. As a result, it is not possible to assess correctness of calculation results.

reliability analysis of PHRS SG is not fully adequate: there is no information about the values for probability of system components failures used while the analysis.

it is not shown by the licensee what signals and devices will be used to add the water inventory in emergency heat removal tanks after 24 hours of PHRS SG operation.

#### 4.2.2. *Findings about containment PHRS*

experimental validation or calculations of containment PHRS capacity (test rig /mock-up experiments data).

reliability analysis of containment PHRS is not fully adequate: there is no information about the values for probability of system components failures used while the analysis.

it is not shown by the Licensee what signals and devices will be used to add the water inventory in emergency heat removal tanks after 24 hours of Containment PHRS operation (it is a common issue for PHRS SG and containment PHRS as they use one tank as water source).

#### 4.2.3. *Current state*

The safety review shows that the PSAR submitted by the licensee is incomplete, however, the revealed shortcomings are not critical and can be rectified in further stages of design realization. The preliminary version of FSAR is under consideration now.

## 5. **CONCLUSION**

Today passive safety systems are one of the important elements (along with active systems) of defence-in-depth of NPPs and provide significant contribution to the safety of the NPP, especially in case of the accidents involving SBO and loss of UHS. In this regard, an important issue is assessing their compliance with existing regulatory requirements, as well as the issue about necessity of developing special regulatory requirements for their assessment.

The experience of safety review of new passive systems has shown that the available regulatory requirements are sufficient to assess their safety and the effectiveness of their performance of safety functions. At the same time, the main attention should be paid to the verification of sufficiency and completeness of the justifications (experimental and calculated) of these systems.

In addition, an important issue that should remain in the sphere of the regulator's attention is the evaluation of the experience of operating passive systems (the presence of failures, test results, the absence of negative influence on the operation of other systems), the results of which, as expected, will be received and included in the SAR within the next years.

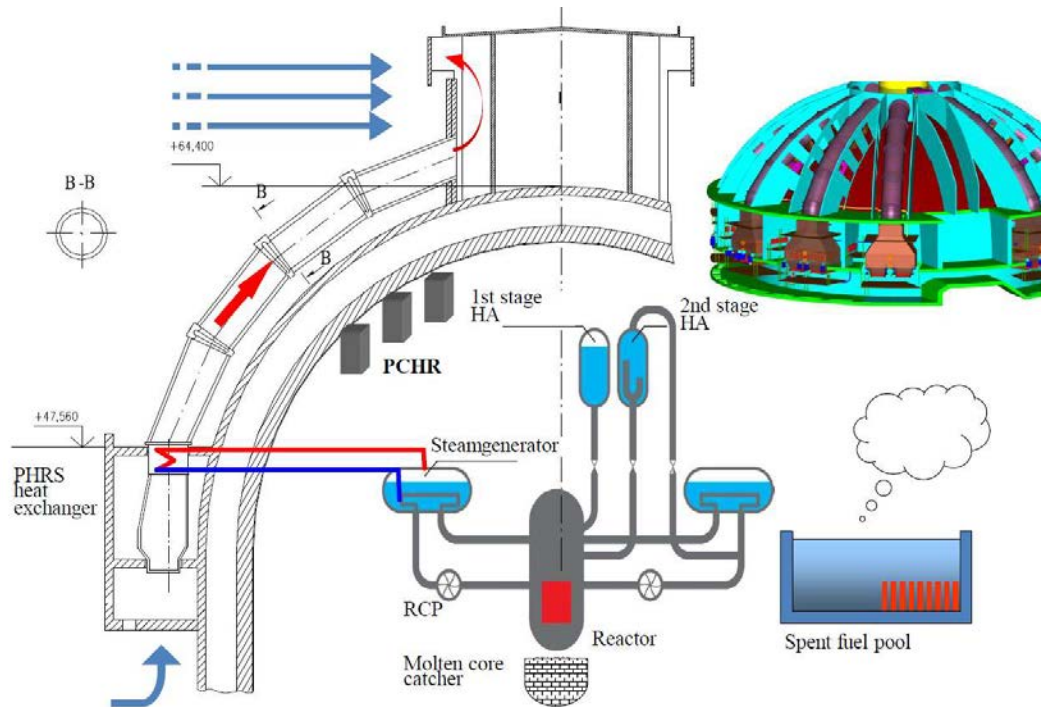
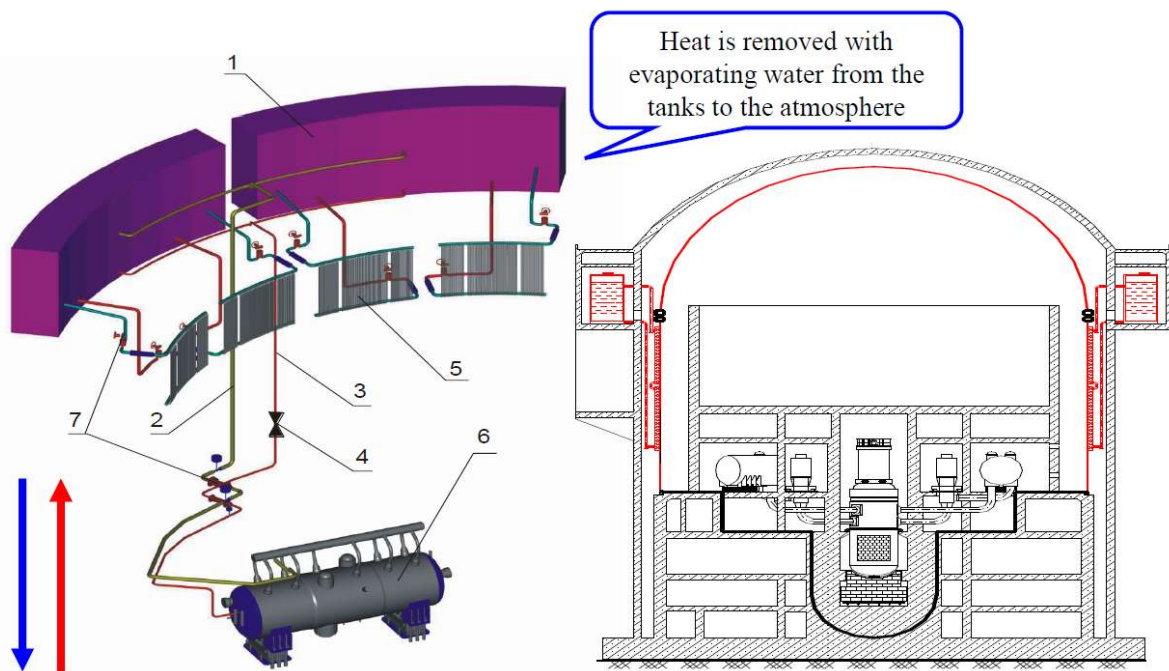


FIG. 1. Configuration of passive safety systems. Novovoronezh NPP-2.



1 – tank; 2 – steamlines; 3 – condensate lines; 4 – SG PHRS valve;  
5 – CPHRS heat exchangers; 6 – Steam generator; 7 – Cut-off valve

FIG. 2. Configuration of passive safety systems. Leningrad NPP-2.

## REFERENCES

- [1] General safety provisions for nuclear power plants. Federal standards and rules in the field of use of atomic energy. NP-001-15, ROSTECHNADZOR, Moscow (1995).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of nuclear power plants. Design. IAEA Safety Standards Series No. SSR-2/1 (Rev. 1). IAEA, Vienna (2016).
- [3] Booklet for Novovoronezh NPP-2,  
[http://www.rosenergoatom.ru/resources/8166b5004aef9f04b6c0f7ec7604272f/broshure\\_nw\\_aep\\_site.pdf](http://www.rosenergoatom.ru/resources/8166b5004aef9f04b6c0f7ec7604272f/broshure_nw_aep_site.pdf)
- [4] The VVER today: evolution, design, safety,  
<http://www.rosatom.ru/upload/iblock/0be/0be1220af25741375138ecd1afb18743.pdf>
- [5] Recommendations in order of execution reliability analysis of systems and components of nuclear power plants important to safety and their functions. Regulatory guide, RB-100-15, ROSTECHNADZOR, Moscow (2015).
- [6] Nuclear safety rules for reactor installation of nuclear power plants. Federal standards and rules in the field of use of atomic energy, NP-082-07, ROSTECHNADZOR, Moscow (2007).
- [7] NP-006-98 (PNAE G 1-036-95). Requirements for the content of safety analysis report for nuclear power plants with VVER type reactors. Federal standards and rules in the field of use of atomic energy, ROSTECHNADZOR, Moscow (1995).
- [8] Draft NP-006-16. Requirements for the content of safety analysis report for nuclear power plants with VVER type reactors, [http://www.secns.ru/science/development/draft\\_regulatory\\_documents/](http://www.secns.ru/science/development/draft_regulatory_documents/)
- [9] Rules for arrangement and operation of nuclear power plant confining safety system. Federal standards and rules in the field of use of atomic energy, NP-010-16, ROSTECHNADZOR, Moscow (2016).
- [10] Rules for Design and Safe Operation of Equipment and Pipelines of Nuclear Power Installations. Federal standards and rules in the field of use of atomic energy, NP-089-15, ROSTECHNADZOR, Moscow (2017).
- [11] Safety review of operation of the Unit 1 of Novovoronezh NPP-2, put into operation after construction (DNP-5-3170-2016). SEC NRS, Moscow (2016).
- [12] Safety review of the construction of Unit 1 of Leningrad NPP-2 in regard with the adjustment of the PSAR (DNP-5-3465-2016). SEC NRS, Moscow (2016).
- [13] Common position addressing Fukushima-related issues. MDEP Design-Specific Common Position No VVER-01. VVER Working Group, 2017.

# DIGITAL I&C SYSTEMS

**Chairperson**

**K. LEE**  
WNA



## **A METHOD FOR EVALUATING DIGITAL CCF ACROSS AN INTEGRATED PLANT DESIGN**

S. SMALL

GE Hitachi Nuclear Energy  
Wilmington North Carolina, USA  
Email: shelby.small@ge.com

I. POPPEL

GE Hitachi Nuclear Energy  
Wilmington North Carolina, USA

### **Abstract**

Methods for evaluating the consequences of digital Common-Cause Failures (CCF) in a Nuclear Power Plant (NPP) primary protection systems are available and have been endorsed by nuclear safety authorities. However, it is difficult to find regulatory guidance defining acceptable methods for evaluating the consequences of digital CCF occurring in other types of systems, and on a plant-wide basis in an integrated fashion. Such methods are needed, given the scope of digital equipment contained in most new NPP designs. It is now common for the majority of a plant's normally operating control systems to be implemented in a single digital technology; a possible CCF concern because these systems have the potential to challenge the protection systems. Digital technology is also routinely "embedded" in mechanical systems and electrical distribution system components that did not traditionally contain digital elements. The paper outlines a methodology for a single, consolidated digital CCF evaluation across an integrated plant design, using the IAEA Defence-in-Depth concept as a framework supporting the evaluation. Emphasis is placed on the fundamental challenges facing an evaluation method of this scope, and the key assumptions regarding digital CCF which are needed in order to perform such an evaluation.

### **1. INTRODUCTION**

The issue of digital Common-Cause Failures (CCF) has become increasingly difficult to address from both a design perspective and a regulatory perspective. This trend is partly due to expansion of both the scope of digital technology in Nuclear Power Plants (NPPs) and the types of digital CCF to consider. The trend also results from the lack of a widely accepted, systematic method to evaluate the digital CCF phenomenon across an integrated plant design and conclude that the risk presented by the phenomenon has been adequately mitigated.

The purpose of the paper is to describe a method for evaluating digital CCF, across an integrated plant scope, which could serve as both a licensing and design basis for new NPP designs. Certain aspects of the digital CCF phenomenon which present particularly difficult situations for designers and analysts are identified. An evaluation method based on the concept of Defence-in-Depth (D-in-D), which addresses those problems, is outlined and its use in a pilot evaluation project is discussed.

### **2. THE CHALLENGES**

The fundamental challenges for any method which attempts to evaluate digital CCF on a plant-wide scale stem from two primary problems: the scope of digital equipment in a new NPP, and the fundamental nature of digital CCF itself. Each of these problems is discussed in the following sub-sections.

#### **2.1. Scope of Digital Equipment in New NPP Designs**

The current generations of new and advanced NPP designs are leveraging digital technology on a scale not seen in previous generations. It is easiest to associate digital technology with the plant's control and protection systems and with Human-Machine Interface (HMI) systems. However, the fact that digital technology has become integral to and embedded in other parts of the plant mechanical and electrical design cannot be ignored. Nuclear safety authorities have taken notice of this development and raised concern about the potential for digital CCF in these 'embedded' digital devices. For example, the United States Nuclear Regulatory Commission (US NRC) has stated:



*“In addition to I&C, examples of safety-related equipment that may use digital technology include emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, time-delay relays, and uninterruptible power sources...The key issue is that the increased use of embedded digital devices (EDDs) in safety-related equipment may increase a facility’s vulnerability to a CCF, or otherwise degrade equipment reliability that could adversely affect safety. Potential safety issues from using EDDs should be adequately addressed” [1].*

This means that digital CCFs can no longer be addressed by simply postulating CCF of a single Instrumentation & Control (I&C) system, and providing a diverse I&C technology to perform the same function as the failed I&C system. Consider for example the case where actuation of Emergency Core Cooling System (ECCS) pumps is needed, and a digital CCF prevents the pumps from starting. A solution which involves independent start signals to the ECCS pumps, generated by a diverse actuation system, does not address the possibility that the digital CCF which prevented the pumps from starting may have occurred in the pumps’ protective relays or power supply circuit breakers. This condition may be common to, and could defeat both the primary actuation logic and the independent, diverse actuation logic.

In addition to EDDs, concerns have been raised relative to normally operating primary plant control and HMI systems, and their potential CCF leading to plant transients which may be different than those traditionally included in a plant’s design basis accident analyses (e.g., simultaneous incorrect actions taken by rod controls, feedwater controls, turbine bypass controls, reactor pressure controls, etc.). The primary plant control functions are typically implemented in a single digital technology across the plant design. A ‘segmentation’ approach to these control systems can be used to implement functions in separate controllers, when those functions were assumed to fail separately in accident analyses. Segmentation introduces important differences between the separate controllers related to input signal trajectories and other potential CCF triggers, but the separate controllers are still comprised of the same digital technology and contain common software elements; at least on the surface, they appear to be subject to the same digital CCF.

Given the extent of digital technology throughout most new NPP designs, it is not practical to evaluate each digital component or even each digital ‘system’ individually across the entire plant design for vulnerabilities to digital CCF, and to somehow collect all of those results into a cohesive evaluation of plant-wide vulnerabilities to digital CCF. Such an approach might also miss vulnerabilities existing because of dependencies between two diverse systems which may rely on shared support systems. The support systems are also likely to be controlled digitally and could therefore fail due to digital CCF.

Instead, it is necessary to perform a digital CCF evaluation at the plant-level to account for the same technology being used across multiple control systems, for embedded digital technology in electrical and mechanical systems, and for dependencies which may exist between diverse digital systems through shared support systems. Because a plant-level evaluation will cover numerous instances of different technology types, it must be somewhat more abstract than would be expected for an evaluation performed specifically for a given digital component.

## **2.2. The Nature of Digital CCF**

A digital CCF can be generally defined as the simultaneous occurrence of identical failures in multiple, redundant digital components of the same technology platform. More specifically, a digital CCF requires the existence of a latent defect in multiple, redundant digital components; and a common triggering condition to which the components are all exposed, resulting in their simultaneous failure.

Because the defects leading to CCF are latent, they are by definition not known to the designer or analyst. If a defect is recognized in the design of a digital component, it is no longer latent and every effort is made to eliminate that defect from the design. Despite these efforts, CCFs are postulated to occur and require demonstration that they do not lead to unacceptable consequences.

To determine the plant’s response to a digital CCF and to demonstrate acceptable consequences, specific output states resulting from the CCF must be postulated. To postulate the output states, the nature of the defect leading to failure must be understood. If a potential defect can be identified and understood, then the design should be modified to remove the defect. However, if the defect is removed there is no CCF left to evaluate. It is a paradoxical situation from which there is no escape because of contradictory rules.

Any evaluation of a plant's response to digital CCF scenarios will be performed assuming output states that are not supported by a clear technical basis. Because there are endless imaginable CCF modes which could be postulated, and no real technical basis to support or deny their existence, it is necessary to establish reasonable boundaries for a digital CCF evaluation which allow it to have a finite scope, and avoid the impossible task of evaluating all combinations of all output states. Any achievable evaluation methodology must define a set of digital CCF modes to be included in the evaluation, and explicitly exclude others.

### 3. DEFINITION OF THE NEED

The international nuclear power community would benefit from the existence of a method to evaluate digital CCF which:

- Integrates evaluation of primary control systems, protection systems, and support systems including EDDs;
- Is fundamentally structured around a D-in-D concept, which is applicable to the complete plant scope and includes clearly defined lines of defence;
- Can be used to evaluate either an existing detailed plant design for demonstration of acceptability or a conceptual new plant design with the results used to derive specific requirements to be met by the detailed plant design;
- Is widely accepted as a sufficient licensing basis to demonstrate acceptable plant defences against a reasonable set of digital CCF scenarios (i.e., it does not attempt to bound all imaginable digital CCF scenarios).

It is difficult to find such a methodology defined and accepted internationally or even in any one region. Digital CCF issues carry significant regulatory risk for new NPPs. Unclear regulatory expectations coupled with inconsistent treatment of the topic between different regions can lead to multiple versions of different digital architectures for the same basic plant design; a situation which benefits no one. Overly conservative regulatory treatment of digital CCF can lead a designer to implement solutions which increase overall complexity of the design and introduce additional failure modes.

It may be awkward, initially, for nuclear safety authorities to endorse a method which is explicitly not designed to bound all imaginable digital CCF scenarios. However, this should be viewed similarly to a traditional design basis accident analyses which serves as a fundamental licensing and design basis for NPPs. In typical design basis accident analyses it is widely accepted that the analysis only assumes a single failure occurring among the equipment of the highest safety classification in conjunction with the event being analysed. In reality, there is no guarantee that only one single failure could occur in conjunction with a design basis event/accident. Why not require the analyses to consider two or three failures? The answer is simple. If a limit is not defined for cases to be analysed, there is no end to the analysis.

Similar to design basis accident analyses, evaluation of digital CCF must be performed with a clear boundary established to distinguish the scenarios which are in scope and those which are out of scope; otherwise an evaluation could never be successfully concluded.

### 4. OVERVIEW OF THE METHOD

This section outlines a methodology which could be used to perform digital CCF evaluation across an integrated plant design scope. The methodology was used as a pilot case to evaluate a NPP design which was certified by the U.S. NRC in the 1990's, but has not been constructed in the United States. The licensing basis design descriptions for that design were used as the exclusive source of information defining the plant's design. The descriptions of the evaluation methodology contained in this section are informed by experience gained during the pilot case evaluation.

#### 4.1. Establish D-in-D Concept

The first step in the method is to establish a D-in-D concept which forms the basis for the remainder of the evaluation activities. The five lines of defence [2] provide a useful framework for this purpose. The D-in-D

concept for the pilot evaluation included Defence Lines 2, 3, and part of 4. The IAEA lines of defence were translated into the U.S. regulatory and safety classification schemes and terminology as follows:

*Defence Line 2* contains those functions which attempt to control or stop a plant transient before any parameters reach a safety system actuation setpoint. If the Defence Line 2 functions are successful, initiation of a safety-related reactor trip or ESF function is not needed. The functions in Defence Line 2 are nonsafety-related.

*Defence Line 3* contains those functions which act to mitigate a design basis event by preventing fuel damage, assuring the integrity of the barriers to release, and placing the plant in a safe state. These functions include reactor trip and actuation of engineered safety features. The Defence Line 3 functions are needed when Defence Line 2 is not effective at intercepting a transient, when the transient is itself caused by a failure of Defence Line 2 functions, or when an event starts “beyond” the capabilities of Defence Line 2. The functions in Defence Line 3 are safety-related.

*Defence Line 4 (partial)* contains those functions which can place the plant in a safe state if the Defence Line 3 functions fail. The Defence Line 4 functions are nonsafety-related.

During the pilot evaluation, it was decided to express the remainder of the D-in-D concept in the form of requirement statements; primarily to support their direct use as acceptance criteria for the evaluation, but also to make the D-in-D concept as unambiguous as possible. The requirement statements were aimed at the ‘plant-level’, meaning that they were not specific to any system or function; instead, they focused on plant functions residing in a given line of defence. Examples of the types of requirements used to define the D-in-D concept for the pilot evaluation are:

- A CCF occurring in Defence Line 2, which impairs mitigation of a design basis event, shall be mitigated by functions in Defence Line 3.
- A CCF occurring in Defence Line 2, which causes a design basis event, shall be mitigated by functions in Defence Line 3, or by a combination of functions in Defence Line 3 and unaffected functions in Defence Line 2. The unaffected functions are determined in accordance with the section “CCF guidelines”. If a combination of Defence Line 2 and 3 functions is credited, then:
  - The credited functions in Defence Line 3 shall not depend on successful occurrence of the credited Defence Line 2 functions, and
  - It shall be confirmed that the design basis event cannot be caused by a digital CCF in support systems which would also render the credited defence line 2 functions ineffective.
- Defence Line 3 functions shall depend only on safety-related support systems;
- Defence Line 2 functions and Defence Line 4 functions shall depend only on nonsafety-related support systems.

Requirements related to diversity and independence between defence lines were also included. In total, 11 plant-level requirements were used to define the D-in-D concept for the pilot evaluation. It should be noted that the pilot evaluation had a scope limited to Defence Lines 2, 3, and part of 4; a D-in-D concept supporting a broader evaluation scope would naturally include more requirements.

## 4.2. Establish Evaluation Scope

The evaluation scope can be defined in terms of the initiating events, the plant systems, and the types of digital CCFs to be included. The pilot evaluation was performed with the following scope:

Plant Events: The evaluation included those design basis events in the plant’s licensing basis accident analysis which start from a full-power operational state, superimposed with a single digital CCF. The definition of included events indirectly defines the scope of defence lines which will be included. In the case of the pilot evaluation, the plant’s licensing basis accident analysis involved functions in defence lines 2, 3, and part of 4.

Plant Systems: The evaluation included primary systems and support systems. Primary systems were defined as those whose functions directly mitigate a design basis event, or whose failure can directly initiate a design basis event. Support systems were defined as electrical supply systems, cooling water systems, and HVAC systems whose failure could prevent mitigation of or initiate a design basis event, but only by way of causing a failure of a primary system which in turn directly affects a design basis event.

Digital CCFs: The pilot evaluation was intended to evaluate a reasonable set of CCF scenarios. It did not attempt to bound all imaginable digital CCF scenarios. Section 4.3 of the paper identifies the specific digital CCF modes which were included.

#### 4.3. Establish Digital CCF Modes and Guidelines

An evaluation of this type is only defensible if clear definition is given to the digital CCF modes which will be considered and how those modes are applied. The pilot evaluation included two CCF modes. A CCF resulting in no action or state change occurring when an action or state change should have occurred was defined as a ‘passive’ CCF mode and was included. A CCF resulting in action or state change occurring when the action or state change should not have occurred was defined as a ‘spurious’ CCF mode and was included.

The pilot evaluation explicitly excluded two other CCF modes. A CCF resulting in some, but not all, actions that should be taken for a given scenario being taken was defined as ‘partial’ CCF mode and was excluded. A CCF resulting in a specific and varied combination of output states across a digital technology platform, with no basis for the chosen combination beyond the fact that it would make the results of an event significantly worse than has previously been evaluated, was defined as a ‘deviant’ CCF mode and was excluded.

The pilot evaluation included the following guidelines to govern application of the included failure modes.

- When a spurious CCF is postulated, it is assumed that a single function acts when it should not. A single function includes all actions ordered on the basis of a single setpoint value. The guidelines regarding availability to credit other functions are as follows:
  - If the spurious CCF occurs in a safety-related technology platform, all other functions in that technology platform are assumed to fail as-is; they maintain their control outputs in the same state that existed immediately prior to occurrence of the CCF. Functions in a different safety-related technology platform are assumed to function normally and correctly;
  - If the spurious CCF occurs in a nonsafety-related technology platform, all other functions in the same control segment are assumed to fail as-is; they maintain their control outputs in the same state that existed immediately prior to occurrence of the CCF. Functions in different control segments can be assumed to function normally and correctly, even if they are in the same technology platform. Functions in a different nonsafety-related technology platform are assumed to function normally and correctly.
- When a passive CCF is postulated, it is applied on a technology platform-wide basis. The guideline regarding availability to credit other functions is the following, regardless of whether the CCF occurs in a safety-related or nonsafety-related technology platform;
  - All functions in the technology platform should be assumed to fail as-is; they maintain their control outputs in the same state that existed immediately prior to occurrence of the CCF.

For spurious CCF modes, the decision to assume a ‘failed as-is’ state for the rest of the functions in the control segment or in the same technology platform is a conservative scheme to isolate the effects of the failed function, and to prevent taking credit for the same digital equipment suffering the CCF. It is just as likely that other functions performed by the equipment, which spuriously actuated a function, would be performed correctly.

Also, specific requirements were generated around establishing a degree of independence between different control segments to support the concept of limiting a spurious CCF to one control segment at a time.

#### 4.4. Establish Assumptions

Two types of evaluation assumptions need to be established; methodology assumptions and design assumptions. Consistent with other types of ‘beyond design basis’ analyses, best-estimate (realistic) methodology assumptions were used for the pilot evaluation. Examples of these assumptions include setting the initial power conditions for events to 100% as opposed to the more conservative 102% used in the licensing basis accident analysis. Offsite power remains available during all events except those where loss of power was the event initiator and no additional failures impacted event mitigation beyond the digital CCF being evaluated.

Design assumptions were established when some aspect of the design was not explicitly defined in the licensing basis or was generally defined but not in enough detail to support the evaluation. These types of assumptions are needed when a conceptual design is being evaluated. However, it would not be necessary if an as-built design was being evaluated. In the pilot evaluation, design assumptions were always followed with a specific design requirement intended to assure that the detailed plant design would be consistent with the design assumptions.

The methodology assumptions were established prior to starting the evaluation and design assumptions were added throughout the evaluation as they became necessary.

#### **4.5. Establish Acceptance Criteria**

The pilot evaluation took advantage of well-formed requirements used to define the D-in-D concept to form the core of the evaluation's acceptance criteria. If the requirements were met, the results were acceptable. The main way that the D-in-D concept requirements needed to be augmented, to support their use as acceptance criteria, was by providing definition of what constitutes successful mitigation of an event superimposed with a digital CCF. These criteria were stated in terms of integrity of coolant boundary and/or containment, and in terms of radiological release values at the site boundary. It is important to note that due to the low probability of CCF occurrence the radiological release values can be relaxed from those used in the accident analyses. These criteria can differ by region, and different values can be used within the framework of the digital CCF evaluation method without adversely affecting the overall methodology.

#### **4.6. Evaluate Support Systems**

The support systems are evaluated by creating plant-wide 'architectures' of the support systems, and then evaluating those architectures against the requirements of the D-in-D concept which are specific to support system functions. Evaluation of the support system functions is performed on a 'generic' basis; meaning that digital CCF in the support systems is not explicitly considered against each design basis event, because the support systems are required to function during all design basis events. Evaluation of the support systems concludes:

- A digital CCF which impairs a support system does not adversely affect primary functions in adjacent defence lines;
- Any transients which could be caused by support system CCF can be mitigated within the established acceptance criteria.

#### **4.7. Evaluate Primary Systems**

Evaluation of the primary system functions is performed on an event-by-event basis for each event included in the scope of evaluation. First, the functions credited for mitigation of an event in absence of CCF are identified. Then, the CCF guidelines (addressed in section 4.3) are used to postulate two types of digital CCFs.

- CCF which could impair the credited mitigation functions;
- CCF which could cause the event.

For both cases, functionality which is not affected by the CCF and which can mitigate the event is identified and mitigation of the event using this functionality is assessed against the acceptance criteria. The evaluation of an event concludes when the plant is in a stable, controlled condition with the critical safety functions relevant for that event being maintained. If such a plant state cannot be achieved or if acceptance criteria is not met, then a vulnerability is identified.

#### **4.8. Summarize Vulnerabilities**

Throughout performance of the pilot evaluation, when a vulnerability was discovered it was described in detail within the context of the related event. As the size of the evaluation document increased, it became evident that a collection and summary of all discovered vulnerabilities was needed, or else it was difficult to locate specific vulnerabilities of interest. At the conclusion of the pilot, the 'vulnerability summary' section was extremely useful for communication of results to project and design managers. It was also a good tool to use for identification of similar vulnerabilities from across the evaluation when considering options to address the vulnerabilities.

### **5. CONCLUSIONS**

A widely accepted methodology to evaluate digital CCF across an integrated plant scope is needed to address the ever-increasing inclusion of digital technology into new NPP designs. Such evaluations should be performed at the plant-level, rather than at the level of individual systems or components. A pilot evaluation of

this type was performed with a scope corresponding to IAEA Defence Lines 2, 3 and part of 4. However, it was designed to be scalable to include a larger set of events or CCF failure modes, if desired. The methodology can be used against a detailed plant design to demonstrate acceptability of the design, or against a conceptual plant design to set requirements which, if met, will assure acceptability of the detailed plant design.

The international regulatory community should consider cooperating to endorse a methodology of this type to support the standardization of plant designs across regions. Such standardization improves:

- Safety through shared operating experiences and minimalization of design variants (reducing risk of design errors;
- Cost competitiveness of nuclear power generation technologies.

## **REFERENCES**

- [1] NUCLEAR REGULATORY COMMISSION, Embedded Digital Devices in Safety-Related Systems, Regulatory Issue Summary 2016-05, Washington, DC (2016).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Specific Safety Requirements No. SSR/1 (Rev. 1), IAEA, Vienna (2016).

© GE-Hitachi Nuclear Energy Americas LLC, published under licence by IAEA, 2017

# DEVELOPMENT OF A METHOD FOR THE ASSESSMENT OF MODERN I&C SYSTEM ARCHITECTURES WITH REGARD TO FAILURE EFFECTS

C. MUELLER, J. PESCHKE, E. PILJUGIN  
 Gesellschaft fuer Anlagen- und Reaktorsicherheit (GRS) gGmbH  
 Cologne, Germany  
 Email: christian.mueller@grs.de

## Abstract

Due to the reconstruction of new nuclear power plants (NPPs) and the retrofitting of existing facilities, more and more digital I&C systems are used for safety-important functions worldwide in NPPs. The structure, operation, and communication of digital I&C systems are strongly influenced by the implemented automatic failure detection and handling procedures (e.g. correction of certain failure types). Therefore, a new method for the sensitivity analysis and assessment of different I&C architectures has been developed to investigate the dynamic behavior of those systems in case of external errors. The paper presents results of the sensitivity analysis for some typical example architectures showing that this method can support the verification and validation activities on the design and operation of digital I&C systems at an early stage.

## 1. INTRODUCTION

More and more digital I&C systems are used for safety-important functions worldwide in NPPs. In general the design of these I&C systems can be implemented on the basis of different technologies, architectures, and platforms, e.g.

- AREVA Teleperm XS (e.g. EPR reactor design, modernization projects in several NPPs: Bohunice NPP, Paks NPP);
- Rolls-Royce Spinline™ (e.g. French NPPs, Dukovany NPP);
- CommonQ/Advant AC160 ABB-System (e.g. AP1000 reactor design).

Based on failure mode and effect analysis (FMEA) [1], fault tree analysis (FTA) [2], and pseudo semi-Markov processes [3] a method for the assessment of modern I&C system architectures with regard to failure effects is being developed at GRS. Therefore, several typical modern architectures have been modeled taking into account specific characteristics of software-based safety-related systems. These model systems are used to develop and validate the new method.

## 2. ANALYSIS

### 2.1. Model systems

For the development and validation of the method for the sensitivity analysis, a number of model systems with increasing complexity are used. All model systems are essentially composed of three different types of units: acquisition units (AUs), processing units (PUs), and voting units (VUs) (Fig. 1 - Fig. 2).

The AUs receive analogue input signals from the transducers (e.g. pressure measurements - "P"), which are monitoring the relevant process parameters for the I&C function. The AUs digitize and subsequently transmit these values via the communication network to the processing units (PUs) as data telegrams. The transmitted signal is marked with a flag. If a signal is detected as faulty, the flag is set to "1" (self-signaling failure ("SF")). If the flag is set to "0", it can be either a true signal ("OK") or a non-self-signaling failure ("NSF").

Inside the PUs the valid signals (flag "0") coming from the AUs are sorted in ascending order and the second maximum is selected from them. If some input signals have self-signaling failures (flag "1"), the second maximum is chosen only from the remaining valid signals (flag "0"). If all but one signal coming from the AUs are flagged with "1", the remaining input signal is used directly as "second" maximum. The second maximum is then compared with a limit value and, if necessary, a binary control signal is generated and forwarded to the VUs. Again, the detected failures of the PUs or of the communication network between the PUs and the voting units (VUs) are marked with a flag "1" and are therefore recognized as invalid signals.

In the VUs, the binary signals from the PUs are evaluated by means of an n-out-of-m voting and, if necessary, a control signal for a component (e.g. motor – “M”) is formed. If only one or two valid inputs are available, the VUs internally switch to a 1-out-of-2 voting so that a single valid signal is sufficient to form a trigger signal. The output signals of the VUs to the analog logic (AL) do not contain error detection information, but self-signaling failures are reported and can be repaired if necessary.

The AL again performs an n-out-of-m voting (as there may be several VUs in an individual model system) and then passes the control signal to the component.

In addition, the following assumptions are made:

- The communication between units is carried out via networks. It is assumed that all hardware failures in the communication networks are always detected and they are therefore always self-signaling. For this reason, the failure rates of the communication paths (for example, between AUs and PUs) are taken into account directly in the failure rates of the corresponding signal-sending components (for example, self-signaling failures of AUs).
- Non self-signaling failed AUs output the minimum possible value.
- Non self-signaling failed PUs output a logical “0”.
- Failed VUs output a logical “0”.
- The software of the AUs, PUs, and VUs is not modeled explicitly so far and the considered failure rates were determined initially only by the possible hardware failures [4].
- Measuring devices, power supplies and interfaces of the I&C system are not explicitly taken into account in the models.

The simplest model system (A222, Fig. 1) consists of two VUs, two PUs and two AUs. The next more complex model systems are A333 (three VUs, three PUs and three AUs, Fig. 3) and A133 (one VU, three PUs and three AUs, Fig. 1). The model system A133B133 (Fig. 4) is composed of two systems, one of the type A133 and one of the type B133. In this case, a distinction is made between diverse sub-systems ( $A \neq B$ ) and non-diverse sub-systems ( $A = B$ ).

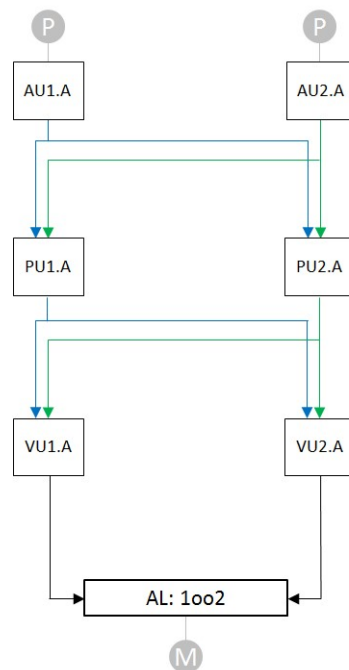


FIG. 1. Model system A222.



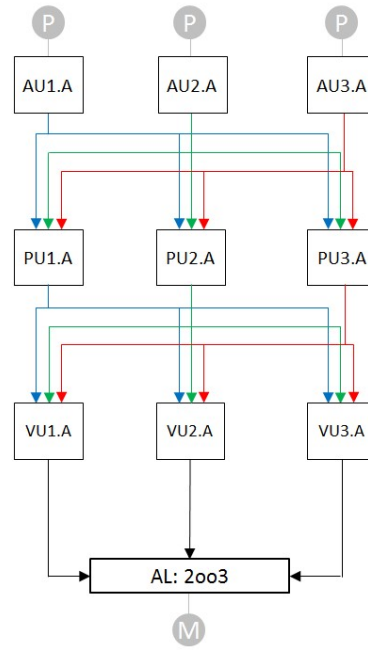


FIG. 2. Model system A333.

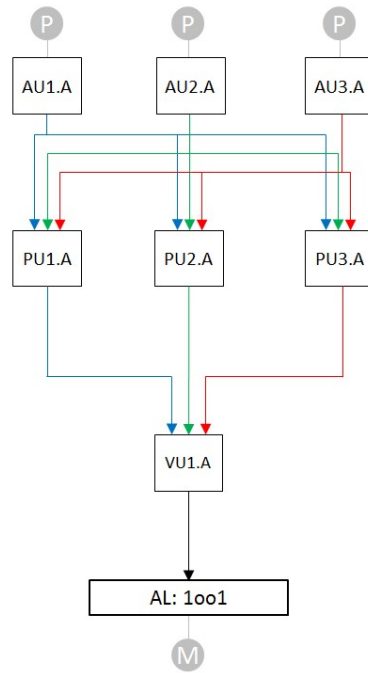


FIG. 3. Model system A133.

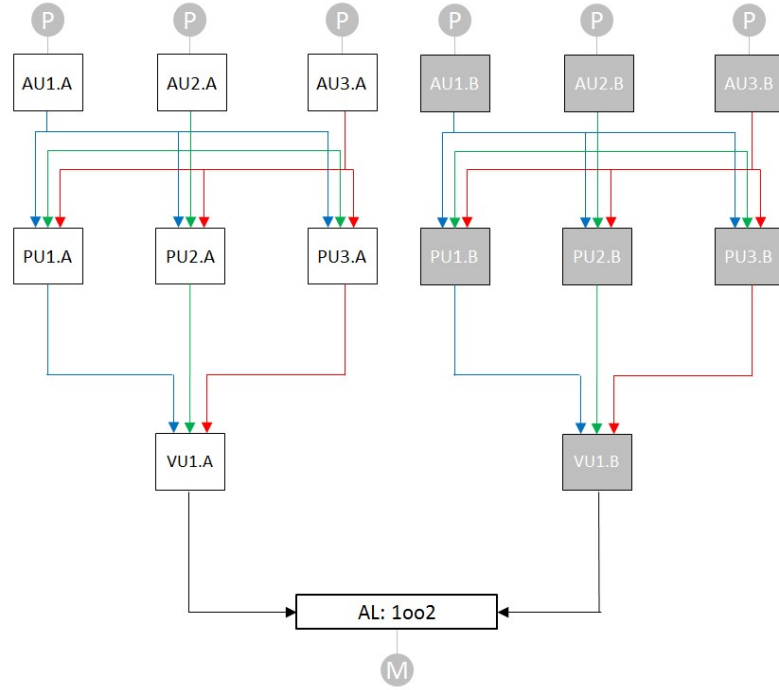


FIG. 4. Model system A133B133. The sub-systems can be either diverse ( $A \neq B$ ) or not ( $A = B$ ).

The system A2MC(1)33 (Fig. 5) consists of two VUs (each with a single master-checker sub-unit), three PUs and three AUs and the system A2MC(2)44 (Fig. 6) consists of two VUs (each with two master-checker sub-units), four PUs and four AUs.

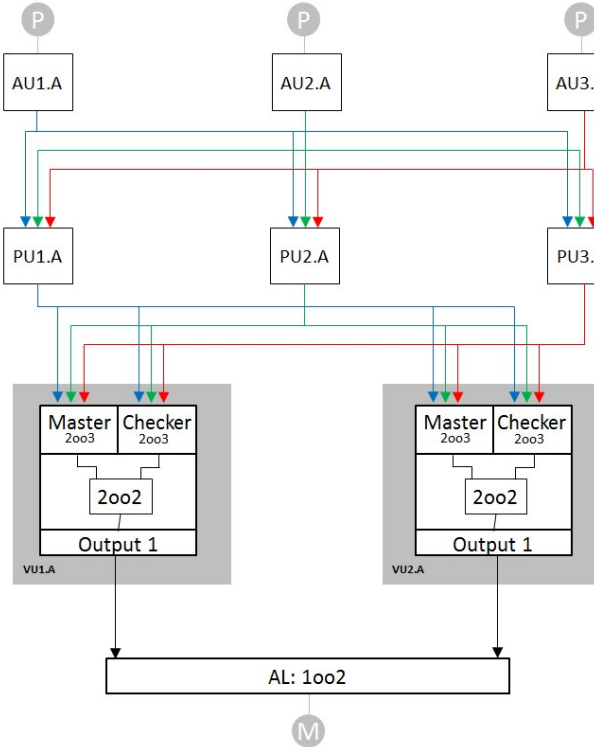


FIG. 5. Model system A2MC(1)33.

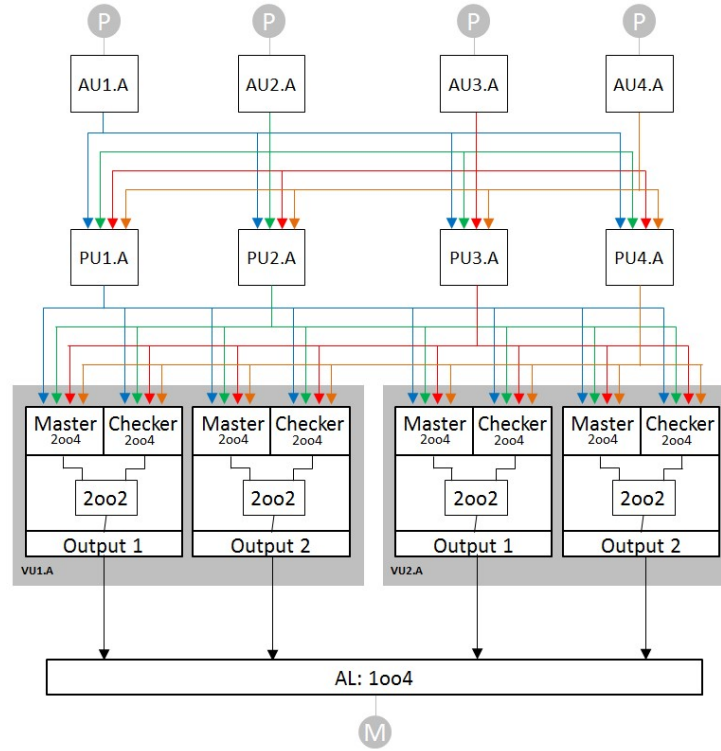


FIG. 6. Model system A2MC(2)44.

For the analysis of the model systems a mission time of one year was chosen and the failure rates for the respective components (AUs, PUs, VUs, Table 1) within all models were determined from the model described in [4] using RiskSpectrum PSA [5]. It was assumed that self-signaling failures are repaired within eight hours and that non-self-signaling failures are detected in weekly rotating inservice inspections of the redundancies (the AL being respectively assigned to the redundancy 1 in all model systems) and then repaired within eight hours, too. In addition, it was assumed that 2.5 % of the non self-signaling failures of a component type (e.g. AUs) and further 2.5 % of non self-signaling failures of all components of a sub-system (a diversity, e.g. “A”) are CCFs (which are detected by the inservice inspections in any redundancy).

TABLE 1. FAILURE RATES (FR) OF COMPONENTS

	Failure Rate	Remarks
FR AL NSF	$1\text{E-}10\text{ h}^{-1}$	
FR AU SF	$2,09832\text{E-}05\text{ h}^{-1}$	including communication with PUs
FR AU NSF	$8,26472\text{E-}08\text{ h}^{-1}$	
FR PU SF	$1,57295\text{E-}05\text{ h}^{-1}$	including communication with VUs
FR PU NSF	$8,26472\text{E-}08\text{ h}^{-1}$	
FR VU SF	$6,97175\text{E-}06\text{ h}^{-1}$	
FR VU NSF	$8,26472\text{E-}08\text{ h}^{-1}$	
FR AU CCF	$2,17493\text{E-}9\text{ h}^{-1}$	CCF of all AUs
FR PU CCF	$2,17493\text{E-}9\text{ h}^{-1}$	CCF of all PUs
FR VU CCF	$2,17493\text{E-}9\text{ h}^{-1}$	CCF of all VUs
FR ALL CCF	$2,17493\text{E-}9\text{ h}^{-1}$	CCF of all components of A

For the VUs of the two model systems A2MC(1)33 and A2MC(2)44, different failure rates apply due to their modified internal structure (see Fig. 5 and Fig. 6). These failure rates were determined in an adapted version of the model described in [4]. In particular, the master-checker-configuration causes all single failures of the VUs to be self-signaling (SF), but all other failure rates remain the same (Table 2).

TABLE 2. FAILURE RATES (FR) OF COMPONENTS (VU-SUB-UNITS WITH MASTER-CHECKER-CONFIGURATION)

	Failure Rate	Remarks
FR AL NSF	1E-10 h <sup>-1</sup>	
FR AU SF	2,09832E-05 h <sup>-1</sup>	including communication with PUs
FR AU NSF	8,26472E-08 h <sup>-1</sup>	
FR PU SF	1,57295E-05 h <sup>-1</sup>	including communication with VUs
FR PU NSF	8,26472E-08 h <sup>-1</sup>	
FR VU SF	1,0288E-05 h <sup>-1</sup>	no NSF due to Master-Checker
FR AU CCF	2,17493E-09 h <sup>-1</sup>	CCF of all AUs
FR PU CCF	2,17493E-09 h <sup>-1</sup>	CCF of all PUs
FR VU CCF	2,17493E-09 h <sup>-1</sup>	CCF of all VUs
FR ALL CCF	2,17493E-09 h <sup>-1</sup>	CCF of all components of A

## 2.2. FMEA

First of all, an FMEA was carried out for all model systems. Since each signal from each unit of a level (e.g. all AUs) is transmitted to each unit of the subsequent level (e.g. to all PUs, see Fig. 1 – Fig. 6) within all model systems, the results of the FMEA can be presented in separate tables for each level. Tables 3-6 show this representatively for the model system A133.

TABLE 3. OUTPUT SIGNALS OF AL OF THE MODEL SYSTEM A133

AL (1oo1)
Output, Quality
1, OK
0, NSF

The analog logic (AL) is not part of the digital I&C system, therefore failures can only be non-self-signaling (Table 3). The output of the AL also depends on the input signals coming from the voting unit VU1.A, e.g. a non-self-signaling failure (NSF) of the VU1.A leads to a NSF of the output of the AL (Table 4).

TABLE 4. OUTPUT SIGNALS OF VU1.A OF THE MODEL SYSTEM A133

VU1.A	AL (1oo1)
Output, Quality	Flag      Output, Quality
1, OK	0      1, OK
0, SF	1      0, SF*)
0, NSF	0      0, NSF

\*) the transferred signal to the AL does not contain error detection information, but self-signaling failures of VU1.A are reported and can be repaired.

This scheme can be transferred analogously to the other components. For example, line 1 of Table 5 can be read as following: If the output signals of the three PUs (PUx.A, x = 1, 2, 3) are correct and valid (“1, OK”), the VU1.A has three valid inputs (“1; 1; 1”, flag “0”). Therefore the 2-out-of-3 voting (“2oo3”) leads to a correct output of the VU1.A (“1, OK”) if the VU has not failed itself.

TABLE 5. OUTPUT SIGNALS OF PUX.A OF THE MODEL SYSTEM A133

PU1.A		PU2.A		PU3.A		VU1.A		
Output, Quality	Flag	Output, Quality	Flag	Output, Quality	Flag	Valid Inputs (Flag 0)	Voting	Output, Quality
1, OK	0	1, OK	0	1, OK	0	1; 1; 1	2oo3	1, OK
~, SF	1	1, OK	0	1, OK	0	1; 1	1oo2	1, OK
1, OK	0	~, SF	1	1, OK	0	1; 1	1oo2	1, OK
1, OK	0	1, OK	0	~, SF	1	1; 1	1oo2	1, OK
0, NSF	0	1, OK	0	1, OK	0	0; 1; 1	2oo3	1, OK
1, OK	0	0, NSF	0	1, OK	0	1; 0; 1	2oo3	1, OK
1, OK	0	1, OK	0	0, NSF	0	1; 1; 0	2oo3	1, OK
~, SF	1	~, SF	1	1, OK	0	1	1oo1	1, OK
~, SF	1	1, OK	0	~, SF	1	1	1oo1	1, OK
1, OK	0	~, SF	1	~, SF	1	1	1oo1	1, OK
~, SF	1	0, NSF	0	1, OK	0	0; 1	1oo2	1, OK
~, SF	1	1, OK	0	0, NSF	0	1; 0	1oo2	1, OK
0, NSF	0	~, SF	1	1, OK	0	0; 1	1oo2	1, OK
1, OK	0	~, SF	1	0, NSF	0	1; 0	1oo2	1, OK
0, NSF	0	1, OK	0	~, SF	1	0; 1	1oo2	1, OK
1, OK	0	0, NSF	0	~, SF	1	1; 0	1oo2	1, OK
0, NSF	0	0, NSF	0	1, OK	0	0; 0; 1	2oo3	0, NSF
0, NSF	0	1, OK	0	0, NSF	0	0; 1; 0	2oo3	0, NSF
1, OK	0	0, NSF	0	0, NSF	0	1; 0; 0	2oo3	0, NSF
0, NSF	0	0, NSF	0	~, SF	1	0; 0	1oo2	0, NSF
0, NSF	0	~, SF	1	0, NSF	0	0; 0	1oo2	0, NSF
~, SF	1	0, NSF	0	0, NSF	0	0; 0	1oo2	0, NSF
0, NSF	0	0, NSF	0	0, NSF	0	0; 0; 0	2oo3	0, NSF
~, SF	1	~, SF	1	0, NSF	0	0	1oo1	0, NSF
~, SF	1	0, NSF	0	~, SF	1	0	1oo1	0, NSF
0, NSF	0	~, SF	1	~, SF	1	0	1oo1	0, NSF
~, SF	1	~, SF	1	~, SF	1	~	~	0, SF

„~“ - any signal (self-signaling failed signals (SF) are not used any further)

Finally, Table 6 shows how the combinations of the output signals of the AUs affect the output signals of the PUs. Again, the first line is used to illustrate how this table can be read: If the output signals of all three AUs are correct and higher than the observed limit inside the PUs (“> limit, OK”) there are three valid (flag “0”) inputs into the PUs (“> limit; > limit; > limit”). So the 2nd maximum is above the limit and the PUs output correctly a logical “1” (“1, OK”).

TABLE 6. OUTPUT SIGNALS OF AUX.A OF THE MODEL SYSTEM A133

AU1.A		AU2.A		AU3.A		PUx.A (x = 1, 2, 3)		
Output, Quality	Flag	Output, Quality	Flag	Output, Quality	Flag	Inputs 2nd Max (Flag 0)	2nd Max	Output, Quality
> limit, OK	0	> limit, OK	0	> limit, OK	0	> limit; > limit; > limit	2nd Max	1, OK
~, SF	1	> limit, OK	0	> limit, OK	0	> limit; > limit	2nd Max	1, OK
> limit, OK	0	~, SF	1	> limit, OK	0	> limit; > limit	2nd Max	1, OK
> limit, OK	0	> limit, OK	0	~, SF	1	> limit; > limit	2nd Max	1, OK
< limit, NSF	0	> limit, OK	0	> limit, OK	0	< limit; > limit; > limit	2nd Max	1, OK
> limit, OK	0	< limit, NSF	0	> limit, OK	0	> limit; < limit; > limit	2nd Max	1, OK
> limit, OK	0	> limit, OK	0	< limit, NSF	0	> limit; > limit; < limit	2nd Max	1, OK
~, SF	1	~, SF	1	> limit, OK	0	> limit	Max	1, OK

AU1.A		AU2.A		AU3.A		PUx.A (x = 1, 2, 3)		
Output, Quality	Flag	Output, Quality	Flag	Output, Quality	Flag	Inputs 2nd Max (Flag 0)	2nd Max	Output, Quality
~, SF	1	> limit, OK	0	~, SF	1	> limit	Max	1, OK
> limit, OK	0	~, SF	1	~, SF	1	> limit	Max	1, OK
~, SF	1	< limit, NSF	0	> limit, OK	0	< limit; > limit	2nd Max	0, NSF
~, SF	1	> limit, OK	0	< limit, NSF	0	> limit; < limit	2nd Max	0, NSF
< limit, NSF	0	~, SF	1	> limit, OK	0	< limit; > limit	2nd Max	0, NSF
> limit, OK	0	~, SF	1	< limit, NSF	0	> limit; < limit	2nd Max	0, NSF
< limit, NSF	0	> limit, OK	0	~, SF	1	< limit; > limit	2nd Max	0, NSF
> limit, OK	0	< limit, NSF	0	~, SF	1	> limit; < limit	2nd Max	0, NSF
< limit, NSF	0	< limit, NSF	0	> limit, OK	0	< limit; < limit; > limit	2nd Max	0, NSF
< limit, NSF	0	> limit, OK	0	< limit, NSF	0	< limit; > limit; < limit	2nd Max	0, NSF
> limit, OK	0	< limit, NSF	0	< limit, NSF	0	> limit; < limit; < limit	2nd Max	0, NSF
< limit, NSF	0	< limit, NSF	0	~, SF	1	< limit; < limit	2nd Max	0, NSF
< limit, NSF	0	~, SF	1	< limit, NSF	0	< limit; < limit	2nd Max	0, NSF
~, SF	1	< limit, NSF	0	< limit, NSF	0	< limit; < limit	2nd Max	0, NSF
< limit, NSF	0	< limit, NSF	0	< limit, NSF	0	< limit; < limit; < limit	2nd Max	0, NSF
~, SF	1	~, SF	1	< limit, NSF	0	< limit	Max	0, NSF
~, SF	1	< limit, NSF	0	~, SF	1	< limit	Max	0, NSF
< limit, NSF	0	~, SF	1	~, SF	1	< limit	Max	0, NSF
~, SF	1	~, SF	1	~, SF	1	~	~	0, SF

### 2.3. FTA

The results of the FMEAs can be directly translated into fault trees. The figures 7 to 12 show the entire fault trees created with RiskSpectrum PSA for the model system A133 based on the FMEA results in the tables 3 to 6.

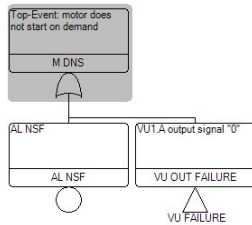


FIG. 7. Top-event in the fault tree for the model system A133: motor does not start on demand.

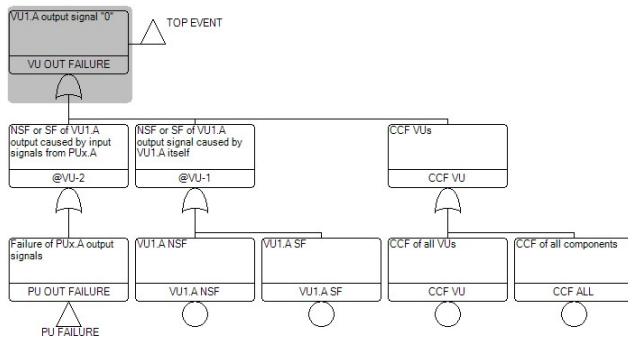


FIG. 8. Failures of VU1.A output signals in the fault tree for the model system A133.

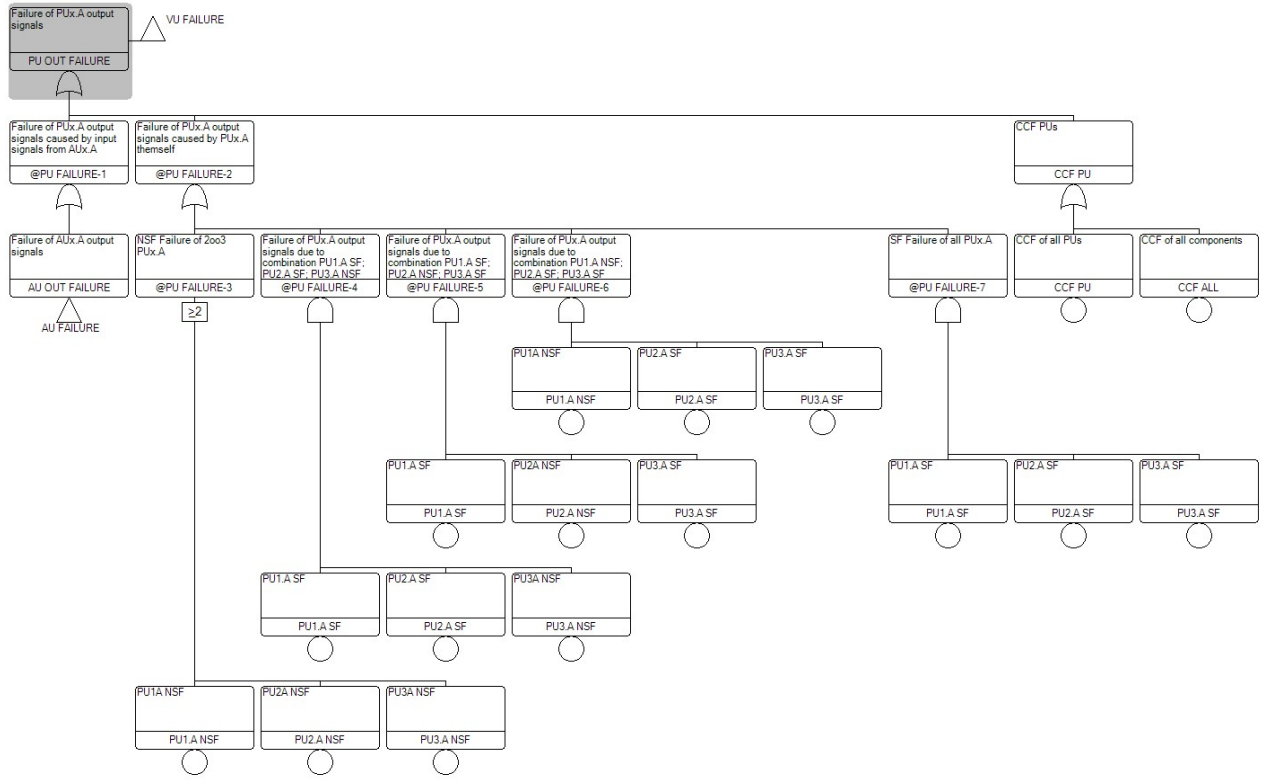


FIG. 9. Failures of PUs output signals in the fault tree for the model system A133.

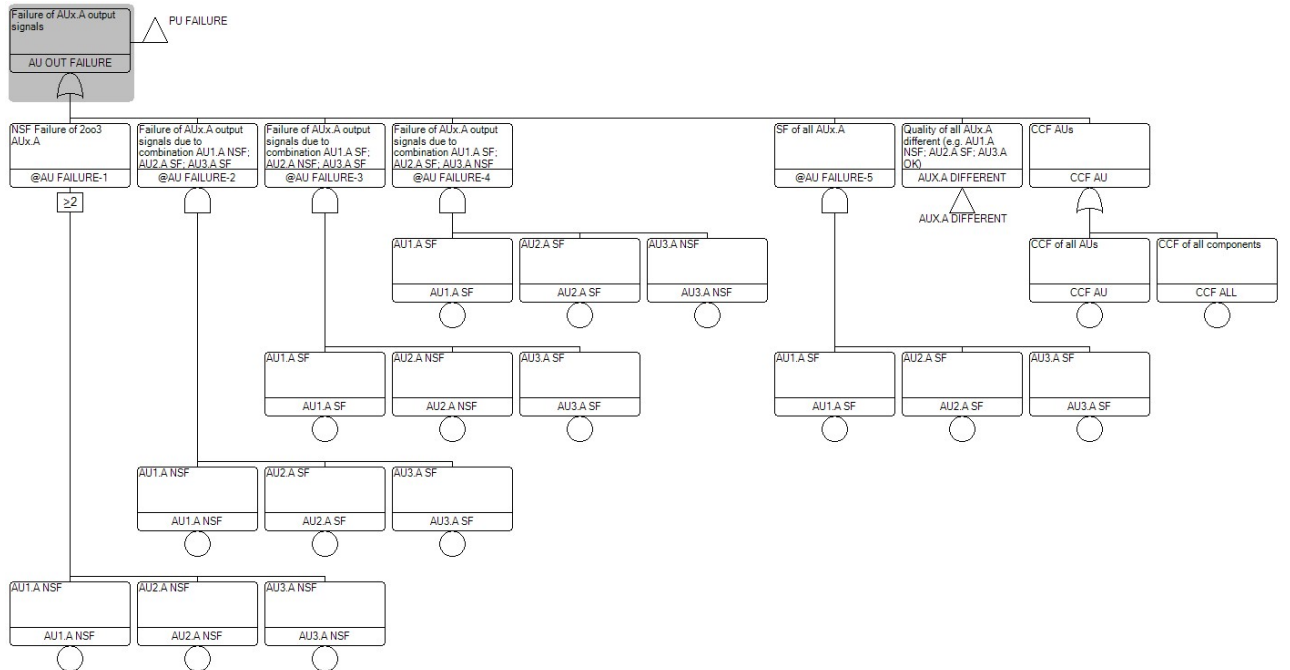


FIG. 10. Failures of AUs output signals in the fault tree for the model system A133.

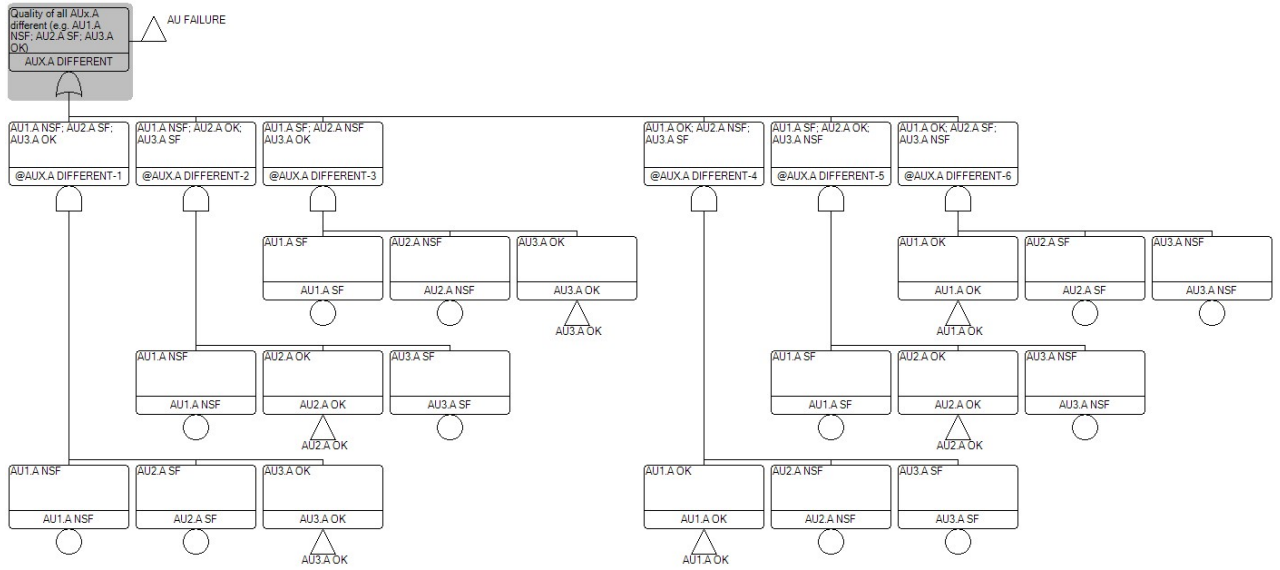


FIG.11. Failures of AUs output signals in the fault tree for the model system A133 (continued).

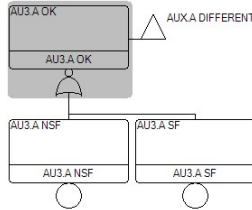


FIG.12. AU3.A is "OK" if it has no self-signaling failure and no non-self-signaling failure ("NOR").

## 2.4. Pseudo semi-Markov process

At present, the analyses are extended using semi-Markov processes. Semi-Markov processes describe the model systems by means of (time-dependent) transition graphs, which elements represent the overall state of the system and are connected with transition arrows with certain transitional probabilities. The work on this is ongoing.

## 2.5. Preliminary Results

Table 7 lists the probabilities of failures on demand for all model systems obtained by fault tree analyses. Since, for example, software failures have not yet been explicitly taken into account so far, the values given are not regarded as absolute probabilities. However, since the same characteristics were used for all model systems, the results are well comparable.

The model systems A222 and A133 have a comparatively low reliability. In case of A222, this is obviously a consequence of the relatively low degree of redundancy and in case of A133, this results from the use of only one single VU.

At a certain degree of redundancy, more redundant components do not lead to significantly higher reliability. Thus the failure probabilities of the more complex model systems A2MC(1)33 and A2MC(2)44 (with very high degrees of redundancy) lie in the same range as the failure probabilities of the model systems A333 and A133B133 (A=B). All are in the order of  $3E-06$ .

A significant increase in reliability can only be achieved by the use of diverse sub-systems. For example, the failure probability of the model system A133B133 (A≠B) is about two orders of magnitude less than the failure probability for the model system A133B133 (A=B).



TABLE 7. TOP-EVENT (FAILURE ON DEMAND) PROBABILITIES FOR THE MODEL SYSTEMS

Model System	Probability
A222	1,151E-04
A333	3,206E-06
A133	1,429E-04
A133B133 (A=B)	3,040E-06
A133B133 (A≠B)	5,483E-08
A2MC(1)33	3,154E-06
A2MC(2)44	3,020E-06

### 3. CONCLUSIONS

At present a method for the sensitivity analysis of failure effects on digital I&C systems is being developed at GRS. Therefore, a combination of failure mode and effect analyses (FMEA) and fault tree analyses (FTA) has already been applied to a series of model systems.

Although the project has not yet been finalized, the influence of diversity can already be compared with the effect of a mere increase in redundancy. Especially due to the influence of common cause failures (CCF) on the reliability of I&C systems, a significant increase of the reliability can only be achieved by adding diversity from a certain degree of redundancy.

The next step will be to combine the FTA with semi-Markov processes and the application of the complete methodology on all model systems. Through the variation of different I&C architectures and parameters, the influence of these architectures and parameters on the reliability of the I&C systems will be determined.

In conclusion, it can be noted that the developed methodology for the sensitivity analysis presented in this paper can support the verification and validation of digital I&C systems regarding potential safety deficiencies in design and operation even at an early stage.

### ACKNOWLEDGEMENTS

The authors want to acknowledge the support provided by the German Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety for funding the GRS development of the methodological approach to the sensitivity analysis of failure effects in modern digital I&C systems in the frame of the R&D project 3615R01343.

### REFERENCES

- [1] INTERNATIONAL ELECTRONICAL COMMISSION, Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA), IEC 60812:2006, Switzerland (2006).
- [2] NUCLEAR REGULATORY COMMISSION, Fault Tree Handbook, NUREG-0492, Washington, DC (1981).
- [3] ROEWKAMP, M., et al., Development and Test Application of Methods and Tools for Probabilistic Safety Analyses, Gesellschaft fuer Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-A-3558, Cologne (2010).
- [4] PILJUGIN, E., et al., Anpassung und Erprobung von Methoden zur probabilistischen Bewertung digitaler Leittechnik, Gesellschaft fuer Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-A-3258, Cologne (2004).
- [5] LLOYD'S REGISTER CONSULTING – ENERGY AB, RiskSpectrum PSA, Sweden, [www.riskspectrum.com](http://www.riskspectrum.com)

## **SPURIOUS ACTUATIONS IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS - EVALUATION FRAMEWORK**

I. GARCIA

U.S. Nuclear Regulatory Commission

Rockville, Maryland, U.S.A

Email: Ismael.Garcia@nrc.gov

### **Abstract**

When a digital Instrumentation and Control (I&C) system or its associated components produce an unintended operation, it is known as a spurious actuation. Spurious actuations could lead to unnecessary challenges to safety equipment, challenge the ability of safety systems to provide their intended functions, or place the plant in an un-analyzed state. There is arguably a lack of clear and sufficient regulatory guidance for assessing spurious actuations. In an attempt to address this guidance gap, this paper provides a generic framework for evaluating spurious actuations in digital I&C systems, components, or supporting systems that are important to safety. The framework provides a methodology for: (1) defining the scope of the evaluation including supporting assumptions; (2) providing options for excluding a spurious actuation from the evaluation; (3) assessing the potential consequences from the assessed spurious actuations; and, (4) defining a high-level acceptance criteria. The methodology discussed by this paper is not to be construed as a requirement, regulation, or acceptable guidance by either domestic or international regulators; instead, it is intended to serve as a potential foundation or technical basis to be used for developing clear and sufficient regulatory guidance for assessing spurious actuations in digital I&C systems.

### **1. INTRODUCTION**

There are two inherent safety functions that safety-related systems provide. The first function is to provide a trip or system actuation when plant conditions necessitate such action. The second function is to not trip or actuate when not required by plant conditions in order to avoid challenges to the safety systems and to the plant. When an I&C system or its associated components produce an unintended operation, it is known as a spurious actuation.

A spurious actuation can be caused by, but not limited to, single failures, common cause failures, maintenance testing errors, design errors, or missing requirements. Triggering events such as environmental effects and plant transients can also cause a spurious actuations. Design attributes such as independence and diversity would help mitigate the risk of a spurious actuation. Modern digital I&C systems can have interconnectivities, dependencies, and commonalities that can facilitate fault propagation thus leading to a potential spurious actuation of more than a single train of plant equipment. Therefore, a spurious actuation of multiple trains of plant equipment may be attributed to inadequate independence among redundant portions of I&C systems, lack of adequate diversity to address dependencies, or commonalities that result from functional or plant process configurations, which are not addressed during the design development or the equipment qualification phases.

Based on the potential adverse effects that spurious actuations could have on safety, their impact needs to be evaluated. Specifically, spurious actuations could lead to unnecessary challenges to safety equipment, challenge the ability of safety systems to provide their intended functions, or place the plant in an un-analysed state. Currently, there is arguably a lack of clear and sufficient regulatory guidance for assessing spurious actuations. Regulators abroad agree that guidance for evaluating spurious actuations is warranted given the increase use of digital I&C systems in new reactor designs and its safety implications. Such feedback is based on recent experience by domestic and international regulators with new reactor application reviews and operating plant issues as well as an examination of the regulatory requirements, relevant industry standards, and international documents.

## 2. EVALUATION FRAMEWORK

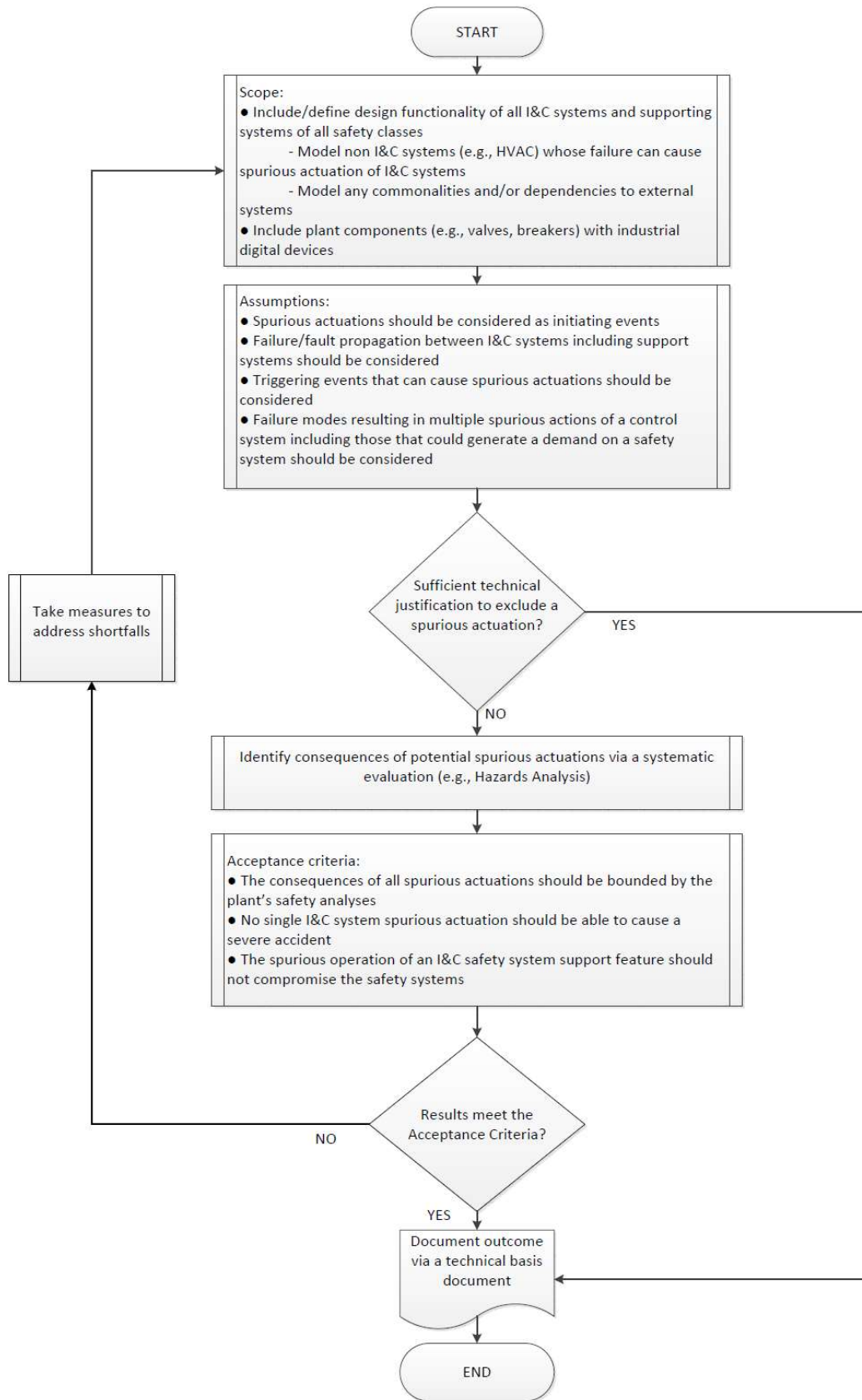


FIG. 1. Spurious Actuations in Digital Instrumentation and Control Systems – Evaluation Flowchart.

Fig. 1 above shows a generic framework for evaluating spurious actuations in digital I&C systems, components, or supporting systems that are important to safety [1]. As shown in Fig. 1, the framework provides a methodology for: (1) defining the scope of the evaluation including supporting assumptions; (2) providing options for excluding a spurious actuation from the evaluation; (3) assessing the potential consequences from the assessed spurious actuations; and, (4) defining a high-level acceptance criteria. Sections 2.1 and 2.2 below discuss some of the key takeaways from this generic framework. This paper does not prescribe a particular evaluation approach as there may be different approaches when performing the evaluation for the identification of the consequences of postulated spurious actuation(s) (e.g. system based, function based, component based or combination thereof). However, the approach taken for performing the evaluation of spurious actuations should be justified for suitability for the particular application.

A preliminary evaluation for spurious actuation should be performed during the early design stages of the I&C component, system or architecture. The results of the preliminary evaluation should be used to inform the I&C component, system and architecture design and should be validated during the later stages of the design development. The final results of the evaluation should be reviewed and re-evaluated when necessary. Examples of when such a review may be required include changes to the I&C components, systems, architecture or supporting systems, and mandatory periodic reviews.

## 2.1. Scope and Assumptions

Despite the fact that the methodology discussed herein is focused on spurious actuations in digital I&C systems, components, or supporting systems that are important to safety [1], the scope of the assessment should include the functionality of all I&C systems and supporting systems of all safety classes. Such a comprehensive assessment is necessary as there may be interconnections between I&C systems of different safety classes; thus errors in one redundant channel or division or lower class systems could cause the failure of another redundant channel or division or higher class systems. Ways in which control system faults, including multiple spurious faults, could generate a demand on a safety system should also be considered as they could lead to adverse safety conditions [2].

As part of the evaluation, the user should define the assumptions concerning the occurrence of multiple spurious actuations or spurious actions<sup>1</sup> in combination with independent postulated initiating events. The use of appropriate architectures and design attributes (e.g., independence and diversity) to (1) avoid the occurrence or (2) reduce its likelihood to an acceptable level of multiple spurious actuations or spurious actuations in combination with independent postulated initiating events might be used as a justification for exclusion as long as sufficient demonstration is provided [2]. A similar approach could be followed to eliminate a given spurious actuation occurrence from further consideration.

## 2.2. Assessment of Consequences and Acceptance Criteria

A systematic evaluation such as a Hazard Analysis should be used to assess the potential consequences of all postulated spurious actuations [3]. The evaluation should employ the use of analysis techniques that can assess the hazards introduced through interconnected digital systems and devices. The feedback paths enabled when the digital elements are networked could lead to the potential propagation of design flaws or any other unsafe interactions. The goal of the evaluation should be to ensure that the consequences of all postulated spurious actuations are bounded by the plant's safety analyses. In other words, if the potential effects of the spurious actuations do not invalidate or exceed the assumptions or results of the plant's safety analyses, then the potential consequences of a spurious actuations are bounded. Alternatively, the evaluation could identify the worst case spurious actuation and ensure that its consequences are bounded. A given spurious actuation of an I&C system or component(s) could be considered worst case if its potential consequences envelope those from other potential spurious actuations.

If the evaluation fails to meet the acceptance criteria, then the user should take hazards control measures to address the shortfall(s) [3]. For example, the user should evaluate the implementation of design attributes such as independence and diversity to avoid the occurrence, or to reduce the likelihood of a spurious actuation to an

---

<sup>1</sup> Unintended operation of an I&C system or component(s) that may result in a failure of some of the items important to safety to fulfil the actions required in response to a postulated initiating event [2].

acceptable level. Hazard control measures such as crediting of manual actions identified as a result of this evaluation should be an acceptable option for controlling identified hazards. Subsequently, the user should reassess the effects of the measures taken to address the shortfall(s) by repeating, as necessary, the evaluation framework shown in Fig. 1.

### 3. CONCLUSION

There may be different approaches when performing the evaluation of spurious actuation(s). This paper does not prescribe a particular approach but instead provides a sample framework for evaluating the consequences associated with spurious actuation. Nonetheless, the approach taken for performing the evaluation of spurious actuations should be justified for suitability for the particular application. The methodology discussed by this paper is not to be construed as a requirement, regulation, or acceptable guidance by either domestic or international regulators. Instead, it is intended to serve as a potential foundation or technical basis to be used for developing clear and sufficient regulatory guidance for assessing spurious actuations in digital I&C systems.

### ACKNOWLEDGEMENTS

This paper was derived from the ongoing work being performed by the Multinational Design Evaluation Programme (MDEP) Digital Instrumentation and Control Working Group (DICWG), which I have the honor and privilege to chair. For additional information concerning the MDEP DICWG visit: <https://www.oecd-nea.org/mdep/>.

### REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection, IAEA, Vienna (2007).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, SSG-039, IAEA, Vienna (2015).
- [3] MULTINATIONAL DESIGN EVALUATION PROGRAMME DIGITAL INSTRUMENTATION AND CONTROL WORKING GROUP, Common Position on Hazard Identification and Controls for Digital Instrumentation and Control Systems (2016), [https://www.oecd-nea.org/mdep/common-positions/MDEP\\_GCP-DICWG-10\\_HazardIDandControl.pdf](https://www.oecd-nea.org/mdep/common-positions/MDEP_GCP-DICWG-10_HazardIDandControl.pdf)

# UNCERTAINTY QUALIFICATION AND SAFETY MARGINS

**Chairperson**

**F. D'AURIA**  
Italy



## ON SOME CHALLENGES IN DEFINING AND USING DEFENSE IN DEPTH AND SAFETY MARGIN CONCEPTS, AS HIGHLIGHTED BY THE SAFETY IMPROVEMENT PROCESS

D. SERBANESCU  
Romanian Academy, Division of Logic, Models in Science  
Bucharest, Romania  
Email: dan.serbanescu1953@yahoo.com

### Abstract

The paper presents results on the evaluation performed by the author for the duration of two decades in Nuclear Power Plants (NPP) safety projects in a special set of cases. The focus is on the lessons learnt from the perspective of the safety decisions for NPP for almost four decades. The paper reflects some insights resulted from the author's participation in safety issues for the same national nuclear project for the last four decades and a prediction on the expected dominating issues in those cases for the next ten years. It was considered, that it is of interest to share with the international community the author's opinions on safety issues and its particular aspects, as they result based on the mentioned before experience.

### 1. INTRODUCTION

The paper presents some issues considered important in the safety decisions taken during the last three decades and on the evaluations going on for the safety decisions envisaged in the next decade, for the particular case of a national nuclear program and as defined by the author.

The safety issues that had to be solved and the safety decisions taken in the nuclear program mentioned under [1] and with the specific reported steps are largely presented in [1].

There were there were two types of possible approaches in the presentation of a particular experience for a specific case of a national nuclear program:

- By evaluation of the safety methods and detailed decisions taken for various complex safety related situation
- By presenting the summary of the lessons, in less formalized manner possible.

Due to the limitations of space for presentation of the first type the author will be presented in a format of a set of lessons learnt. However, the deterministic probabilistic approaches aside with the evaluation using decision theory methods are largely presented in [2] reflecting the national reports issued at the time of decisions and international presentations made by the author as representative of the national regulatory body under various IAEA events in the last 25 years.

Therefore, the following situation will be presented in a format of an expert opinion approach, (based on the reported experience and documents [2, 3]), as participant at safety decision process at national level and involvement in international projects in the last four decades. The goal of the paper presentation is to illustrate for a particular case, some challenges in safety. They were related to various aspects and also connected with the implementation of concepts like defense in depth and safety margin and decision making process in the licensing process. The case is related to a country that embarked on a nuclear NPP program four decades ago.

In 1976 Romanian leadership, advised by top national nuclear scientists, decided to embark on a nuclear program, by importing a Western type of technology and building a whole nuclear civil program for NPP. It was a rare action, if not the only one of this type at international level by that time, as Romania was in a different political team by that time.

However, it was not the first step in this direction, as five years before a Western technology type of reactor (TRIGA) was built and for that the US safety regulations were adopted. But by adopting US NRC type of regulations Romania had by the time of starting CANDU project a regulatory safety challenge, because the prescriptive type of regulations (considered in force for NPP, too) did have some points of difference with the Canadian licensing approach. Restart of the project after political changes underlined the expected possible licensing problems and were subject to regulatory decision on a case by case basis, while restructuring the regulatory pyramid at national level. This happened in an international context mainly guided by IAEA and EU safety documents. Therefore, the paper is based and directed exclusively by the safety notions and definitions



adopted at international level and the references in this paper are all based on them presenting only particular experience of their implementation in Romania (for details references [1, 3] may be consulted).

The expert evaluation and presentation of author's opinion for each case was formulated in an international context that is largely presented in [4]. In reference [4] there is the author's evaluation of some safety issues evolving during the years, connected also with the events at global level, not only NPP related directly and also with the major accidents that took place in NPP. The approach in [4] is the author's view on how the NPP technology evolved from its beginning to present times, with an accent on safety issues.

## 2. CASES AND OBJECTIVES OF THE EVALUATIONS

The paper presents the safety issues from an expert perspective that actively participated in the decision process of the licensing process on Cernavoda NPP, for the following cases:

Case A: Licensing process of Cernavoda NPP unit 1 and decisions on restart Cernavoda unit 2 construction, aside with the decision on conservation of units 3-5. This involved the period of completion of construction of unit 1, commissioning of unit 1 by an international consortium and first initial year of operation of unit 1. In unit 2 continuations of works for construction but at a slower pace. The period was 1993-1997.

Case B: Licensing of Cernavoda passing into a mature stage of operation and restarting of construction of unit 2. This period was 1997-2000.

Case C: Mature operation of unit 1 and first initial operation of unit 2. This period is from 2000-2010.

Case D: Preparation for refurbishment for unit 1 and evaluations on new generation IV type of research reactors to be built, preparations to restart activities for completion of units 3 and 4. Period is 2012-2017.

Case E: Foreseen period of refurbishment of unit 1, start of preparation of refurbishment for unit 2, possible commissioning of units 3 and 4, possible construction of new generation IV research reactor. Period is from 2017 on, with a projection on the next ten years.

The review includes a set of periods that cover a two-decade period in the NPP history. The following strategies for a period starting from safety reviews from 1990's and up today are defined (the evaluation of the status is related to the cases A-E and specific situation under presentation in the paper):

- S1 (Period 1 - Cases A, B and C) – During this phase the safety concepts are consolidated and recognized internationally in standard like format, defined as the first period. Vendors are adapting the initial safety philosophy to the changes required to fit the national regulations (of USNRC type) and a national licensing process organized like a regulatory project was defined. New set of regulations are under preparation, enveloping the experience gained. Interface and full implementation of safety approaches from IAEA, EU and Canada were used as guiding expertise. The first reports under Convention on Nuclear Safety are submitted and Romania is in preparation for aligning safety approaches to EU set of requirements.
- S2 (Period 2 Case D) – In this phase the safety concepts, national regulatory approaches were consolidated. Special issues were under research for advanced new generations of NPP and / or restart of units 3-4, as well as lifetime extension issues. Consolidation considered a certain optimism (specific to the “nuclear renaissance” period actually) and did not anticipate intense actions to review approaches to be adopted after Fukushima accident. During this period Romania became member of the EU and mature regulatory environment
- S3 (Period 3- Case E) – This is dominated by post Fukushima actions and events on safety. There is ongoing work (at international level reflected also at national level) on issues like independence of all the safety layers of the Defense in Depth (DiD) and the issues related to the extension of the Design Basis Accidents (DBA) in the format of Design Extended Conditions (DEC), that tackles the issues of Safety Margins.

## 3. RESULTS

As presented in the introduction, the method illustrated in this paper for evaluation of safety issues in each case is based on expert judgment, as a view of an expert directly involved in the process of licensing. A detailed systematic multi-criteria decision analysis (MCDA) approach of the cases is in [1].

### 3.1. Specific features of the inputs for decision for the evaluated cases

There were specific inputs that had to be considered for the safety decisions on cases A-E that actually governed the specifics of the safety related decisions, as follows:

For the period 1:

- The set of safety documents developed by the owner of the CANDU concepts at the level of the 1980's and later on with the updates from the Vendor and experience of other CANDU owners.
- Core Damage Frequency (CDF) and other risk metrics insights as per the PSA level 1 developed in Romania for Cernavoda NPP in the early 1990's and reviewed to a more mature state up to 2000.
- The probabilistic safety envelope of the CANDU concept defined originally by the Canadian designer in a set of Reliability Analyses (RA) and Safety Design Matrices (SDM).
- Results from the commissioning process of Unit1 and the intensive interface with IAEA and Canadian regulator.
- Regulatory experience gained after the licensing process of unit 1 and systematic review of the regulatory pyramid in order to document the new status.

For the period 2:

- The review of compliance with DiD and SM and of the postulated events (including possible extension of DBA list) were considered based on the experience from unit 1 and coordinated with international and CANDU owners evaluations.
- Design changes as implemented to consolidate the SM and the DiD layers in accordance with experience from CANDU community.
- A plant specific PSA level 1 for internal and external events completed and its use for operation and as risk monitor started.
- PSA level 1 becoming part of the required licensing safety documentation and used for current operation of units.
- PSA level 2 and severe accidents evaluations (Severe Accidents Management Guidelines – SAMG).
- Full scale Long Term Operation (LTO) and ageing programs.
- Develop and implement Periodical Safety Review (PSR).
- Implementation of risk management throughout all the plant processes – hardware and software and use of the elements of Risk Informed Decision Making (RIDM) for decisions on SM and DiD.
- Alignment to new EU safety directives and preparation for the first reports under it.
- Participation in international actions on review the DBA and adopt DEC concepts, with direct impact on national approach on DiD and SM for plants in operation and their long term perspective and for the restart of construction of units 3 and 4.
- Completed PSA level 2 and severe accidents evaluations review.
- Work on specific CANDU issues of refurbishment of an operating unit in order to extend the operating lifetime.
- Work on restarting a project of NPP after it was stopped and conservation assured for a long period of time.

For the period 3:

- Implementation full scale of LTO and specifics of refurbishment for unit 1.
- Continuation of alignment to new EU safety directives and preparation for the reports under it as per WENRA agreed guidelines.
- Final decisions and implementation on DEC for old and new units.
- Decisions on specifics of licensing for research reactors of generation IV.
- Preparations for shutdown and decommissioning of unit 1 and refurbishment for unit 2.

### 3.2. Main results

The main insights based on expert evaluations are in accordance with the detailed list and description of the MCDA tools used as an alternative to expert judgment as presented in [1]. Those insights illustrate some major aspects on SM and DiD, as well as on safety in general, and they are listed as perceived by the author:

On safety and safety programs in general:

- There is a high impact on the implementation work for regulating and self-regulating on safety if the nuclear program for a country has a first start, with a vendor from a country owning the concept. To make things more complicated the safety concepts of the owner itself and the community of that NPP type evolves from the moment the plant starts to be built to the moment it has to be regulated as an operating plant.
- It is of high priority to build and make operable a regulatory safety environment in an importing NPP country, as there is no substitute for the need to build the own national capabilities and human expertise.
- The importing country has a very difficult task to build and preserve the knowledge accumulated and the staff trained at the end of the initial process.
- NPP is an evolving technology, with all the implications of this classification and the evaluations of its major accidents (for details see [4]).

On specific safety issues, including DiD and SM:

- If the importing country of a NPP has initial regulatory framework having differences on safety issues (including the manner DiD and SM are considered) than there is a tremendous case by case work, that needs also international support in order to implement the best SM and DiD concepts for the new built.
- For the cases under periods 1 to 2 the paper underlines the fact that the conceptual framework considering SM and DiD came asymptotically to an equilibrium from the regulatory point of view, reflecting the maturity reached on safety issues at the national level.
- However this asymptotic level indicates in author's opinion on a possible resurgence of the more "traditional" deterministic evaluations in the future. This means that the trend of an increased role of intrinsic safety features, of using passive components improving human and organizational factors contribution to the safety evaluation is going to be maintained.
- The final safety decisions taken for all the cases were considered and are confirmed as solid conservative ones, while not putting a burden on the licensing process. However, the decision process was based on systematic evaluation of inputs, use of MCDA tools and international peer review and support.
- On the other side it is also noted that the change control in the era or post Fukushima changes becomes of highest priority for maintaining the initial designed set of SM and DiD layers. It might be that by avoiding cliff edge effects (CEE) for instance, future changes of post Fukushima type may endanger basic safety feature already existent in the initial basic design, in our opinion this is the best way how changes have to be made extremely carefully.

#### 4. CONCLUSIONS

The paper presents the evaluation performed in a specific case of NPP cases within a significant period for the lifecycle.

There are many insights from the practical experience of performing safety evaluation with the objective to check the level of compliance with safety requirements, protection in layers (DiD) and the level of available SM and hence to judge on the conservatism of the decisions taken. The cases are related to real situations and therefore experience could be of use for further similar cases.

The paper presents also some insights on the potential issues of concern in the safety evaluations, of which SM and DiD evolutions were considered dominant. However, it is mentioned that it should not be forgotten the fact that NPP is a technology and that SM and DiD approaches (for example if we take the interpretation proposed in [4]) are changing systematically and a continuous update is needed for the safety regulatory environment.

#### REFERENCES

- [1] SERBANESCU, D., A specific experience on some challenges in defining and using defense in depth and safety margin concepts, as highlighted by the safety improvement process, basic information for the paper submitted to IAEA for conference Topical Issues on Nuclear Safety, DOI: 10.13141/RG.2.1.4859.2488, IAEA, Vienna, Austria, 6-9 June 2017,  
[https://www.researchgate.net/publication/316542989\\_A\\_specific\\_experience\\_on\\_some\\_challenges\\_in\\_defining\\_a\\_n\\_d\\_using\\_defense\\_in\\_depth\\_and\\_safety\\_margin\\_concepts\\_as\\_highlighted\\_by\\_the\\_safety\\_improvement\\_process](https://www.researchgate.net/publication/316542989_A_specific_experience_on_some_challenges_in_defining_a_n_d_using_defense_in_depth_and_safety_margin_concepts_as_highlighted_by_the_safety_improvement_process)
- [2] SERBANESCU, D., <http://lu.linkedin.com/in/danserbanescu1953>

- [3] SERBANESCU, D., <http://independent.academia.edu/danserbanescu>;
- [4] [https://www.researchgate.net/profile/Dan\\_Serbanescu](https://www.researchgate.net/profile/Dan_Serbanescu)
- [5] SERBANESCU, D., Understanding major accidents – Shifting paradigms in safety and risk, Safety Summit Vienna 27-28 Sept 2011,  
[http://www.academia.edu/3763738/Understanding\\_major\\_nuclear\\_accidents\\_shifting\\_in\\_paradigms\\_for\\_safety\\_and\\_risk](http://www.academia.edu/3763738/Understanding_major_nuclear_accidents_shifting_in_paradigms_for_safety_and_risk)

## BEPU AND SAFETY MARGINS IN NUCLEAR REACTOR SAFETY

F. D'AURIA  
University of Pisa (DESTEC/GRNSPG)  
Pisa, Italy  
Email: f.dauria@ing.unipi.it

H. GLAESER  
Consultant,  
Eching, Germany

N. DEBRECIN  
University of Zagreb (FEEC)  
Zagreb, Croatia

### Abstract

Approaches like Best Estimate Plus Uncertainty (BEPU) and concepts like Safety Margins (SM) are well established in Nuclear Reactor Safety (NRS). However continuous improvements in analytical techniques and in the sophistication of hardware products do not necessarily correspond to new industrial applications within Nuclear Power Plants (NPP) technology. The declining condition for nuclear technology also contributes to the lag between developments and applications definitely causing NPP safety at a level below the achievable level. The possibility to extend BEPU to all areas of the Final Safety Analysis Report (FSAR), so-called BEPU-FSAR is outlined in the paper. This should be combined with the Extension of the SM concept (E-SM). BEPU-FSAR techniques may be at the origin of E-SM which also will need specific monitoring hardware. All of this may open new horizons for NRS and for acceptance of NPP by the public and the decisions makers. The paper describes recent accomplishments in the areas of BEPU and E-SM.

Key Words: Licensing, Best Estimate Plus Uncertainty, Safety Margins.

### 1. INTRODUCTION

Nuclear Reactor Safety involving fission and water cooled or moderated reactor constitutes the general framework for the paper. NRS is an established technology since several decades, starting from the discovery of nuclear fission. On the one hand well known accidents have challenged the sustainability of nuclear technology and undermined the trust of the public. On the other hand, innovative ideas and proposals are possibly needed to restore the confidence and to escape the irreversible loss of competence primarily in those Countries where the technology was developed and exploited for several decades since its discovery.

The last statement shall be seen as the triggering point for the present paper which is based upon activities discussed in Refs. [1] to [5].

Licensing is the legal part of NRS. Country specific laws must be pursued within the licensing process, e.g. the Code of Federal Regulation in the United States. The Final Safety Analysis Report which is related to individual NPP units is the end results of the licensing process and brings to the permission of operation of the unit. The documentation of Accident Analysis (AA) is the key part of the FSAR. Noticeably, procedures to perform safety assessment and thresholds of acceptability fixed by Regulatory Bodies are part of the licensing and of AA.

Acceptance criteria are the common words used for the 'thresholds of acceptability'. Safety Margins (SM) may be considered as a consequential concept derived from acceptance criteria, see e.g., Ref. [6]. According to Ref. [7] the general definition (absolute terms) is: "The safety margin is the distance between an acceptance criterion and a safety limit. If an acceptance criterion is met, the available safety margin is preserved". An extension of the SM concept is discussed in Ref. [4]: let's call this extension E-SM.

Best Estimate Plus Uncertainty is an approach which is consistent with the capabilities of system thermal-hydraulic codes and their application to the AA [8]. BEPU has been widely applied to the analysis of Large Break Loss of Coolant Accidents (LBLOCA) [9], and more recently to the overall set of accidents part of the Chapter 15 of the FSAR, [10], see also [1] and [2]. BEPU can be extended to all the analytical parts of the safety analysis report as discussed in Ref. [11]: the extended application is called BEPU-FSAR.

The purpose of the present paper is to connect BEPU-FSAR and the E-SM which can be derived from the application of numerical codes or procedures. Snapshot information necessarily incomplete and not systematic about BEPU and E-SM is provided first.

## 2. THE EXTENDED SAFETY MARGIN CONCEPT

The concept of 'Safety Margins' is well established within the NRS and in related AA. The SM value can be defined as the difference or the ratio in physical units between the limiting value of an assigned parameter (typically, the threshold value for the connected acceptance criterion) the surpassing of which leads to the failure of a system or component, and the actual value of that parameter during the life of the plant.

The existence of suitable margins ensures that Nuclear Power Plants operate safely in all modes of operation during their life. Sample SM relate to physical barriers designed to protect against the release of radioactive material, such as fuel matrix and fuel cladding (limiting values are associated with departure from nucleate boiling ratio, fuel temperature, fuel enthalpy, clad temperature, clad strain, clad oxidation), reactor coolant system boundary (pressure, stress, material condition) and containment (pressure, temperature); other SM are connected with dose to the public being close or far from the NPP.

The accident phenomenology and the related timing are estimated as complete as necessary within the Deterministic Safety Assessment (DSA) framework. In turn, the Probabilistic Safety Assessment (PSA) approach allows demonstration of the completeness of the set of different scenarios and best estimate methods. The approaches have been developed rather independently from each other. This poses the problem of consistent integration. Hence, a generalization of the concept of safety margin may be beneficial. In addition, the concepts of safety margins and of quantifying changes in safety margins are key components of the discussions for modifications in plant design parameters and operational conditions. This includes, for example, power up-rates, life extensions, use of mixed oxide fuels, different cladding materials, design and operation of passive systems and changes to technical specifications. Those modifications impact safety margins in deterministic analyses, while others impact the reliability of systems and components, and yet others impact safety margins and reliability simultaneously.

Looking at the evolution of occurred accidents in complex systems, an extended definition of SM appears worthwhile. For instance, this may include the consideration of pilot mental status history and of conditions for locking the cabin door in case of aircraft as well as the surveillance of the construction site for a NPP. A multidimensional space for SM in NRS has been envisaged [4]. This shall have multi-face and multi-field attributes because of the several design-safety-licensing aspects and involved technological fields.

The multidimensional space can be defined for SM noting that risk space shall be taken as synonymous of safety space. The dimensions for the space embracing the definition of SM can be defined as [4]:

- a) The key elements characterizing NRS.
- b) The technological sectors or the key scientific disciplines of NRS and NPP design and operation.
- c) The Structures, the Systems and the Components (SSC) constituting the NPP.
- d) The time spans which form the life of the NPP.

Human factors shall be considered as part of any of the 'dimensions' above. Furthermore, the definitions of elements, sectors, SSC and time spans with a consequent sub-categorization process allow arriving at a few ten thousands detectable SM quantities, thus constituting the E-SM ensemble. Monitoring the combination of possibly un-influent E-SM values contributes to the additional safety barrier against the release of fission products. For instance, the combination of a certain number of signals (e.g. in the case of TMI-2 leaking pressurizer valve combined with the presence of a manual valve in the auxiliary feed-water line having the possibility to remain close, etc.) shall prevent the operation of reactor unit well before conditions are created for the occurrence of a safety relevant event.

Pairs of quantities are needed to form an E-SM: on the one hand there is the monitored or the calculated value; on the other hand there is the threshold or the acceptable value. It is intended that monitored values come from specific hardware and calculated values from BEPU-FSAR as mentioned in next section; and threshold value needs an endorsement by regulators.

### 3. THE BEST ESTIMATE PLUS UNCERTAINTY APPROACH

A textbook is needed for a comprehensive description of BEPU: on one side, it is straightforward to discuss the outcomes of a BEPU calculation; on the other side it is difficult to explain shortly what BEPU is. An attempt is made hereafter to give an idea of BEPU.

The complexity of nuclear thermal-hydraulics and the impossibility to obtain analytical solutions from equations derived from fundamental principles of physics is at the origin of BEPU. The following limitations can be mentioned in this connection:

- Turbulence is a property of moving fluids. Turbulence is barely known for single phase flows; moreover two- or more-phases flows of technological interest are inherently turbulent. Equations to calculate turbulence in transient situations either do not exist or are not qualified.
- No model exists to calculate the motion of a set of bubbles in a boiling-condensing system involving formation, growth, coalescence and collapse processes (partly connected with the turbulence statement above).
- Convection heat transfer and pressure drops, i.e. the fundamental mechanisms involved with two phase flow mixture evolutions, are calculated based on empirical formulations which are based upon a variety of drawbacks.
- Complex processes or mechanisms relevant in NRS like reflood, radiation heat transfer, countercurrent flows and those characterizing component (e.g. fuel rods, pumps, valves, separators) performances also need specific empirical/imperfect formulations: in most cases those formulations cannot be proved at the scale of the NPP target of the calculations.
- The averaging in time and space, noticeably at the levels of flow cross section area and of volume occupied by fluid, is unavoidable: the size of the integration domain is typically larger than the scale of involved phenomena.

Therefore, approximations are at the basis of any numerical approach to simulate a system of interest. Thus, the objective of a model is to calculate the reality in the best possible way consistently with current knowledge, hence the words Best Estimate (BE). The application of those BE models to experimental situations shows unavoidable (known) errors sometimes referred as accuracy of a calculation. Then errors are expected in the prediction of NPP system performances: those (unknown) errors constitute the uncertainty of a calculation, [12], hence the words Plus Uncertainty and the final acronym BEPU. In principle the uncertainty of a calculation must consider all the approximations introduced in modeling of reality.

Verification and Validation (V & V), scaling, procedures for uncertainty quantification, for the consistent application of computational tools to AA and for coupling of numerical codes constitute the pillars of current BEPU. The intimate connection between PSA and DSA is also part of BEPU.

### 4. BEPU-FSAR AND THE CONNECTION WITH E-SM

BEPU, as it is now, constitutes a recognized resource for the application of nuclear thermal-hydraulics system codes and the AA [2]. The established BEPU methods and procedures can be extended to any part of the FSAR where an analytical derivation is needed. This ensures a homogeneous consideration of requirements in the different sectors of FSAR: for instance, the probability and the consequence of external hazards shall be modeled and evaluated by techniques having same rigor and similar consideration of errors as the techniques utilized for internal accident analysis. Furthermore, the systematic identification of boundaries in chains of adjacent technological areas constitutes a valuable consequence of the extension. One example is geology, soil properties, soil-structure interaction, civil structure resistance and mechanical structures resistance: combined BE calculations shall be performed where stresses in primary system piping following an earthquake are a function of local soil amplification or damping of waves originated at the epicenter. The bases for the extension of BEPU techniques to cover all areas of NRS have been put [11], and called BEPU-FSAR.

BEPU-FSAR constitutes the logical framework for the systematic identification and characterization of E-SM quantities and for computing the actual margins in case of accident or during the lifetime of the concerned NPP. An overly simplified example dealing with clad ballooning during LBLOCA is outlined hereafter:

- Ballooning occurrence is unavoidable and calculated at least in selected fuel assemblies. This causes crack openings and release of fission gases.

- Fuel fragmentation causes at least two main problems: a) accumulation of fragmented UO<sub>2</sub> debris in the bottom part of the ballooned region with possible difficulty in cooling; b) exit of solid fission products from the crack.
- Parameters can be defined and calculated to give rise to a few E-SM based on: 1) tolerable burn-up combined with linear heat generation rate; 2) emergency system design conditions to cope with the ballooned region; 3) tracking of solid fission products possibly demonstrating their confinement into the containment.

## 5. CONCLUSIONS

BEPU-FSAR and E-SM constitute the two-tier integrated proposal for improving NRS technology. Introducing related findings in NPP design has the potential:

- a) to create an additional safety barrier to the release of fission products;
- b) to prevent severe accident occurred so far.

Innovation in NRS seems essential to restore the confidence towards nuclear technology. Cost of the (proposed) innovation shall be below 1% the cost of one individual NPP.

## REFERENCES

- [1] D'AURIA, F., MAZZANTINI, O., The Best-Estimate Plus Uncertainty (BEPU) Challenge in the Licensing of Current Generation of Reactors, IAEA Int. Conf. on Opportunities and Challenges for Water Cooled Reactors in the 21st Century, IAEA, Vienna (2009).
- [2] D'AURIA, F., CAMARGO, C., MAZZANTINI, O., The Best Estimate Plus Uncertainty (BEPU) approach in licensing of current nuclear reactors, J. Nuclear Engineering and Design, **248** (2012) 317.
- [3] D'AURIA, F., DEBRECIN, N., Perspectives in licensing and nuclear reactor safety technology, Invited at Conf. Innovative Designs and Technologies of Nuclear Power, ISTC NIKIET, Moscow (2014).
- [4] D'AURIA, F., GLAESER, H., KIM, M-W., A Vision for Nuclear Reactor Safety, Key-Speaker at 46th Jahrestagung Kerntechnik Annual Meet., Berlin (2015).
- [5] D'AURIA, F., GLAESER, H., DEBRECIN, N., Independent Assessment for new Reactor Safety, ENS TopSafe Conf., Vienna (2016).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, "Accident Analysis for Nuclear Power Plants", Safety Report Series, SRS-23, IAEA, Vienna (2002).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Implications of power up-rates on safety margins of nuclear power plants, TECDOC 1418, IAEA, Vienna (2004).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide, SSG-2, IAEA, Vienna (2009).
- [9] GALETTI, M. R., D'AURIA F., Questions arising from the application of Best-Estimate Methods to the Angra-2 NPP Licensing Process in Brazil, Int. Meet. on Best-Estimate Methods in Nuclear Installation Safety Analysis (BE-2000) IX, Washington D.C. (2000).
- [10] PETRUZZI, A. et al., The BEPU Evaluation Model with RELAP5-3D for the Licensing of the Atucha-II NPP, J. Nuclear Technology, **193** (2016) 113.
- [11] MENZEL, F., et al., Using of BEPU methodology in a Final Safety Analysis Report, International Nuclear Atlantic Conference – INAC 2015, Sao Paulo, Brazil (2015).
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, Safety Report Series, SRS-52, IAEA Vienna (2008).



## ASSESSMENT OF BASE-ISOLATED CAP1400 NUCLEAR ISLAND DESIGN

Y. JIE

Shanghai Nuclear Engineering & Research Institute

Xuhui District/ Shanghai, China

Email: yangjie@snerdi.com.cn

L. SHAOPING

Shanghai Nuclear Engineering & Research Institute

Xuhui District/ Shanghai, China

### Abstract

As we know, Japanese KashiwazakiKariha and Fukushima NPPs have experienced strong earthquake beyond design basis, requirement for enhancing the condition of design basis ground motion and the seismic isolation technology are getting more and more attention worldwide. The paper presents the research on the seismic isolation with locking device of the CAP1400 nuclear island (NI), which can increase the seismic capacity of CAP1400 units from 0.3g to 0.6g (0.6g in horizontal and 0.4g in vertical), in the condition of keeping the superstructures of CAP1400 NI standard design unchanged. A series of nonlinear time-history analysis are performed to predict the maximum displacement and acceleration of the isolation layer, the maximum stress of the isolation units, and the floor response spectra of each story of the superstructure in the design basis earthquake of 0.6g, considering the realistic mechanical properties and the layout of the isolator. At the same time, a shaking table test of a reducedscale model ofthe base-isolated nuclear structures is introduced in the paper. The dynamic characteristic was examined, together with the vibration acceleration and displacement under different seismic intensities.

### 1. INTRODUCTION

Base isolated structure system is a passive control system, which reduces the response of a structure to horizontal ground motion

In order to confirm the isolation effect of the CAP1400 Nuclear Island structure, a series of nonlinear time-history analysiswere performedand shaking table tests of a reduced-scale model were accomplished. The dynamic characteristics of the isolated model structure for design and beyond-design basis earthquake shaking were tested, including the horizontal peak accelerations, displacement of the superstructure, and the force and the hysteretic curve of the isolated bearings.

The results of this study provide the technical basis for the base-isolated design of CAP1400.

### 2. BASE ISOLATED DESIGN OF CAP1400 NUCLEAR ISLAND STRUCTURE

CAP1400 Nuclear Island (NI) structure consists of steel containment vessel, containment internal structure, shield building, and auxiliary building. These buildings are founded on a commonbasemat. The size of the basemat is 91.4m×43.5m, and the height of NI structure is 75.5m. The total weight of the NI structure is  $20.5 \times 10^4$ t.

The target of base-isolated design of CAP1400 NPP is making the seismic design benchmark of safe shut earthquake (SSE) to 0.6g in horizontal direction instead of the original 0.3g. Adopting seismic isolation solution can increase the safety of the superstructure and the devices inside the superstructure with the benefit of realizing the standard design, which can enlarge the adaptability of the nuclear plant site.

The isolated bearings are laid under the basemat, and the spacing is 3m~4m. The type of the isolated bearing is lead rubberbearing, and the total amount is 450. Lead rubber bearings typically use natural rubber as their elastomeric material. Lead is an ideal material because it has high horizontal stiffness before yielding and then behaves perfectly plastic after yielding. It can forever nearly recover its original mechanical properties following inelastic action such as that imposed by an earthquake.

In order to avoid the breakage of component (e.g., pipes, cable trays, cable ducts and conduits) that crosses the isolation interface under small earthquakes, lock devices are added to the rubber bearing. And these devices will not affect the function of isolation system under big earthquake.

Fig. 1 shows the layout of the isolation unit.

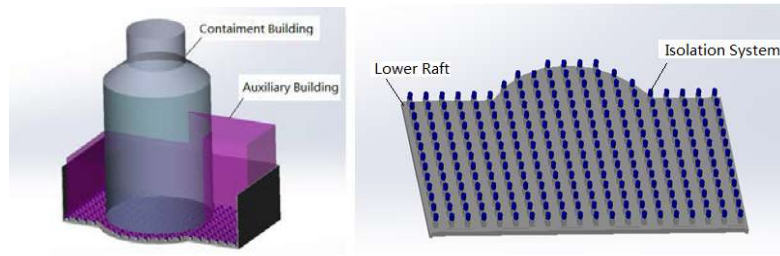


FIG. 1. Layout of Isolation Units.

### 3. FINITE ELEMENT METHOD ANALYSIS OF BASE-ISOLATED DESIGN OF CAP1400 NPP

The analysis model of the nuclear island stick model is composed of auxiliary and shield building, containment internal structure, steel containment vessel and reactor coolant loop, see Fig. 2. The hysteresis behaviour of isolation unit in horizontal direction is modelled by element type Combin40.

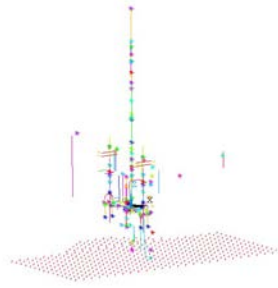


FIG. 2. Analysis model of base-isolated Nuclear Island.

A series of nonlinear time-history analysis are performed to predict the maximum displacement and acceleration of the isolation layer, the maximum stress of the isolation units, and the floor response spectra of each story of the superstructure in the earthquake 0.6g, considering the realistic mechanical properties and the layout of the isolator.

### 4. SHAKING TABLE TEST RESULT OF BASE-ISOLATED DESIGN OF CAP1400 NPP

A reduced-scale earthquake simulation of base-isolated nuclear structures on a shaking table was performed, which provided realistic data to improve and validate current modelling approaches (see Fig. 3).



FIG. 3. Reduced-scale shaking table test.

The study was primarily focused on the response of superstructure and the isolation unit. The test results of a reduced-scale nuclear island model tested on a shaking table were compared with three-dimensional finite element simulation results.

### Acceleration response

Fig. 4 illustrates the benefits of seismic isolation using an acceleration distribution plot in isolation layer and superstructure, in which node 1 represents lower raft, and nodes 2~5 represent superstructure of different elevations. From the plot, we find the acceleration of superstructure in horizontal direction reduce significantly.

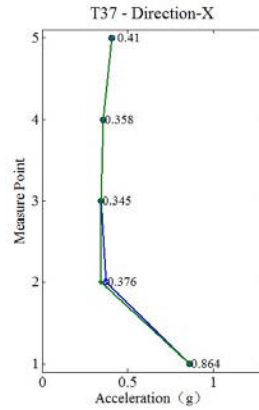


FIG. 4. Acceleration distribution plot in isolation layer and superstructure.

The acceleration time histories of analysis and test results are compared in Fig. 5. According to the comparison of acceleration results under different load conditions, the test results match the analysis results very well, especially under the unidirectional loading condition.

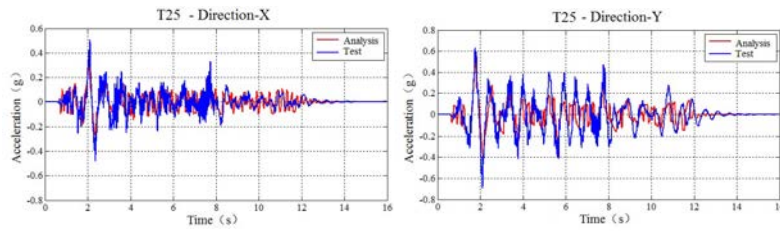


FIG. 5. Acceleration time histories of analysis and test results.

### Hysteretic behaviour of isolation layer

From the test, the shear force-displacement hysteretic curves of the isolated layer were obtained. The hysteretic curves of test results are compared with the numerical simulation in Fig. 6.

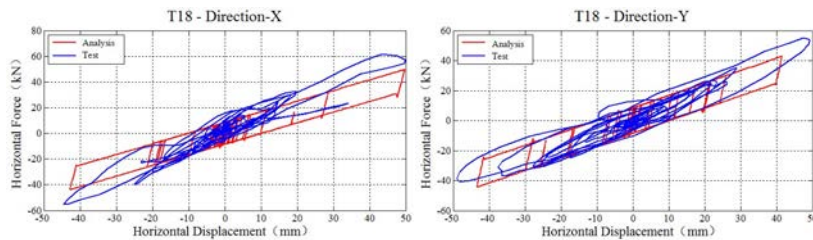


FIG. 6. Hysteretic curve under biaxial loading condition.

From the results, it can be seen that the shape of the hysteresis curve is more stable, and closer to the numerical simulation results under unidirectional loading condition. And under the multi direction loading, the measured hysteresis curves show a more complex shape, but the overall trend is consistent with the numerical simulation results.

## Floor response spectra

Fig. 7 illustrates the benefits of seismic isolation using an acceleration response spectrum. The red line is the spectra of standard design in 0.3g earthquake, and the blue line is the spectra of base-isolated design in 0.6g earthquake.

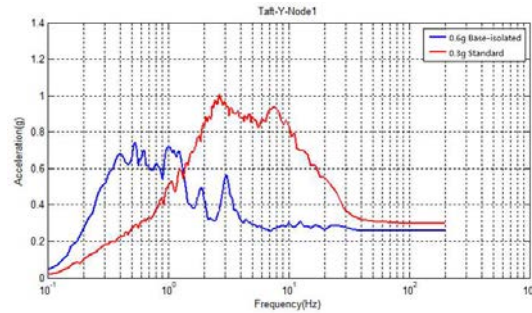


FIG. 7. Comparison of the Spectra of the isolation layer in horizontal direction between the base isolated model and fixed base model.

From the comparison results above, the floor response spectra in horizontal direction reduce significantly in the frequency range that larger than 1Hz, but amplify in the frequency range that less than 1Hz.

Although modern isolation systems substantially decouple the superstructure from horizontal ground shaking, none mitigates response to vertical ground motion.

The amplification of the response spectra in the low frequency range of horizontal direction and in the vertical direction has been evaluated. They have little contribution to the response of the components and systems contained in the superstructure.

## 5. CONCLUSION

Finite element analysis and shaking table tests were performed for the isolation and non-isolation models of CAP1400 nuclear island structure. By the comparison with the test and analysis results, the following conclusions are obtained:

The natural frequency of the isolated structure is about 20% of the non-isolated structure. Base isolation technology extends the natural period of the structure, and increases the damping to reduce the input of earthquake of the superstructure. So the floor response spectra in horizontal direction reduce significantly in the frequency range that larger than 1Hz, but amplify in the frequency range that less than 1Hz.

Under the action of 0.6g earthquake, the frequency of the base-isolated structure is reduced by 2%, which demonstrates that the structure is only slightly damaged. But the frequency of the non-isolated structure is decreased by 30%, which demonstrates that the structure is degenerated into the elastic plastic state.

The peak acceleration response of the isolation layer is much smaller than the acceleration of the non-isolated structure's basement, which indicates that the acceleration of the superstructure has been effectively controlled, and the earthquake response of the structure reduces significantly through the base isolation technology.

Under the action of different levels of seismic wave, the hysteretic curve is full, which shows that it has good energy dissipation capacity.

The calculation and analysis of the isolated structure are in good agreement with the experimental results, which shows the analysis result could be used for the design of CAP1400.

## ACKNOWLEDGEMENTS

Funding for this study was provided by National Science and Technology Major Project. Additional support for testing of the isolation system at shaking table was provided by China Academy of Building Research. The isolators and connection plates were provided by Liuzhou OVM Machinery Corporation. The authors are grateful to all sponsors for making this possible.

## REFERENCES

- [1] HALL, J.F., Problems encountered from the use (or misuse) of Rayleigh damping. *Earthquake Engineering and Structural Dynamics*, **35** 5 (2006) 525.
- [2] ERDURAN, E., Evaluation of Rayleigh damping and its influence on engineering demand parameter estimates. *Earthquake Engineering and Structural Dynamics*, **41** 14 (2012) 1905.
- [3] RYAN, K.L., POLANCO, J., Problems with Rayleigh damping in base-isolated buildings, *J. Struct. Eng.*, **134** 11 (2008) 1780.
- [4] PANT, D.R., WIJEYEWICKREMA, A.C., ELGAWADY, M.A., Appropriate viscous damping for nonlinear time-history analysis of base-isolated reinforced concrete buildings, *Earthquake Engineering and Structural Dynamics*, **42** (2013) 2321.
- [5] WANG, T., WANG, F., DING, L.T., Theoretical and experimental study on three-dimensional base-isolated nuclear power plant, *China Civil Engin. J.* **45** 1 (2012) 238.
- [6] ZHOU, F.L., *Engineering structure vibration control*, Seismological Press, Beijing (1997).
- [7] LI, D.M., *Analysis of a nuclear power plant containment isolation seismic response*, Harbin Engineering University Harbin (2007).
- [8] FRANO, R.L., FORASASSI, G., Isolation systems' influence in the seismic loading propagation analysis applied to innovative near term reactor, *Nucl. Engin. Design*, **240** 10 (2010) 3539.

## A SCHEME FOR HARMONIZATION OF TERMINOLOGY ON SAFETY MARGINS AND CRITERIA

V. MEČÍŘ  
ČEZ, a.s. - NPP Temelín  
Temelín, Czech Republic  
Email: vaclav.mecir@cez.cz

J. MACHÁČEK  
ČEZ, a.s. - NPP Temelín  
Temelín, Czech Republic  
Email: jaromir.machacek@cez.cz

R. MECA  
ÚJV Řež  
Husinec – Řež, Czech Republic  
Email: Radim.Meca@ujv.cz

### Abstract

Many international documents contain variety of terms dedicated to criteria and margins problem. Different international documents were issued by different organizations and the documents were created by experts from different areas such as regulatory, scientific, safety analyses (nuclear and radiation), technical specification, operation and others. However Nuclear Power Plant staff deals with all the areas and often one can find one specific item called in different terminology and different items called identically.

This situation called out for attempt to systemize the terminology among different areas.

Therefore, after thorough review of international documents from different areas of concern to NPP staff, the scheme of criteria terminology was created. Considering the design, manufacturing, assembly and operation processes, which contain conservatisms, only after that, corresponding margins were identified by its nature. Only then, to different, broadly used margins terms these identified by its nature margins were assigned. Proposed Criteria and Margins terminology could be used by different groups of experts. Definitions are provided along with practical examples. In order to make the scheme user friendly, scheme animation is provided.

### 1. INTRODUCTION

Margin management is recognized worldwide as one of very important area for safe and reliable NPP operation, but comparing terminology used in different guiding documents may be source of confusion for those who need to use more than one guide. Essentially in every activity connected with NPP, conservative approach is preserved, even when best estimate methods are used. All applicable criteria are demonstrated to be met with “satisfactory” margin at NPP design stage as well as operation stage, using different methods. These methods use conservative input data, conservative models etc. It can be understood, that there is a built in conservatism within the NPP design covering modes of operation, which is, in general, not quantified, but it is assumed that it exists.

In order to properly understand margins and conservatism built in the NPP design, it should be noted that the problem of margin management in principle should cover the entire NPP design – licensing - operation chain. The particular margin management is NPP specific, but the terminology should be clear and unambiguously defined trough out entire NPP design – licensing - operation chain and therefore guides issued by international organizations involved too. It should be understood, that for safe and reliable NPP operation the mutual understanding across entire NPP design – licensing - operation chain which means that harmonized terminology is important too. A question is, how and where to start with terminology harmonization. The entire NPP design – licensing – operation chain can be essentially seen from the top to bottom. The “Top” can be represented by customer requirements, regulatory requirements, and essential material properties. Then standards, acceptance criteria, design practices, SSC manufacturing and assembly can follow down to NPP startup, operation and modifications, including safety enhancement, power up rates and LTO.

For the purpose of criteria and margin management terminology harmonization, taking into account that different licensing practices may exist in a country of a designer and a country of a utility, two schemes were

created. First scheme (Fig. 1) should help to understand where are the sources of margins, which may emerge from conservatism built into the NPP design documentation including operating procedures, SSC manufacturing and assembly stages. The second scheme (Fig. 2) then expands the approach to the NPP licensing and operation stage. Both schemes reflect the fact that in particular general design criteria may be satisfied via different limits of physical parameters expressed in different units at design and operation stage. Within the definition/abbreviation part of report, where appropriate, attempt is made to juxtapose terms used in different international guides, which potentially can have the same meaning within the criteria and margin scheme.

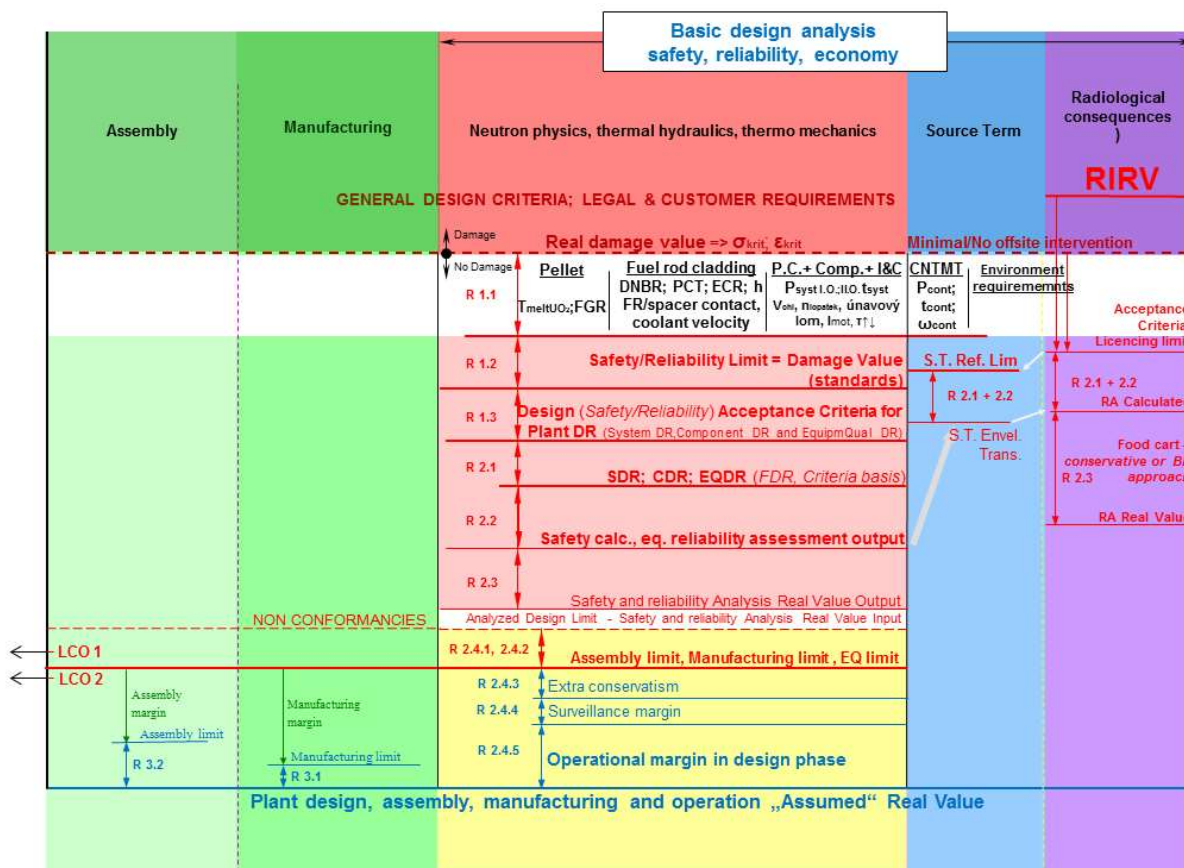


FIG. 1. Design phase Criteria-Margin scheme.

## Harmonization approach

The proposed way for terminology harmonization is based on:

- Essential design and licensing process for new plant SSC design with built in different type of conservatisms (which may be seen as not quantified potential margin), plant startup and operational experience feedback, modifications and ageing, taking into account methods improvements, which may generate quantifiable margins (positive margin) or reveal deficiencies/non conservatism (negative margin) over plant operation.
- Criteria hierarchy and the way how they were established, covering entire NPP design – licensing – operation chain starting from GDC to operation criteria.
- Identification of types of possible margins, then grouping them by its nature and only after that assign them broadly used terms as Safety..., Design..., etc. margin.
- The following definitions are used:

AC – Acceptance Criteria – criteria, expressed in terms of physical parameters in order to demonstrate that General Design Criteria (Requirements) are met. AC are Safety, Design, Manufacturing, Assembly and Operational. To each Safety AC parameter can be assigned Safety, Acceptance and Licensing limit.

AL – Acceptance Limit - value set up by regulator taking into account probabilistic nature of processes, events and the way, how the safety limit was obtained based on the experimental data and conditions.

Calc.Value – Calculated value within given methodology.

CDR – Component Design Requirements - Requirements to the components, which need to be met in order to comply with System DR and AC resp. their AL values.

DL – Dose Limit – Postulated value at which damage to human/nature occurs.

LCO – Limiting Condition for Operation in Condition I assured in ultimate case by reactor shut down or trip initiated by operator or systems at reaching specific set points

LL – Licensing Limit – Regulatory approved value, which shall not be exceeded during licensing process, using specific approved methodology within specific project –  $LL \leq AL \leq SL = PDV$

PDV – Postulated Damage Value – value at which damage is postulated

RIRV – Radiation Impact Real Value – value at which radiation harm/damage occurs

RSAC – Reload Safety analysis Checklist - parameters with limits which shall be satisfied for core design

RV – Real Value – As a matter of the fact, such value can be known indirectly (measurement at different then evaluated conditions e.g., Real Damage Value - RDV, calculation, measurement with subsequent calculation)

SL – Safety Limit – value, at which SSC, function fails /is damaged = PDV

ST ref. lim. – Source Term reference limit

$\sigma_{krit}$  – stress at which SSC fails/is damaged

SSC – Structure, System, Components

Margin – difference expressed in terms of physical parameters as a result of demonstration that current necessary conservatism can be less than conservatism originally implemented in the NPP SSC design.

Criteria structure relating on the above definition can be created for licensing and operation stage, (Fig. 2) with identified types of margin as follows:

**R1 Criteria Margin** – Difference between limiting value corresponding to GDC (damage value) and value at which it is postulated that CCS will fail – Postulated Damage Value. It consists in:

R1.1: Transition from GDC to actual AC expressed in terms of set of physical parameters

R1.2: Method of  $SL = DV$  set up for each AC such as:

- Selection of acceptable measure of no failure (e.g. 95/95),
- Conditions and experimental data treatment
- Selection of DV as e.g.: average, RMS, Min, Max,

R1.3: The way of AC values setup such as e.g.:  $DV \text{ minus uncertainty, } AC = DV$

**R2 Methodology Margin** – Difference between AC value and actual calculated value (Plant, System, Component, Equipment qualification design requirement). It consists in:

R2.1: Difference between AL - the conditions at which AC Limit was setup and LL corresponding to the analytical method used to demonstrate AL limit is met (in the Basic Design Analyses scheme covers also conservatism implemented due to parallel activities in design process)

R2.2: Difference between required properties and calculation result at specified design input

R2.3: Design / SA Methodology consist in:

R2.3.1 – Selection and justification of initiating events taking into account frequency, initial and boundary conditions and single failure principles

R2.3.2 – actual modelling of processes, including user effects.

R 2.4: Selection of input values used in safety analyses) connected with:

R 2.4.1 – methodology (e.g. to cover possible non-conservatism of scenarios R2.3.1)

R 2.4.2 – the way of accounting for SSC reliability

R 2.4.3 – extra conservatism (Design /licensing schedule, Processes knowledge, Capabilities of manufacturing and assembly

R 2.4.4 – Surveillance considerations e.g. *Calibration accuracy, conditions, frequency*

R 2.4.5 – Additional supplier's conditions

**R3 As Built Margin** consists in:

R3.1: Manufacturing due to better, then in design assumed limiting, values

R3.2: Assembly due to better, then in design assumed limiting, values

R3.3: SSC Servicing



**R4 Operational Margin:** difference between actual value of monitored parameter and its limiting value in operational procedure

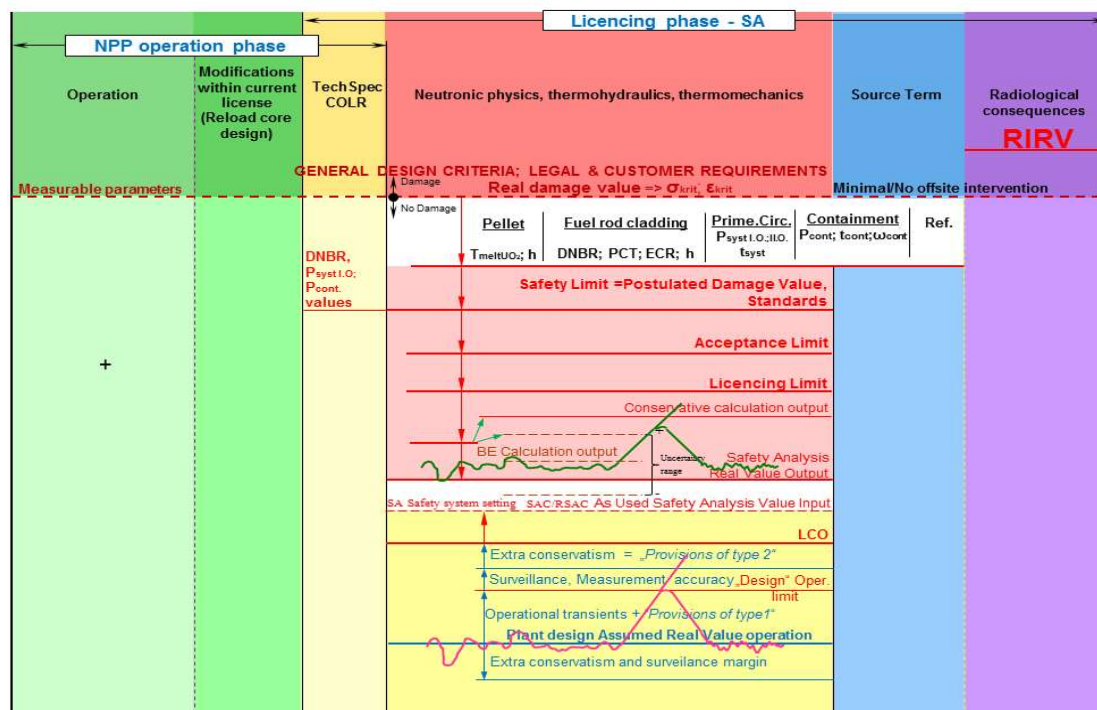


FIG. 2. Licensing-Operational phase Criteria-Margin scheme 1.

At the end, the general terms for Margin can be assigned (Fig. 3) as:

Safety margin – R1.1 – R1.3, Licensing margin R2.1, Output design margin R2.2, R2.3, Input design margin R2.4.1 – R2.4.4, R3.1 – R3.3, Operational margin at the design (including modifications) stage R2.4.5, resp. Operational margin at the operation stage R4.

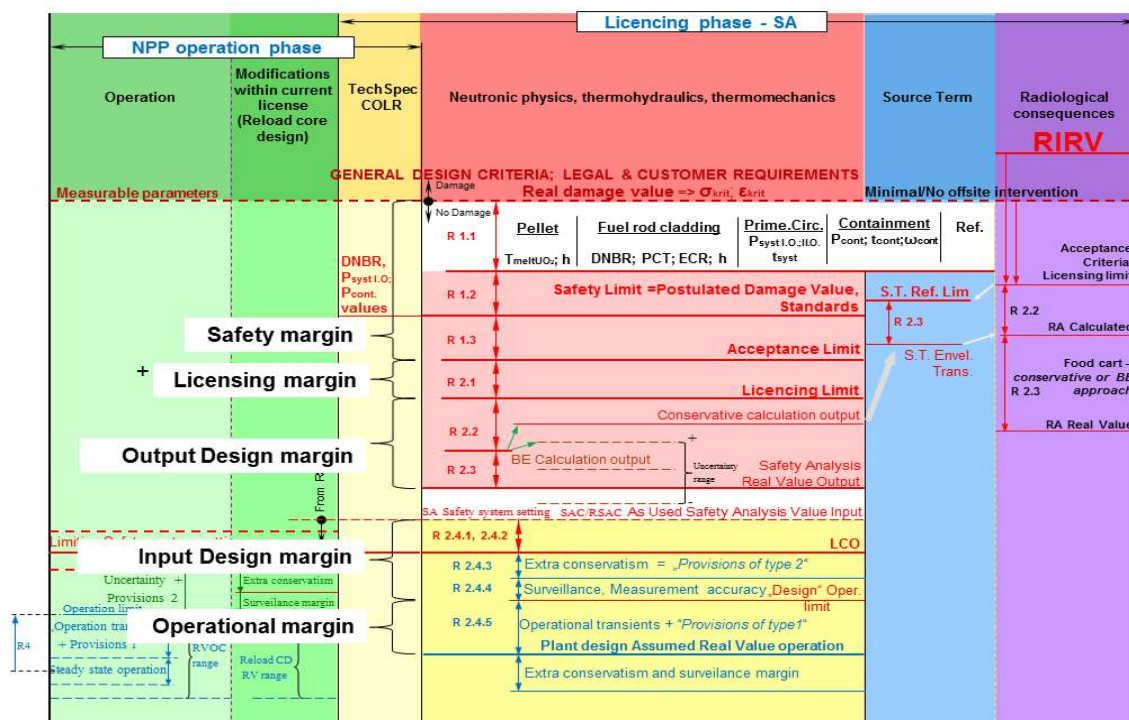


FIG. 3. Licensing-Operational phase Criteria-Margin scheme 2.

Applicability to Low water level in accumulator with references to documents and examples of limits as practical example of presented approach is demonstrated on Fig. 4:

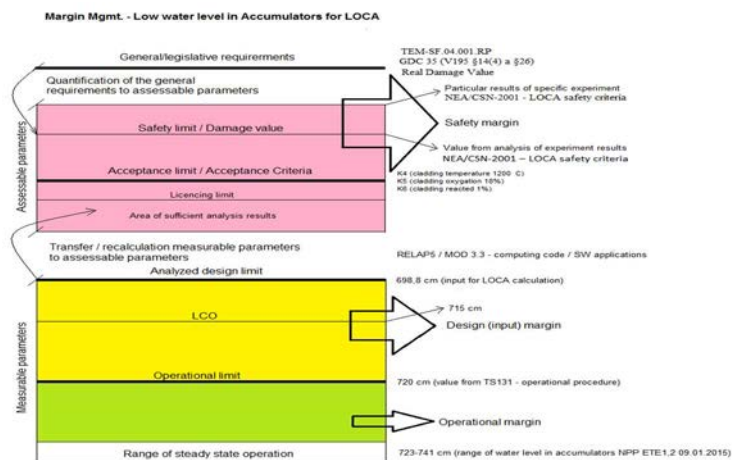


FIG. 4. Licensing-Operational phase Criteria-Margin scheme 2.

## ACKNOWLEDGEMENTS

Authors would like to express great appreciation for discussion, support and participation in scheme development to the following experts:

ČEZ, a.s. – Temelín: A. Vald, J. Šejda, O. Kvasnička, V. Pfützner,  
 UJV Řež: J. Mišák, J. Macek, J. Klouzal, L. Denk, I. Tinka, Z. Zůna,  
 AEP: E. Vald, ŠJS: J. Jeník, M. Ruchař, VUJE: Š. Rohár, TRACTEBEL Engineering: Jinzhao Zhang,  
 EdF: N. Waeckel, Independent consultant: M. Holan.

## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions, IAEA-NS-G-2.2, IAEA, Vienna (2002).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Margins of Operating Reactors, Analysis of Uncertainties and Implications for Decision Making, IAEA-TECDOC-1332, IAEA, Vienna (2003).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Differences in Fuel Safety Criteria, IAEA-TECDOC-1381, IAEA, Vienna (2003).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Implications of power up rates on safety margins of nuclear power plants, IAEA-TECDOC-1418, IAEA, Vienna (2004).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Best estimate safety analysis for nuclear power plants: uncertainty evaluation, IAEA SRS No. 52, IAEA, Vienna (2008).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Power Uprate in Nuclear Power Plants: Guidelines and Experience, IAEA Nuclear Energy Series No. NP-T-3.9, IAEA, Vienna (2011).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA-TECDOC-1791, IAEA, Vienna (2016).
- [8] WORLD ASSOCIATION OF NUCLEAR OPERATORS, Guidelines for Plant Status and Configuration Control at Nuclear Power Plants, WANO GL 2001-04, UK (2002).
- [9] WORLD ASSOCIATION OF NUCLEAR OPERATORS, Excellence in the Management of Design and Operating Margins, WANO GP ATL-11-005, UK (2011).
- [10] INSTITUTE OF NUCLEAR POWER OPERATIONS, Configuration Management Process Description, INPO AP-929, USA (2005).
- [11] INSTITUTE OF NUCLEAR POWER OPERATIONS, Excellence in Management of Design and Operating Margins, INPO 09-003, USA.

- [12] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, OECD NEA/CSNI/R(2003)10: Survey of Fuel Safety Criteria.
- [13] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, Fuel Safety Criteria Technical Review, OECD NEA/CSNI/R(99)25, 2000.
- [14] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, OECD NEA/CSNI/R(2007)9, Safety Margins Action Plan – Final Report, 2007.
- [15] Evaluation of Safety and Safety Margins in the light of the accident of the NPP.
- [16] Fukushima, State Office for Nuclear Safety Czech Republic Revision 1, March 2012.

## SMR REGULATORY PERSPECTIVES

**Chairperson**

**M. EL-SHANAWANY**  
United Kingdom



## SMALL-SIZED REACTORS OF DIFFERENT TYPES: REGULATORY FRAMEWORK TO BE RE-THOUGHT?

W. KRÖGER  
ETH Zurich  
Zurich, Switzerland  
Email: kroeger@ethz.ch

### Abstract

All types of large reactors, subject of intensive development, are represented in SMR lines. A study of evolutionary (mostly water cooled), revolutionary (sodium or gas cooled), and exotic (salt or lead cooled) designs focused on safety characteristics and assessment against tightened-up requirements; notably robustness against malicious interventions and instability of societies. In general, lower power and operating pressure reduce the potential of catastrophic releases; increased safety margins and special design characteristics almost eliminate risk of severe core damage, triggered by RIA or SBO. Active systems and early operator actions are avoided; the need for a containment, and emergency planning is often negated. However, concept-specific accident scenarios such as fierce chemical reactions, flawed fuel addition, overcooling/freezing or air/water ingress deserve attention. Most developers claim that classical regulatory approaches to safety are inappropriate. However, relying on “one line of defense” and replacing active systems by passive, inherent mechanisms result in a shift of safety proofs to material properties, validity of experiments and computer codes, completeness of scenarios – under constraints of increased uncertainties. Furthermore, some reactor concepts are closely linked to elements of the fuel cycle, introducing new challenges. It seems to be evident that new regulatory concepts need to be developed - aiming to avoid unnecessary safety measures, while ensuring exceedingly high standards - and regulators to be educated, both in parallel with technological developments.

### 1. INTRODUCTION

A thorough assessment of past operating experience, based on a comprehensive nuclear events with database [1], emphasizes that severe nuclear accidents are rare in absolute and relative terms due to disproportional, far-reaching design and operational measures – if well followed and implemented. Nevertheless, the physical process (surplus of neutrons, radio-toxic fission products, decay heat production) and current technology (high power density and size, meltable fuel claddings and structural materials, high operating pressure, etc.) make today's reactors highly vulnerable to perturbations and deficits of the operational context; although substantially low frequency, the potential of large radioactive releases and associated frightening consequences cannot be ignored.

### 2. KEY REQUIREMENTS FOR LESS VULNERABLE DESIGNS AND MEANS TO ACHIEVE THEM

As a way out, we suggest that future nuclear power reactors should be less dependent on: properly designed safety systems and security measures as well as protection against external events of both natural and malicious/intentional origin, the adequacy of broader infrastructure, safety culture, operational modes and, *last but not least*, on the stability of our societies [2]. For this the following technical requirements are put forward:

- Elimination of potential reactivity induced accidents by reactor core design or at least controllability by passive means. This can be achieved by:
  - (a) subcritical systems (receiving additional neutrons from accelerator driven systems);
  - (b) weak, negative reactivity coefficients (graceful reaction on increasing fuel temperature, power, void fraction, burn up);
  - (c) small reactivity surplus at startup with fresh fuel; and
  - (d) fail-safe design of shutdown absorber rods.
- Forgiveness against loss of active core cooling, including total loss of power by reactor design and inherent/passive means. This can be done by:
  - (a) low power density and power size (to avoid exceeding critical temperature limits);
  - (b) strategies to avoid high fission product inventory, e.g., by dispersed fuel;

- (c) temperature resistant fuel cladding and structural materials;
  - (d) sufficient heat storage capability and inherent/passive heat transfer mechanisms in case of loss of normal (forced) cooling/loss of coolant (depressurization)/total loss of power; and
  - (e) passive decay heat removal systems.
- Securing structural integrity to avoid geometric disorders (losing core cooling capability) or loss of confinement of radioactive inventory. This can be obtained by:
    - (a) low primary circuit pressure or leak/rupture proof components (notably pressure vessel);
    - (b) radiation resistant and robust core structures; and
    - (c) underground siting for protection against extreme external impact.
  - Use of chemically non-reactive, non-toxic materials and fluids, or avoiding direct contact of reacting substances, e.g., by intermediate cycles.
  - Avoidance/incineration of long-lived radioisotopes (actinides) by fuel cycle designs allowing for reduced long-term stewardship. This can be achieved by:
    - (a) switching to fuel cycles (thorium) with drastically smaller generation of long-lived minor actinides, or waste burner core designs; and
    - (b) striving for enhanced closed fuel cycles or for long-term stable, high burn-up spent fuel as an open fuel cycle option.
  - Intrinsic proliferation resistance characteristics of the fuel, fuel cycle and related processes, inter alia by:
    - (a) avoiding the use of highly enriched uranium (HEU); and
    - (b) striving for online reprocessing, or facilities/processes including fuel fabrication at reactor location.

### 3. SMR CONCEPTS AND PRINCIPAL SAFETY CHARACTERISTICS

All types of large reactors, presently in operation, under construction or subject of intensive development, are represented in SMR (small modular reactor) lines. A comprehensive study of evolutionary (mostly water cooled), innovative/revolutionary (sodium or gas-cooled), and highly innovative/exotic (molten salt or lead cooled) designs was carried out, which focused on safety characteristics and their assessment against the strengthened requirements outlined before. Key characteristics and design specific features are depicted in Table 1 for selected concepts,

TABLE 1. CHARACTERIZATION OF BASIC DESIGNS APPROACHES, DISTINGUISHED BY COOLANT, AND WITH SPECIFIC SMR CONCEPTS TAKEN INTO CONSIDERATION

Design Approach	Evolutionary	Innovative - revolutionary		Highly innovative - exotic	
Characteristics/ Design Features	Water	Sodium	Gas (Helium)	Molten Salt	Lead
Selected concepts	mPower   NuScale	PRISM	HTR-PM	SaWB	BREST-OD- 300
- Neutron spectrum	thermal	fast	thermal	semi-thermal, fast	fast
- power density [MW/m <sup>3</sup> ]	<80	290 (?)	8	70	150
- pressure [MPa]	14.1   ?	unpressurized	80	unpressurized	unpressurized
- type	pool	pool; IHX	loop	pool, overflow tank; IHX	loop
- purpose	burner	waste burner	burner	waste burner	converter
- fuel (enrichment)	UO <sub>2</sub> (5%)		(U, Th)O <sub>2</sub>		(U+Pu)N

Design Approach	Evolutionary	Innovative - revolutionary		Highly innovative - exotic	
Characteristics/ Design Features	Water	Sodium	Gas (Helium)	Molten Salt	Lead
Selected concepts	mPower   NuScale	PRISM	HTR-PM	SaWB	BREST-OD-300
- power size	180 MWe   50 MWe	(U, TRU)O <sub>2</sub> (15%) 311 MWe	(8.5%) 100 MWe	U, Th, TRU dis- solved in salt 50 MWt	300 MWe
- basic safety approach	integral design passive	passive	inherent/ passive	inherent/ passive	inherent/passi ve
- cladding/ structural material	metallic	metallic	ceramic	salt - metallic	metallic
- construction	factory	factory	on-site/ factory	factory	on-site
- siting issues (reactor)	underground	underground	underground	underground	above ground

Based on mostly preliminary information, a more specific assessment of selected SMR concepts has been made by evaluation against strengthened technical requirements/design criteria. The results (see Table 2) indicate a high potential for far-reaching improvements compared to most

TABLE 2. ASSESSING SELECTED SMR CANDIDATE CONCEPTS AGAINST STRENGTHENED REQUIREMENTS

Key requirements	Candidate reactor concepts – varying coolant				
	Water Large EPR	Sodium – fast (PRISM)	Molten Salt – fast (SaWB)	Helium – thermal (HTR-PM)	Lead – fast (BREST-OD-300)
Elimination of Reactivity Induced Accidents	+	-(-)	--	++	-(~)
Forgiveness against Loss of Active Core Cooling	--	-	~	++	-(~)
- avoid exceeding critical temperatures	--			++	
- avoid high fission product inventory	--	+1	++2	+1	+1
- provide sufficient heat storage & transfer capacity	+	++	+	+	++
Structural Integrity	-(-)	+	+	++	+(+)
- avoid high operating pressure	--	+3	++	+	+3
[suitability of underground siting]	[-]	[?]	[++] <sup>4</sup>	[++] <sup>4</sup>	[+]
Use Non-chemically Reactive/ Toxic Materials	+	--5	-5 (-) (non-stable)	++	+
Avoid Long-lived Radioisotopes	--	+	++	+	++



Key requirements	Candidate reactor concepts – varying coolant				
	Water Large EPR	Sodium – fast (PRISM)	Molten Salt – fast (SaWB)	Helium – thermal (HTR-PM)	Lead – fast (BREST-OD-300)
Enhance Proliferation Resistance - avoid high enriched uranium	+	-	-	~	-
	++	-(-)6	-(-)6	-(-)6	-(-)6

<sup>1</sup> due to small power size

<sup>2</sup> in case of dispersed fuel & due to small power size

<sup>3</sup> not pressurized but high static load

<sup>4</sup> foreseen

<sup>5</sup> intermediate cycle (IHx) foreseen

<sup>6</sup> close to HEU lower limit

advanced large light water reactors like the EPR, which here serves as a benchmark, and that may finally achieve very ambitious and challenging specifications, although not fulfilling all of them yet, and may prove less proliferation resistant.

#### 4. REGULATORY APPROACH AND NEED FOR MODERNIZATION

Most developers pretend to basically apply well-established safety objectives and fundamental principles for their concepts, notably the defense in depth principle. However, they claim that classical approaches are inappropriate, too burdensome, need to be adapted to the characteristics of the particular SMR concept, and need to become more efficient<sup>1</sup>, for the small water reactors the least.

To come up with an independent appraisal, we made reference to the technical safety objective and the strategy of defense in depth as one of the fundamental principles, all developed within the IAEA-INSAG framework /4/ and widely accepted as the regulatory basis for existing plants. Then we contrasted key safety characteristics of large water-cooled nuclear power plants (EPR as an example) with those of highly innovative revolutionary – exotic SMR concepts, highlighted before. Obviously to prevent, with high confidence, accidents in nuclear plants, and to pay special attention to severe accidents with serious radiological consequences are objectives, commonly shared by all plant designers. However, for current designs it has been assumed that the prevention of accidents cannot be totally successful and additional protection has to be achieved by the incorporation of many engineered features into the plant to cope with design basis accidents /4, para 21/; the likelihood of even multiple failures of provided redundant active safety systems, and resulting serious accidents, has to be proven small as one of the key requirements within the regulatory process. Most of the SMR designers argue that, due to favorable physical properties and inherent safety features or at least passive rather than active safety systems, such failures can be excluded. And, to exaggerate, severe core damage accidents and serious releases of radioactive substances, triggered by „classical“ accident scenarios, in particular loss of core cooling accidents, e.g., following station blackout conditions, can be deterministically excluded.

Along these lines the defense in depth principle (which centered on several levels of protection including successive release barriers) has been applied in existing plants to compensate for potential human and mechanical failures. Most SMR designers do not question the relevance of this concept, but claim to re-assess the vulnerability of barriers and the necessary lines of defense, e.g., whether (i) the failure of the primary circuit/pressure vessels must be assumed in case of unpressurization and (ii) the loss of the first barriers, i.e. the fuel and fuel cladding, must be assumed in case of temperature resistant fuel elements (i.e. coated particles and ceramic fuel balls of HTR-PM). Most SMR do not deny the need for secondary safety containment, in principle, but discuss the adequacy of current design requirements such as leak tightness, though the HTR-PM safety concept relies on „one line of defense“.

In general, we largely share this reasoning. Also in our view there is clear evidence that a pure application of current regulatory requirements and best practices is not meaningful and poses unnecessary (economic) barriers to the deployment to most of the SMR concepts. However, their adaptation to the innovative safety features of most of the considered designs poses challenges, that are hard to achieve: Relying on other/reduced lines of

---

<sup>1</sup> In the USA the Nuclear Energy Innovation and Modernization Act aims to modernize the NRC „to bring increased efficiency and fiscal accountability ...“

defense, replacing active safety systems by inherent/passive mechanisms, claiming reduced or no emergency planning zones, etc. result in a shift of safety proofs to material properties (often at extreme conditions), demonstration of sufficient quality/validity of small and large-scale experiments and computer codes. Eliminating “classical” accident scenarios and design base accidents raises the question of sufficient completeness of accident scenarios taken into consideration including new, concept-specific accident scenarios, etc. – all under constraints of lack of sufficient knowledge and experience, and under increased uncertainties. For most fast reactor concepts, reactivity induced accidents deserve special attention and measures. Furthermore, some concepts are closely linked to elements of the fuel cycle (e.g., the molten salt reactors with on-line chemical reprocessing) and use highly enriched fuel, foresee below ground siting and off-site fabrication, introducing new conditions and challenges, respectively.

## 5. CONCLUSIONS

Our investigations into selected SMR concepts in general, and highly innovative concepts in particular, have indicated a high potential to meet extremely ambitious safety requirements. They also highlighted and confirmed safety features, which are significantly different from those of existing large power plants. Therefore the regulatory framework for very promising SMR concepts must be re-thought to avoid unnecessary burden and obstacles for the development and commercial deployment, for water-cooled bridging technologies the least. The adaptation of basic safety principles and regulatory requirements as well as education and training of the respective staff turned out to be a huge technical and organizational challenge and need to be taken up in a timely fashion, provided that the interest in SMR is real and continued.

## REFERENCES

- [1] WHEATLEY, S., KRÖGER, W., SORNETTE, D., Comprehensive Nuclear Events Data Base: Safety and cost perspectives, Proc. ESREL, Slovenia (2017).
- [2] SORNETTE, D., A civil super-Apollo project in nuclear R&D for a safer and prosperous world, Energy Research & Social Science, **8** (2015) 60.
- [3] WORLD NUCLEAR ASSOCIATION, Small Nuclear Power Reactors, WNA (2017).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Basic safety principles for nuclear power plants, 75-INSAG-3 rev. 1, INSAG-12, IAEA, Vienna (1999).

## STUDY ON PLUME EMERGENCY PLANNING ZONE DETERMINATION FOR CAP200 SMALL MODULAR REACTOR

W. XUAN, L. LIAO, D. SUN

Shanghai Nuclear Engineering Research & Design Institute

Shanghai, China

Email: wangxuan@snerdi.com.cn

### Abstract

In China, due to the requirement of "Criteria for emergency planning and preparedness for nuclear power plants: Part1, The dividing of emergency planning zone." (GB/T 17680.1-2008), for PWR nuclear power plant, its external plume EPZ should be within 7km-10km, and its internal plume EPZ should be within 3km~5km. However, the scope of the standard for the emergency planning area is currently limited to conventional nuclear power plants, and for the current SMR, its emergency planning size is not included.

The paper presents emergency planning zone (EPZ) sizing method for Small Modular Reactor (SMR), as well as NNSA requirement, calculation process, the probability of accident truncation and the choice of meteorological data, and gives suggestions on EPZ determination for CAP200 SMR.

The paper also gives a case study, and Shidaowan nuclear power plant is chosen as the study site. According to the CAP200 source term and meteorological data of the site, use MACCS2 computer program to calculate the severe accidents consequence. Conclusion show that project dose exceeding probability is less than 30% at the distance of 500m, which directs that for CAP200 SMR, its plume emergence is limited to the on-site area, and off-site emergency response can be simplified.

## 1. INTRODUCTION

Nuclear power plant off-site emergency plan is the last step of the nuclear safety principle, which is very important to protect the safety of the public and protect the environment. The emergency planning zone is an important technical basis and main issue for making emergency plan. According to requirement of China standard "Criteria for emergency planning and preparedness for nuclear power plants-Part1: The dividing of emergency planning zone." (GB/T 17680.1-2008) [1], after taking into account for the reactor power, internal plume emergency planning zone should be within 3km~5km, and external plume emergency planning zone should be within 7km~10km. However, this standard is limited to large pressurized water reactor nuclear power plant, but for the current small reactor, it does not give instructions.

Compared to large reactors, SMR can achieve higher safety, shorter construction cycle time, better economy and application flexibility than the traditional pressurized water reactors, and SMR can also be applied to different requirements and conditions, it is a new nuclear energy system. SMR can meet the needs of small and medium-sized grid power supply, urban heating, industrial process heating and desalination and other special areas [2].

In the paper, case study of CAP200 is used to illustrate the calculation process of SMR plume emergency planning zone, and give recommendations for its size.

## 2. GENERAL METHODS AND CRITERIA FOR THE DETERMINATION OF PLUME EMERGENCY PLANNING ZONE

### 2.1. Concept of emergency planning zone

The emergency planning zone refers to the area that has been set up around the nuclear power plant in advance to formulate contingency plans and make emergency preparedness to protect the public in a timely and effective manner in the event of an accident at the nuclear power plant. The emergency planning area generally includes the plume emergency planning zone and the ingestion emergency planning zone. China's plume emergency planning zone is divided into internal and external areas, in the internal area, evacuation and other emergency protection measures should be prepared. Since the ingestion and drinking water control is not a "short term emergency" protection strategy, and the determination method of ingestion emergency planning zone is

similar to the plume emergency planning zone, thus, this paper mainly studies and discusses the division means of CAP200 plume emergency planning zone.

## 2.2. Method of determining emergency planning zone

Whether the large PWR or SMR, the method to determine the emergency planning zone is usually divided into three steps: firstly, choose suitable accident type and source term; secondly, estimate individual project dose and averted dose during the early plume exposure; thirdly, compare the estimated dose level and the contamination level with the generic optimization intervention level, then determine the size of EPZ.

In addition to the requirements of "Criteria for emergency planning and preparedness for nuclear power plants-Part1: The dividing of emergency planning zone." (GB/T 17680.1-2008), the (NUREG-0396) report [3] issued by the National Nuclear Regulatory Commission (NRC) and the white paper for the establishment of the Small Modular Reactor Emergency Response Plan zone issued by NEI [4] are also considered. NUREG-0396 noted that at the recommended emergency planning zone boundary, the probability of dose exceed the corresponding intervention level should be less than 30% during the entire core melt accident sequence. The NEI White Paper states that the cutoff probability of a severe accident can be  $1\text{E-}07$  / year in the case of a SMR emergency planning zone determination.

"Principles for the Safety Review of SMR(Trial) in China" [5] states: Under the condition of not taking off-site interventions, the public should be provided with higher off-site intervention levels than large PWR nuclear power plants. For an important sequence of the beyond design basis accident, the effective dose for individuals (adults) at the site boundary should be less than 10 mSv throughout the entire accident.

## 3. CAP200 PLUME EPZ DETERMINATION

### 3.1. Site overview

In the paper, Shandong Shidaowan nuclear power plant site is chosen as anc case study site, to illustrate the calculation process of CAP200 SMR plume EPZ. Shidaowan nuclear power plant site is located in Weihai City, Shandong Province. The site is about 120km away from Yantai City in the northwest, about 68km away from Weihai City in the northwest, about 23km away from Rongcheng City in the northwest and about 105km away from Shandong Haiyang Nuclear Power Plant in the southwest. The site is near the Yellow Sea, most of the natural ground elevation is between 0m~30m.

The site's dominant wind direction is SSW, calm wind frequency is 3.9% and the average wind speed is 3.63m/s.

### 3.2. Choose of accident type

When calculating the CAP200 plume EPZ, its input conditions include the total core inventory, release share, accident probability, meteorological condition, distance segment, etc. The core inventory of CAP 200 is calculated using the "total amount of radioactivity at the end of the compact reactor cycle", which has the similar severe accident prevention and mitigation strategy as the CAP1000 reactor type and a similar containment leak rate. Its severe accident sequence is also consistent. The severe accident source term of CAP200 reactor contains six release classes. The following table gives a description of the six accidents types and their release frequency.

TABLE 1. CAP200 SEVERE ACCIDENT RELEASE CATEGORIES

Release type	Name	Description	Frequency (/reactor.yr)
IC	Complete containment	The containment remains intact, and conventional leaks cause the release of radionuclides into the environment.	$1.78\text{E-}07$

Release type	Name	Description	Frequency (/reactor.yr)
BP	Containment bypass	Containment failure occurs before the core damage, fission products from the reactor coolant system through the secondary circuit or other connecting system into the environment.	6.53E-09
CI	Containment isolation	Containment failure occurs before the core damage, because the failure of closure of the containment or the valve, leading to fission product release.	3.19E-10
CFE	Early failure of containment	The release of fission products into the failing containment is caused by a dynamic severe accident after the core has melted (before core collapse).	9.05E-09
CFI	Medium term containment failure	The release of fission products to the failure containment was caused by a dynamic severe accident after the core was melted (after the collapse of the core, 24 h before).	2.08E-10
CFL	Late containment failure	The release of fission products to the failure containment was caused by a severe accident after 24 hours.	5.96E-11

It can be seen from the above table that only the release frequency of the IC accident sequence in the six release categories exceeds  $1\text{E-}07$  per site year. According to the NEI white paper, the cutoff probability of severe accident for the SMR is  $1\text{E-}07$  per site year, thus, for CAP200, only the IC accidents is considered.

### 3.3. Methods and parameters

When calculating CAP200 plume EPZ, MACCS2 computer program is used. The MACCS2 program was developed by the US Sandia National Laboratories for the US Nuclear Regulatory Commission (NRC), its purpose is to calculate the off-site consequences of severe accidents.

MACCS2 program is an important component of the three-stage PSA study in nuclear power plants. MACCS2 computer model consists of three basic modules which are ATMOS, EARLY and CHRONC. The ATMOS module mainly calculates the diffusion and transport of plume. The EARLY module mainly calculates the early dose, acute health effects and gives early emergency response actions. The CHRONC module mainly calculates long-term dose, chronic health effects, medium and long-term emergency response actions, as well as the economic costs. This paper mainly uses ATMOS and EARLY two modules. The main calculation parameters are as follows:

#### 1) Weather sequence

Based on the MACCS2 program's data entry requirements for atmospheric diffusion and transport, meteorological data is based on yearly data from the site tower observations, including hourly data such as wind direction, wind speed, stability, and precipitation.

The Monte-Carlo sampling method is used to classify the meteorological data. The weather classification is divided into 32 classes, and four representative weather series are extracted from each category. Therefore, the total number of representative weather series are 128.

#### 2) Atmospheric diffusion parameters and mixing layer height

Atmospheric diffusion parameters of the site are in Table 2, mixed layer height is in Table 3.

TABLE 2. DIFFUSION PARAMETERS RECOMMENDED VALUE  $\Sigma Y = AX^B$ ,  $\Sigma Z = CX^D$ 

Stability	Horizontal diffusion parameter ( $\sigma_y = ax^b$ )		Vertical diffusion parameter ( $\sigma_z = cx^d$ )	
	a	b	c	d
A	0.300	0.933	0.143	0.972
B	0.247	0.931	0.176	0.871
C	0.218	0.919	0.197	0.784
D	0.169	0.906	0.209	0.725
E	0.115	0.909	0.140	0.723
F	0.093	0.896	0.119	0.678

TABLE 3. MIXED LAYER HEIGHT

Stability	A	B	C	D
Mixing layer. height (m)	900	900	350	200

### 3.4. Results

The figure below shows the results of IC accident.

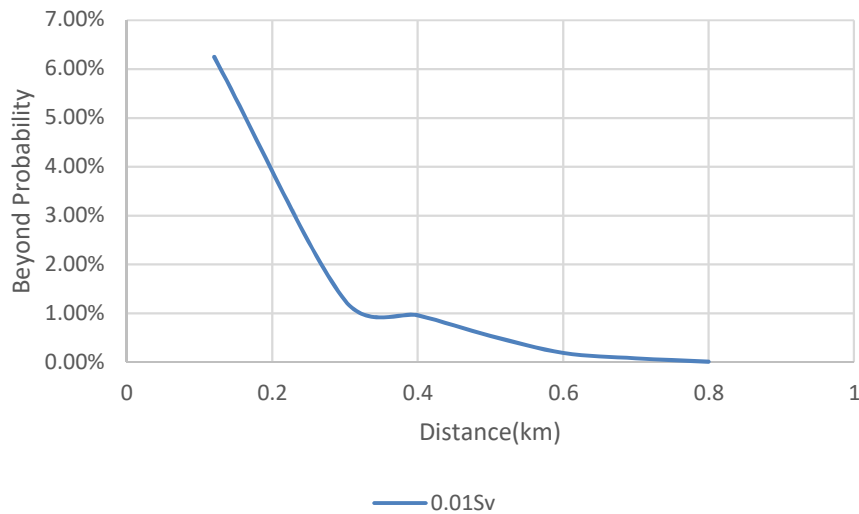


FIG. 1. Project dose exceeding probability.

It is calculated that the conditional probability of effective dose exceeding 10mSv is 1.26% at 300m, 0.54% at 500m, and only 0.01% at 800m. The plant boundary of CAP200 is 500m. Thus, according to the calculation results, the probability of the effective dose higher than 10mSv at 500m from the center of CAP200 reactor is far less than 30%. This indicates that for CAP200 SMR, its plume EPZ is limited to the site area and the off-site emergency response can be simplified accordingly.

## 4. CONCLUSION

This paper chooses Shidaowan nuclear power plant as a case study site, and CAP200 plume EPZ is calculated. The core inventory of CAP 200 is calculated using the "total amount of radioactivity at the end of the

compact reactor cycle", and for CAP200 reactor type, only IC severe accident should be considered during the determination of plume EPZ.

The plant boundary of CAP200 is 500m, according to the calculation results, the probability of the effective dose higher than 10mSv at 500m from the center of CAP200 reactor is far less than 30%. This indicates that for CAP200 SMR, its plume EPZ is limited to the site area and the off-site emergency response can be simplified accordingly.

Because the meteorological conditions at different sites have certain influence on the calculation of accident consequences, results of this paper only reflect the specific characteristics of the coastal site, and other sites still need to be analyzed according to the site characteristics.

## REFERENCES

- [1] National Standard of the People's Republic of China, Criteria for emergency planning and preparedness for nuclear power plants, Part 1: The dividing of emergency planning zone, GB/T 17680.1-2008, China (2008).
- [2] DONG, F., WANG, W., LUO F., WU, Q., Study on SMR EPZ determination. Research and Discussion, **1** (2014) 7.
- [3] US NUCLEAR REGULATORY COMMISSION, Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light Water Nuclear Power Plants, NUREG-0396, Washington, DC, USA (1978).
- [4] Establishment of the Small Modular Reactor Emergency Response Planning.
- [5] Principles for the Safety Review of SMR (Trial) in China.

## **PREPARING FOR SMALL MODULAR REACTOR APPLICATION REVIEWS: NRC PERSPECTIVE**

A. BRADFORD  
U.S. Nuclear Regulatory Commission  
Rockville, MD, USA  
Email: [anna.bradford@nrc.gov](mailto:anna.bradford@nrc.gov)

### **1. INTRODUCTION**

The U.S. Nuclear Regulatory Commission (NRC) has spent the last several years preparing to review applications for small modular reactors (SMRs). The NRC is implementing new guidance to assist the staff in focusing on review areas that are unique to SMR designs. The staff identified policy and technical issues that needed to be resolved to support design certification and combined license reviews for SMRs and has actively engaged the industry, and the SMR vendors in particular, to fully define the issues and to explore viable approaches to their resolution. The NRC is implementing an enhanced safety-focused approach to reviewing SMR applications that considered regulatory requirements, safety margin, defense-in-depth, risk insights, safety classification, and performance monitoring. It focuses review time and resources on the most important contributors to safety and adds to the effectiveness of the NRC's review. The NRC conducted pre-application readiness assessment audits for an SMR early site permit application and for an SMR design certification application. Finally, the NRC worked with the International Atomic Energy Agency (IAEA) to develop the SMR Regulators' Forum that will be used to develop position statements on key issues for suggested revisions to existing, or development of new, IAEA documents.

Currently, the NRC is reviewing a design certification application for the NuScale SMR. This review began in March 2017. The NRC is also reviewing an application for an Early Site Permit (ESP) for the Clinch River site; this ESP application is based on the eventual siting of an SMR at that site. This review began in January 2017. Although both of these reviews are in the early stages as of the date of this paper, the NRC expects that they will proceed effectively and efficiently due to the preparation activities that are discussed below.

### **2. PRE-APPLICATION INTERACTIONS**

The NRC's final policy statement on the regulation of advanced reactors states: "To provide for more timely and effective regulation of advanced reactors, the Commission encourages the earliest possible interaction of applicants, vendors, other government agencies, and the NRC to provide for early identification of regulatory requirements for advanced reactors and to provide all interested parties, including the public, with a timely, independent assessment of the safety and security characteristics of advanced reactor designs. Such licensing interaction and guidance early in the design process will contribute towards minimizing complexity and adding stability and predictability in the licensing and regulation of advanced reactors."

Early resolution or identification of a clear path to resolution for issues related to SMRs will enable designers to incorporate appropriate changes during the development of their designs before submitting a design certification or license application. Accordingly, the NRC has been interacting with designers of new SMRs to become familiar with the new designs and technologies, and to provide feedback on potential key design, technology, and licensing issues and on their technology development program plans. These interactions also provide information to assist in determining NRC infrastructure development and research needs and plans.

The NRC also conducted SMR workshops with SMR designers, the Department of Energy, the industry, and other stakeholders to discuss potential policy issues that are common to more than one design. The staff encouraged the participants to work together or with other organizations to generically address issues common to all nuclear designs in order to focus the issues, propose and obtain consistent resolutions, and effectively use resources.

As a result of these pre-application activities, the NRC staff identified a number of potential policy and licensing issues based on the preliminary design information. In general, these issues resulted from key differences between the new designs and current-generation pressurized-water reactors (such as size, moderator, coolant, fuel design, and projected operational parameters), but they also resulted from industry-proposed review-approaches



and industry-proposed modifications to current regulatory policies and practices. Specific examples of issues identified are emergency preparedness zone size, license structure for multi-module facilities, operator staffing, and licensing of prototype reactors.

After these issues were identified, the NRC developed approaches for resolving each issue. Some of the issues were able to be resolved after more in-depth consideration of the current regulatory framework, while others required design-specific solutions. For example, for multi-module licensing, the NRC determined that it preferred to license each module individually, but that it would remain open to considering other approaches proposed in the future by specific applicants.

### 3. GUIDANCE DEVELOPMENT

The NRC has revised or developed guidance documents in support of SMR reviews. For example, the NRC determined that it would be advantageous to more fully integrate the use of risk insights into pre-application activities and the review of applications. Therefore, the Commission directed the staff to develop a design-specific, risk-informed review plan for each SMR design to address review activities, which the NRC has implemented by developing new Design Specific Review Standards (DSRS). The DSRS uses design-specific information, which was gleaned from pre-application interactions with the reactor designer, to focus the NRC review appropriately. The NRC developed a new Part 2 to the Introduction of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," which provides a methodology to apply a graded review approach to SMR systems and components in consideration of the safety and risk significance. Where the guidance has been modified, sections of the DSRS are used in place of the corresponding sections in NUREG-0800.

The DSRS reflects NRC staff safety review methods and practices which integrate risk insights and, where appropriate, lessons learned from the NRC's reviews of previous design certification and license applications, and are tailored to the particular SMR design. For example, if a SMR design does not have reactor coolant pumps, then the DSRS would reflect how the NRC expects to review the application areas that are related to that topic. Additionally, reviewers have the flexibility to adjust the graded review approaches based on application specifics. The development of a DSRS is not a requirement but rather is decided on a case-by-case basis for each design.

The NRC issued a draft DSRS for public comment for the mPower SMR design in 2013. However, the draft DSRS was not finalized due to the fact that mPower decided to suspend their pre-application activities with the NRC.

The draft DSRS for the NuScale design was issued for a 60-day public comment period in 2015. The NRC received approximately 700 comments, the vast majority of which were from the NuScale company. The final NuScale DSRS was issued in 2016 and is being used by the NRC staff during the ongoing review of the design certification application.

In addition to the development of DSRS guidance, the NRC also developed new guidance on pre-application readiness reviews. Pre-application readiness reviews are conducted approximately six months before the applicant is planning to formally submit its application, and it is a voluntary activity. The intent is to identify information gaps between the draft application and the technical content expected to be in the final application submitted to the NRC, identify major technical or policy issues that may adversely impact the docketing or technical review of the application, and become familiar with the application, particularly in areas where prospective applicants are proposing new concepts or novel design features. The NRC has found pre-application readiness reviews to be helpful in improving the quality of the application and in planning NRC resources in preparation for the application review.

### 4. ENHANCED SAFETY-FOCUSED REVIEW

Another approach that the NRC is using for its current SMR application review is the Enhanced Safety-Focused Review (ESFR). This continues the NRC's long-standing approach of considering regulatory requirements, safety margin, defense-in-depth, risk insights, safety classification, and performance monitoring when determining main areas of focus during reviews. It focuses review time and resources on the most important contributors to safety and adds to the effectiveness of the NRC's review. In order to develop the specifics of the ESFR, the NRC established a working group in 2016 to consider current design information and to encourage a

holistic review approach. The working group included members from each organizational unit that would be involved in review of an SMR application.

The ESFR working group developed tools that could be used by the application reviewers to assist in determining the level of review needed. For example, a structures, systems, and components (SSC) tool aided the reviewers in evaluating whether more or less focus was needed on a particular SSC. The working group experts also evaluated which areas of the SMR application would likely be more challenging to review (based on aspects such as first-of-a-kind approaches, lack of operating experience, new methodologies, etc) or would likely require a reduced review effort (based on design changes, large margins, simpler approaches, etc).

As an SMR application review continues, the ESFR will help to ensure that the NRC remains focused on the most important areas of the design, and will promote a consistent review approach throughout the entire review.

## 5. SMR REGULATORS FORUM

In preparing for SMR applications, the NRC believes that there is value in sharing insights with other regulators internationally. Therefore, the NRC assisted in the establishment of the SMR Regulators Forum at the International Atomic Energy Agency. The goals of the forum were to establish an understanding of each member's regulatory views on common issues to capture good practices and methods, enabling regulators to inform changes, if necessary, to their requirements and regulatory practices. This will help enhance safety and efficiency in licensing. The forum would also document and disseminate the results of the discussions, and interact with key stakeholders to effectively inform the forum activities.

The forum was formed in 2015 and the members are Canada, China, Finland, France, the Republic of Korea, the Russian Federation, the United Kingdom, and the United States. A representative from the NRC was the Chairperson of the forum and led a series of meetings over the last two years. The forum has separate working groups that focused on the areas of graded approach, defense-in-depth, and emergency planning zones.

The forum has issued a report that addresses these three areas and has developed proposals for future work areas for the forum to undertake. The NRC has found participation in this group to be useful as the agency was preparing to receive SMR applications.

## 6. SUMMARY

The NRC has spent the last several years preparing to review applications for SMRs. The preparations include pre-application interactions with identification and resolution of policy and technical issues, the development of design-specific guidance, the formation of an internal working group to promote an enhanced safety-focused review, and participation in an international SMR regulators' forum. Throughout the pre-application and application phases, the NRC encourages frequent and substantive interactions with SMR designers and other stakeholders because such communications improves the efficiency and effectiveness of the review process. The NRC is now well positioned to review SMR applications.



## IAEA SMR FOCUSED INITIATIVES

**Chairperson**

**W. KRÖGER**  
Switzerland



## SMR REGULATORS' FORUM PILOT PROJECT REPORT

### *Considering the application of a graded approach, defence-in-depth and emergency planning zone size for Small Modular Reactors*

S. MAGRUDER  
International Atomic Energy Agency  
Vienna, Austria  
Email: S.Magruder@iaea.org

D. JACKSON  
United States Nuclear Regulatory Commission  
Washington, DC, United States

K. HERVIOU  
Institute for Radiological Protection and Nuclear Safety  
Paris, France

M. DEVOS  
Canadian Nuclear Safety Commission  
Ottawa, Canada

S. COOK  
Canadian Nuclear Safety Commission  
Ottawa, Canada

P. DUPUY  
Institute for Radiological Protection and Nuclear Safety  
Paris, France

K. THOMAS  
United States Nuclear Regulatory Commission  
Washington, DC, United States

#### **Abstract**

The SMR Regulators' Forum was formed in 2015 to understand key challenges that are emerging in Small Modular Reactor (SMR) regulatory discussions. A 2-year pilot project was launched to understand each member's regulatory views on common issues, to capture good practices and methods. This would enable regulators to inform changes, if necessary, to their requirements and regulatory practices. The following issues related to SMRs have been addressed: graded approach, defence-in-depth and emergency planning zones. Key Conclusions of the Forum so far are that most national regulatory frameworks already enable applying a graded approach for all nuclear installations including SMRs. Accordingly, the Forum considers that the defence-in-depth concept and principles are still valid for SMRs. There is also a need to have a coordinated response should an accident in the plant challenge public safety and the environment. Therefore, EPZ should exist around SMR, even if possibly reduced regarding large NPPs. The paper identifies additional areas of interest for future work of the forum such as exploring where efficiencies can be gained by sharing of information and closer cooperation between regulators.

#### **1. INTRODUCTION**

There is a sustained global interest in small modular reactors (SMRs), which are expected to play an important role in globally sustainable energy development as part of an optimal energy mix. Such reactors have the potential to enhance energy availability and security of supply in both countries expanding their nuclear energy programmes and those embarking on a nuclear energy programme for the first time.

Today, SMR technology is rapidly evolving and the regulatory guides and process to assess this emerging technology are lagging and in some cases not yet available. In the future, robust, technology neutral regulatory review methodologies would be beneficial to minimize the time to adopt and commercialize new nuclear technologies.

The International Atomic Energy Agency (IAEA) has several dedicated projects and activities supporting the licensing and safety issues of SMRs in Member States. Over the years, the IAEA has produced a number of major publications and has convened a series of international forums addressing a variety of SMR issues. The SMR Regulators' Forum was formed in 2015 to understand key challenges that are emerging in Small Modular Reactor (SMR) regulatory discussions. A 2-year pilot project was launched to understand each member's regulatory views on common issues, to capture good practices and methods. Canada, China, Finland, France, Republic of Korea, Russian Federation and United States participated in this pilot project, with the IAEA ensuring the scientific secretariat. The steering committee was chaired by the US NRC and the IRSN.

The paper presents the conclusions and recommendations of the SMR Regulators' Forum Pilot Project that met regularly between March 2015 and May 2017.

## 2. SCOPE OF THE PROJECT

Within the 2-year pilot project, the Forum addressed the following issues for both light-water and non-light-water reactor designs:

- 1) Graded approach: Regulators are being approached with SMR safety case proposals that are seeking to relax regulatory requirements for design and safety analysis. Therefore, there was a need to clarify the regulatory view of grading and what this means.
- 2) Defence-in-depth: A number of SMR designers are proposing alternate ways to address Defence-in-Depth (DiD) in their designs. The Forum looked at these approaches and attempted to develop common positions around certain regulatory practices to ensure that the fundamental principles of DiD are maintained.
- 3) Emergency Planning Zones (EPZs): on the basis of the alleged characteristics of SMRs, smaller EPZs are being proposed by some SMR vendors. The Forum examined existing practices and strategies for understanding how flexible (i.e., risk informed) EPZs are established in order to have a common position on this issue.

The goals of the pilot project were to establish an understanding of each member's regulatory views on common issues identified in the scope above to capture good practices and methods, enabling regulators to inform changes, if necessary, to their requirements and regulatory practices. Working groups addressed respectively the three above-mentioned issues. They adopted the following SMR Definition: Small Modular Reactors typically have several of these features:

- Nuclear reactors typically <300 MWe or <1000 MWt per reactor;
- Designed for commercial use, i.e., power production, desalination, process heat (as opposed to research and test reactors);
- Designed to allow addition of multiple reactors in close proximity to the same infrastructure (modular reactors);
- May be light or non-light water cooled;
- Claims of preventive measures to reduce risk, e.g., inherently safe fuel, enhanced coolants, practical elimination of situations that could lead to large releases has been achieved.

The IAEA publications on SMR designs serve as references for the discussion.

It should be noticed that the main limitations encountered by the Forum is the fact that development and deployment of SMRs around the world is at a very early stage in terms of maturity of technologies and varying degrees of activity occurring in Forum member countries. Another constraint was the lack of information from SMR design vendors on the implications of such things as new novel design principles and features (e.g., passive systems) and whether these challenged or complemented Defence-in-depth principles. For example, to what extent does a multi-module facility design include coupling of modules and sharing of systems? Are designers concluding that provisions for Defence-in-depth in levels 3 and 4 can be reduced in the presence of simple "inherently safe" design features normally associated with level 1?

### 3. MAIN FINDINGS FROM THE PROJECT

#### 3.1. Use of a Graded approach for SMR

The concept of Graded Approach is widely discussed in the IAEA safety framework including in documents applicable to nuclear power plants. Evidence of the use of a graded approach exists in the national regulatory frameworks for all SMR Regulators' Forum Member States in one form or another. Essentially, the Graded Approach means that the level of analysis, verification, documentation, regulation, activities and procedures used to comply with a safety requirement should be commensurate with the potential hazard associated with the facility without adversely affecting safety. In some cases, analyses may result in the need for less protective measures, but the opposite is also true.

Use of the Graded Approach can enhance regulatory efficiency without compromising overall safety by focusing on specific issues that are important to safety.

Applying a Graded Approach in reviewing an application for a license to perform a set of activities requires the regulatory staff to have a global understanding of a project, risks presented by activities and approaches to prevent and mitigate events following a defence-in-depth approach. The use of grading by both an applicant for a license and the regulator is heavily influenced by the information supporting the safety proposal. So-called 'proven' approaches and concepts are generally well supported and lend themselves to a more straightforward safety case assessment. In those cases, a regulator's technical assessment can then be focused on more innovative part of the facility where uncertainties are higher and additional margins or even safety and control measures may be needed. Generally, the more proven the approaches and concepts are in a new reactor design, the more straightforward and efficient the regulatory review will be. This presents a significant conundrum for developers of new technologies such as SMRs that utilize more advanced technologies with a goal to enhance both safety provisions and economic performance. In this case, the design may be composed of fewer systems, but these systems will seek to employ passive and inherent behaviours. The argument made by proponents is that this should lend itself to greater use of grading; however, in practice, these approaches are still developing the necessary evidence to demonstrate 'proven-ness'. Until the proven-ness has been established, it is difficult to claim credits for those features in a safety proposal because uncertainties need to be addressed and factored into the safety demonstration. In addition, regulatory attention in a technical assessment must factor in uncertainties from these proposals into licensing decisions. This is of particular importance for new SMR technologies, and particularly for demonstration projects and first-of-a-kind designs where uncertainties are greater. For example, a demonstration project generally integrates a number of novel features such as new fuels, passive and inherent features and compact arrangements of Structures, Systems and Components (SSCs). The intent is to demonstrate integrated performance and gather operating experience (OPEX) to further support safety claims and effectiveness of plant features. Lack of OPEX per novel feature increases uncertainties which are then individually reflected in safety analyses and affect the overall outcomes. The regulatory process would seek to understand how uncertainties are being addressed in the design and in operation until the OPEX has been generated and reviewed. In past practice, this has resulted in the need for supplemental measures in the demonstration plant such as greater safety margins, additional SSCs, restrictions on the operating envelope.

From a safety perspective, member regulators of the Forum agree that SMRs should be treated as Nuclear Power Plants (NPPs) and that the starting point in use of the Graded Approach is the requirements established for NPPs. In general, IAEA and national regulations requirements and guidance can be applied to activities referencing SMRs. Nevertheless, there may be a need for regulators to define specific requirements in special cases such as marine based facilities where different requirements are justified. Then, the way the applicant demonstrates that their requirements are met may be graded.

#### 3.2. Application of the Defence-in-depth concept

In general, all five DiD levels as defined for typical large Generation III NPPs and taking into account lessons learned from the Fukushima accident are also applicable to SMRs. Appropriate features should be included in the SMRs design at each level. In order to ensure the successive levels of DiD, and despite the efforts of SMR designers on DiD levels 1 and 2 reinforcement, it is important to get a clear demonstration of the effectiveness of the design safety features to mitigate postulated initiating events (level 3) and of the features to mitigate severe



accidents (level 4) for all operating modes. For DiD level 5, no matter how much other levels may be strengthened, effective emergency arrangements and other responses are essential to cover the unexpected.

The independence among DiD levels, as far as practicable, is considered to be an important requirement to enhance the effectiveness of DiD in international and national standards and documents. The Fukushima accident has confirmed and reinforced this requirement. Therefore, it should apply to SMRs as well. In the case of SMRs, it could be investigated whether the SMR specific features, in particular the compact design of the modules and the multi modules design, may particularly challenge the independence of DiD levels.

Taking into account SMR specific features, selected site characteristics could be an important challenge for DiD reinforcement. The design shall take due account of site-specific conditions to determine the maximum delay time by which off-site services need to be available. Siting aspects may have important influence on SMR safety design and different DiD levels due to applicable range of suitable site for SMR installations, including underground, underwater or floating on water. Moreover, new site configurations may require the evaluation of additional specific external hazards and environmental phenomena. For multi-unit/module plant sites, designs shall take due account of the potential for specific hazards giving rise to simultaneous impacts on several units/modules on the site.

Regarding design issues, an important challenge for DiD in SMR design is to achieve a well-balanced safety concept based on the use of optimal combination of active, passive and inherent safety features. All inherent safety characteristics that are provided by the design and credited in the safety demonstration should be duly substantiated by SMR designers. The requirements and criteria for this demonstration should be defined beforehand and developed, which may need particular guidance. The use of passive systems may induce new challenges: new innovative technologies without sufficient operational experiences, uncertainties related to qualification and reliability assessments, operational aspects as periodic testing, maintenance and in-service inspections. Particular attention should be paid to these issues at each of the design, construction and operation stages of SMRs. Further development of safety criteria and requirements may be necessary. This includes the application of failure criteria for safety functions involving passive systems. In case of uncertainties in passive features reliability or common cause failure mechanisms in active systems, a combination of active and passive safety systems may be desirable. Such a combination could even strengthen safety function performances at DiD levels 3 and 4 and improve the independence between those two levels.

Common mode events due to internal hazards and their influence on DiD levels independence should be considered, taking into account SMR design specifics (e.g., modules, compact design and multi units/modules aspects). Moreover, multi modules/units aspect should be considered in the safety assessment of internal and external hazards. As the concept of SMR “module” is not equivalent to the “unit” or “plant” concept for large reactors, the safety principles developed for the “multi-units” issue cannot be transposed to “multi-modules” in SMR facilities. Therefore, principles and requirements for the safety assessment of a “multi-module” SMR should be developed.

It is necessary to demonstrate that for “multi-modules” facilities, connections, shared features and dependencies among modules are not detrimental to DiD. A “multi-modules safety assessment” could contribute to verifying that all common features and dependencies don’t induce unacceptable effects.

Even if the SMR concept is based on modular design with small unique power on multi modules/units sites, the SMR design shall take due account of the potential consequences of several – or even all – units failing simultaneously due to external hazards. It may affect the methodology for EPZ assessment.

As for large reactors, probabilistic safety assessment (PSAs) should be used for SMRs to complement the deterministic approach on which the design relies first. PSAs could be used in particular to check that DiD principles have been properly applied. PSA results could reflect the reliability of the features implemented at each DiD level and the sufficient independence of the levels. PSAs could also be used for the identification of so-called complex DEC sequences and for the assessment of the risks induced by multi-modules. Therefore, methods to deal with passive features and with multi-module issues in PSAs should be investigated or enhanced.

Post-design activities were not discussed in detail. However, manufacturing and transportation are specific aspects to focus on for many SMRs. Since there is an increasing role of the manufacturer/producer of the main equipment of the module in the factory conditions, inspections performed in the factory are particularly important and new guidance for procedures for such inspections may need to be developed. A well planned and properly documented site acceptance testing and commissioning program should be prepared and carried out.

### 3.3. Emergency planning zone

Managing SMR events involving the potential for releases of radioactive material that challenge public safety and the environment indeed require a coordinated response. Therefore, the Forum considers that EPZ should exist around SMR, even if possibly reduced regarding large NPPs.

EPZ for SMRs is scalable depending on the results of a hazard assessment, the technology, novel features and specific design criteria, as well as for some, policy factors. The IAEA safety requirements and methodology for determining the EPZ size are effective in establishing an emergency preparedness and planning program, such that if a release does occur, protective actions will be implemented to protect the public and environment.

For SMRs without on-site refueling capability, there is a need to consider the establishment of an EPZ at any intermediate stop and land-based maintenance facility used for the handling and the storage of the fuel assemblies.

## 4. CONCLUSIONS AND RECOMMENDATIONS<sup>1</sup>

The Forum reached the following general conclusions and recommendations during the pilot project:

- a) From a safety perspective, SMRs should be treated as Nuclear Power Plants (NPPs), and the starting point in the use of the graded assessment approach should be the requirements established for NPPs.
- b) A fundamental principle for ensuring nuclear safety, the Defence-in-Depth concept, is valid for SMRs, and should be a fundamental basis of the design and safety demonstration of SMRs.
- c) The IAEA safety requirements and methodology for determining the EPZ size are effective in establishing an emergency preparedness and planning program, such that if a release does occur, protective actions can be implemented to protect the public and environment. However, it should be recognised that the same design of SMR implemented in different countries may result in different EPZ sizes.
- d) In many cases, it is not necessary to develop new licensing processes for SMRs, as the existing processes, with some minor programming efficiency applied, are sufficient.
- e) In order to better inform future work of the Forum, it should be encouraged, early in the next phase, to organize SMR safety information exchanges among designers, regulators and their TSOs, and to exchange information and share common positions on Defence-in-Depth with member states in an effort to enhance international harmonization, where possible.
- f) Significant benefit could be gained if the IAEA were to lead the development of a technical document that further explains what the Graded Assessment Approach is, how it is used to ensure safety for Nuclear Power Plants, including SMRs, how existing tools are used to develop high quality information to inform a decision making process, and confirming that it doesn't represent a reduction in overall safety of NPPs.

The pilot project report will be published as an IAEA non-serial report later this year.

---

<sup>1</sup> The opinions expressed in this paper — and any recommendations made — are those of the participants and do not necessarily represent the views of the IAEA, its Member States or the other cooperating organizations.

## APPLICABILITY OF IAEA SAFETY STANDARD SSR-2/1 TO WATER-COOLED SMALL MODULAR REACTORS

K. MADDEN

International Atomic Energy Agency

Email: K.Madden@iaea.org

S. MAGRUDER

International Atomic Energy Agency

Email: S.Magruder@iaea.org

H. SUBKI

International Atomic Energy Agency

Email: H.Subki@iaea.org

### Abstract

In 2016, the International Atomic Energy Agency (IAEA) conducted a study on the graded approach application of the IAEA design safety requirements contained in SSR-2/1, Safety of Nuclear Power Plants: Design, to small modular reactors (SMRs) with a focus on water-cooled and high temperature gas reactors. Each of the eighty-two SSR-2/1 design safety requirements were evaluated for their applicability to SMR designs by a team of international experts that included vendors, regulators and internal personnel. The approach utilized was to bin the requirements into one of the following five categories: applicable as is; applicable with modification; applicable with interpretation; new criteria; and not applicable. For water-cooled SMRs, proposed changes were made to thirteen SSR-2/1 design safety requirements and one new design safety requirement was suggested. The results of the study will be used as an input to the development of future IAEA safety standard review processes in order to reflect practices in this area and foster their practical applicability to SMRs.

### 1. INTRODUCTION

A continuously increasing interest in nuclear power has been obvious over the past several years in several Member States with already established nuclear power programmes, as well as in Member States at various stages of preparation or initiation of a nuclear power programme. At present, there are at least 50 SMR designs for which research and development (R&D) work is being undertaken. The following three industrial demonstration SMRs are in advanced stages of construction: CAREM, a 30 MW(e) PWR in Argentina; HTR-PM, a 250 MW(e) high temperature gas cooled reactor in China; and KLT-40S, a floating power unit in the Russian Federation. These designs are scheduled to begin operation between 2018 and 2020. Dozens of SMR designs are also being prepared for near term deployment, including the NuScale reactor, which is currently being reviewed for design certification in the United States, the SMART reactor developed by Republic of Korea and the ACP100 being developed in China. As a result of these different design approaches, technologies and safety features, Member States must establish new design safety requirements or apply their current design safety requirements to advanced reactor designs.

A study on the current practices of applying the IAEA Safety Standard SSR-2/1 design safety requirements to SMR technologies was organized by the IAEA and contributions were made by a team of international experts. The participants evaluated the application of SSR-2/1 design safety requirements to at-large SMR designs expected to be deployed in the near-term. This included the water-cooled reactor, water-cooled floating reactor and high temperature gas reactor SMR designs. The results of the study were then compiled and distributed to the team members prior to the consultancy meeting held at the IAEA headquarters in Vienna, Austria in February 2017. The consultancy was divided into two working groups representing the gas-cooled and water-cooled SMR designs. Each working groups developed a common understanding for each of the eighty-two design safety requirements in SSR-2/1 which is described here within. The participants developed contributions to a project report as a part of a home-based assignment to document the results of the consultancy meeting. The contributions related to water-cooled SMRs are documented within this paper. The contributions related to high temperature gas reactor SMRs are expected later this year. This input will be used in the development of future IAEA safety standards review process in order to reflect practises in this area and foster the practical applicability to SMRs.

## 2. WATER-COOLED SMALL MODULAR REACTOR GENERIC DESIGN DESCRIPTION

A SMR is generally defined as an advanced reactor that generates equivalent output capacity of up to 300 MW(e) and is designed in modules aiming for the economy of serial production. SMRs are derived from designs used in the design of standard nuclear power plants, including water-cooled, high-temperature gas cooled, liquid metal cooled with fast neutron spectrum, and molten salt-cooled reactors.

For water-cooled SMR designs, many of the designs adopt the integrated pressurized water reactors (iPWR) concept, for which due to the lower thermal power of up to 1000 MW(th), the components within the primary reactor coolant system (e.g. steam generators, pressurizer) can be installed within the reactor vessel together with the core. This integration of the primary cooling system is an approach to enable modular deployment. From a safety point of view, the potential for large and medium breaks, such as hot/cold leg, pressurizer surge line, and primary pump suction/discharge line breaks are eliminated by a function of design. While most of SMR designs are land-based, some countries are also pioneering in the development and application of floating and marine-based nuclear power plant powered by PWR-type (pressurized water reactor) SMRs. Innovative features allow SMRs to converge to provide safe, reliable and affordable plants and are described as follows:

- 1) Design Simplification and Compactness
  - (a) The integral configuration results in a lighter weight, better transportability and compact reactor. This integration yields substantial reduction in the size of the nuclear steam supply system (NSSS). Some iPWR SMR designs adopt natural circulation for the primary heat removal from the core. The need for primary pumps can then be eliminated; hence, loss of flow event due to pump failure is practically eliminated. Natural circulation also reduces mechanical complexity. Other designs adopt conventional forced convection either using horizontally or vertically mounted primary pumps at the reactor vessel through nozzles. In-vessel steam generator (SG) cartridges are adopted for all iPWR SMR designs. The once-through helical coil steam generator is one of the types being utilized and offers a larger heat transfer area in a compact geometry.
- 2) Enhanced Safety
  - (b) Most if not all PWR-based SMRs adopt passive safety systems, which are based on natural laws, such as gravity-driven and natural circulation (e.g. buoyancy force). The integral design of NSSS module eliminates external coolant loop piping, which eliminates the large-break loss-of-coolant accident (LBLOCA). The passive engineered safety features (ESFs) eliminate the need for external power under accident conditions. With these passive safety systems, small-break LOCAs do not significantly challenge the safety of the plant. The expected core damage frequency (CDF) is expected to be of the order of  $10^{-6}$  to  $10^{-8}$  per year; however, this needs to be confirmed by further detailed probabilistic safety analysis (PSA) as the designs evolve.
- 3) Economic Competitiveness
  - (c) SMRs are intended for specific markets in which large reactors would not necessarily be applicable or competitive. SMRs may provide an attractive and affordable nuclear power option for developing countries with small electrical grids and limited investment capability. The adverse impacts of the economy of scale is compensated by offering the economy of mass production of prefabricated modules, a simplified and standardized design, shorter construction time, less operation and maintenance cost, the option of incremental capacity increase, and cogeneration of electricity and process heat.

## 3. PROCESS

In 2016, the IAEA conducted a study on the applicability of the IAEA Safety Standard SSR-2/1, Safety of Nuclear Power Plants: Design, to SMR technologies; the study focused on water-cooled and gas-cooled SMRs. First, a home-based assignment verifying the applicability of SSR -2/1 to SMRs was completed by Member State participants. The Member States were asked to grade the applicability based on the following criterion:

- Applicable as is
- Applicable with modification
- Applicable with interpretation

- Not applicable
- New criteria

The difference between applicable with modification and applicable with interpretation should be noted. Applicable with modification infers that the text needs to be modified for the requirement to be applicable to the design; whereas, applicable with interpretation infers that the definition of a pre-existing word must be modified for that specific technology and therefore does not result in changes to the text. After determining the applicability of a requirement, participants were asked to provide input into what modification or interpretation was required, if any. Further, to aid in the understanding of the specific change, participants were also requested to provide rationale for said change. Following receipt of the participant's comments, the IAEA compiled said requirements into a common document for review at a consultancy meeting from 20 – 24 February 2017 in Vienna.

Based on the differences in technology, the February 2017 consultancy meeting was divided into two working groups; one for water-cooled SMRs and another for gas-cooled SMRs. Each group completed an intensive review of the received comments and developed a common understanding among participants for each of the comments requiring modification and/or interpretation. The working groups focused on addressing comments required as a result of direct changes required for their specific SMR technology. The working groups avoided changes where changed were solely related to the improvement of the document as a whole rather than a focus on the direct impact from a technology-specific viewpoint.

When reviewing the requirements, the working groups utilized a liberal interpretation of qualifiers, such as necessary and appropriate. Participants regarded these qualifiers as options allowing one to opt-out of said requirement should it be deemed unnecessary or inappropriate where required.

#### 4. AUDIENCE

The intended audience for this project report is Member State design organizations, technical support organizations, regulators and operators interested in developing a nuclear power plant programme or with an existing nuclear power plant programmes.

#### 5. SUGGESTIONS TO SSR-2/1 APPLICABILITY TO WATER-COOLED SMALL MODULAR REACTORS

Changes were recommended to about 15% of the SSR-2/1 design safety requirements. Note, the changes were developed with the assumption that standard water-cooled nuclear power plants and water-cooled SMRs would be included together in a future document; rather, than requiring a new design safety requirement standard to be developed that is exclusive to SMRs. Figure 1 provides the distribution of changes required in SSR-2/1 based on the suggestions made.

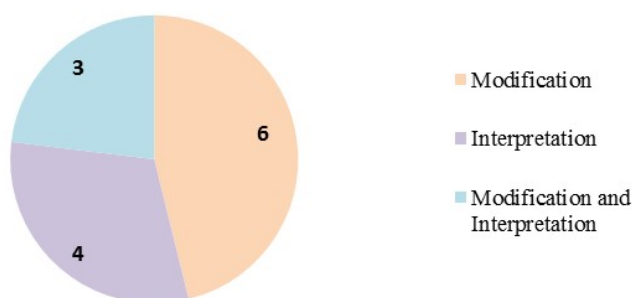


FIG. 1. SSR-2/1 Distribution for Recommended Changes.

A common theme was identified among the recommended changes to the SSR-2/1 design safety requirements. For a number of these suggestions, the contributing factor was related to the fact that several SMRs can be part of a single plant; thereby, allowing a nuclear power plant to have several cores. As such, the terminology “core,” “module,” “unit” and “plant” needs to be consistently applied throughout SSR-2/1. As a result of SMRs allowing for multiple cores within one plant, some requirements related to the location, segregation and

independence of safety systems were suggested for change. In addition, consideration for compactness of design had to be considered as this may affect access to containment at full power. Further changes related to emergency power supply systems were evaluated and augmented to consider that in the case of some SMR designs, safety features may not be dependent on electrical power. One of the benefits of SMRs is that these plants can be manufactured almost completely at a manufacturing facility as a result of simplified systems and smaller footprints. Other changes were suggested based on the option for a fleet solution to waste management given that several units may be considered for a site.

Table 1 provides a detailed list and explanations for the changes suggested to SSR-2/1 design safety requirements for water-cooled SMRs.

TABLE 1. SUGGESTED CHANGES AND NEW DESIGN SAFETY REQUIREMENTS FOR CONSIDERATION TO SSR-2/1

Requirement No.	Suggested Changes and New Design Safety Requirements for Consideration
11, Provision for Construction	<p><u>Proposed changes, suggestions or consideration to text:</u> In 4.19, change wording “in a provision of construction and operation” to “in a provision of manufacture and construction.”</p> <p><u>Interpretation required:</u> None.</p> <p><u>Justification for proposed modification and/or interpretation:</u> An industry viewed best practice is to manufacture SMR components and modules in a factory setting rather than to construct the entire plant at the final plant site. In this view, SMR power plants are in many cases being designed to optimize offsite manufacture of major portions of the nuclear power plant to leverage the value of this best practice. From this practice, multiple advantages are gained, including the:</p> <ul style="list-style-type: none"> <li>Ability to build more of the plant as modules in factories;</li> <li>Factory packaging of modules can ensure they arrive on site in an as expected state so that quality can be assured;</li> <li>Use of modules enables easier inspection to ensure that equipment and components are in an as expected state prior to installation; thus, ensuring quality and hence safety.</li> </ul> <p>With the implementation of factory manufacturing, there is a need for the inclusion of manufacturing as one of the provisions associated with this specific safety requirement. Additionally, Requirement 11 provides for, and is bounded by the aspects associated with the manufacture, construction, assembly, installation and erection activities and specifically does not include any necessity of recognizing the impacts of operations. To this end, “operation” is proposed to be removed from this requirement as proposed to ensure consistency of application of this safety requirement.</p>
12, Features to Facilitate Radioactive Waste Management and Decommissioning	<p><u>Proposed changes, suggestions or consideration to text:</u> In paragraph 5.15A, change the word ‘located’ to ‘located and/or segregated.’</p> <p><u>Interpretation required:</u> Broaden the interpretation of sources of internal and external hazards to include those that could arise from any connection to process heat facilities coupled directly to SMRs.</p> <p><u>Justification for proposed modification and/or interpretation:</u> The interpretation of the use of the word ‘located’ in the current requirement implies separation by distance. As SMRs are intended to be more compact nuclear power plants, protection against zonal effects can be provided by appropriate barriers as much as through separation by distance.</p> <p>Future applications of SMRs include the direct use of process heat from the power plant, e.g. for district heating, heat processing or water desalination. It is important to note that these additional connections are also potential sources of hazards.</p>

Requirement No.	Suggested Changes and New Design Safety Requirements for Consideration
17, Internal and External Hazards	<p>Proposed changes, suggestions or consideration to text: <i>Add a new sub-item:</i></p> <p>‘4.20A. Where there are multiple units of the same type, consideration should be given to the derivation of a fleet solution for waste management and the decommissioning process’.</p> <p>Interpretation required: <i>None.</i></p> <p><u>Justification for proposed modification and/or interpretation:</u> The requirement as currently written can be interpreted as applying only to a single nuclear power plant. SMRs by design could be built in larger numbers in a geographic area, and therefore, could enable a fleet solution to be derived for the effective and safe management of waste and the decommissioning process. This may enable consideration to be given to the construction of a single facility that is built solely for that purpose. Such a fleet facility would have greater throughput of waste thereby offering a greater opportunity for the application of advanced processing technology to reduce environmental impact.</p>
33, Safety Systems, and Safety Features for Design Extension Conditions, of Units of a Multiple Unit Nuclear Power Plant	<p><u>Proposed changes, suggestions or consideration to text:</u> Each unit, which may be comprised of one or more reactor cores, of a multiple nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.</p> <p><u>Interpretation required:</u> The term “unit” is interpreted to mean a single large reactor core and dedicated secondary and auxiliary systems. If the term “unit” can be interpreted (or defined via a glossary) as a collection of smaller reactor modules, then the wording of the original requirement is acceptable as written.</p> <p><u>Justification for proposed modification and/or interpretation:</u> SMRs introduce an additional level of reactor grouping than has been traditionally the case. Existing experience is to have a plant (or site) comprised of one or more single reactor units and associated secondary and auxiliary systems. SMRs introduce the possibility of units being comprised of multiple smaller cores with shared secondary or auxiliary systems. The safety requirements must be clear as to whether they pertain to an individual reactor primary system (module), a grouping of modules (unit) or the entire plant/site.</p>
45, Control of the Reactor Core; 46, Reactor Shutdown; 51, Removal of Residual Heat from the Reactor Core; 52, Emergency Cooling of the Reactor Core	<p>Proposed changes, suggestions or consideration to text: <i>None.</i></p> <p><u>Interpretation required:</u> The term ‘the reactor core’ can be one core or several cores.</p> <p><u>Justification for proposed modification and/or interpretation:</u> In case of an SMR, there may be several cores in one plant. Each of the cores in the plant shall be inherently stable. In a large NPP, we use ‘control of the reactor core’ even when there are more than one reactors located in the same plant. In the case, means for the removal of residual heat need to be provided for each core. The terminology of “core”, “module”, “unit” and “plant” needs to be consistent throughout SSR-2/1.</p>
57, Access to the Containment	<p><u>Proposed changes, suggestions or consideration to text:</u> Replace: “airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions” with “controlled and monitored access ways to ensure containment functionality during reactor power operation and in accident conditions.”</p> <p>Interpretation required: <i>None.</i></p> <p><u>Justification for proposed modification and/or interpretation:</u> Maintaining at least one door closed during reactor power operations and in accident conditions ensures reactor containment integrity is maintained during the time personnel access to the interior of containment is desired. Many SMR containments are not designed for any human habitation during power operations and are not equipped with large doors or equipment access hatches. Some, such as the NuScale Power Module, with its small volume containment vessel, utilizes by design, appropriately sized manway-like access hatches and openings rather than doors or airlocks.</p> <p>To ensure consistency in the intent of this safety requirement in its application to SMRs, it is appropriate, as proposed, to modify the wording to ensure the access ways to containment are “controlled” and “monitored” to ensure containment functionality during reactor power operations and in accident conditions. With this proposed change, reactor designers will be</p>

Requirement No.	Suggested Changes and New Design Safety Requirements for Consideration
	afforded the opportunity to employ containment access means and methods that are not limited to “doors and airlocks” and which are directly appropriate for the containment system associated with their particular design, all the while, remaining in compliance with the intent of the requirement.
68, Design for Withstanding the Loss of Off Site Power	<p><u>Proposed changes, suggestions or consideration to text:</u> Change the requirement to: “If a system important to safety at the nuclear power plant is dependent upon power, the design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. If required, the design shall include an alternate power source to supply the necessary power in design extension conditions.”</p> <p><u>Interpretation required:</u> Add a new paragraph of interpretation: 6.45B. The design of a power plant may incorporate safety features that are not dependent on electrical power. In this case, consideration should be given to requirements 6.44A and 6.44C for alternate power sources to further strengthen the adopted defence in depth against design extension conditions.</p> <p><u>Justification for proposed modification and/or interpretation:</u> The current requirement as written can be interpreted that an emergency power supply is required to maintain safety in the event of a loss of off-site power. SMR may be designed with passive or non-power dependent safety features and therefore are not reliant on power in order to maintain safety. Therefore, inclusion of extensive emergency power supplies could be unnecessary.</p> <p>In addition, alternate power sources may not be required to make the design of the SMR robust against Design Extension Conditions.</p>
73, Air Conditioning and Ventilation Systems	<p><u>Proposed changes, suggestions or consideration to text:</u> Change sub-item 6.49 to: “6.49. The design should minimize spread of contamination from areas of high contamination to areas of low contamination.”</p> <p>Add sub-item 6.49A: “6.49A: The design of any air conditioning, air heating, air cooling or ventilation should consider margin for dealing with foreseeable future extension in capacity of the plant.”</p> <p>Interpretation required: <i>None</i>.</p> <p><u>Justification for proposed modification and/or interpretation:</u> For 6.49: Even though the negative pressure differential (partial vacuum) has been utilized for the minimization of contamination spread for the existing nuclear plants, other mechanisms can be utilized to achieve the aim. The original requirement describes the negative pressure differential as only measure for the minimization of contamination spread, and as such requires generalization for SMR application. Especially for the SMR with passive safety system, alternative means can be employed for isolating areas of contamination from clean areas when an accident occurs.</p> <p>For 6.49A: Some SMR designs adopt extension of power capacity during plant lifetime through additional module installation. Changes in requirements or capability may result in the addition of new equipment which could increase the load on HVAC systems. Therefore, consideration should be given to including margin in the design capability of HVAC to allow for the potential addition of new equipment at a later date. This will reduce the impact on equipment important to safety.</p>
76, Overhead Lifting Equipment	<p><u>Proposed changes, suggestions or consideration to text:</u> Remove “overhead” from the title and the body of the requirement. Also, replace “crane” with “lifting equipment”.</p> <p>Interpretation required: <i>None</i>.</p> <p><u>Justification for proposed modification and/or interpretation:</u> Limiting the lifting equipment to overhead equipment only may have two undesirable effects: Some SMRs designs do not allow for the use of overhead lifting equipment because of a lack of overall volume to handle the items. Requirement 76 as it is currently written is not applicable for such designs.</p> <p>Due to the compactness of some SMRs designs, overhead lifting equipment may have a negative impact on safety by increasing the risk of dropping loads.</p> <p>The proposed change removes this limitation, allowing for more adapted lifting equipment when appropriate, such as jacks, fork lifts, etc.</p>



Requirement No.	Suggested Changes and New Design Safety Requirements for Consideration
	It should be noted that the new formulation will most likely have very little impact on the lifting equipment used in large scale plants: the items to be lifted are heavy enough to necessitate overhead lifting.
No. 78 Systems for Treatment and Control of Waste	<p><u>Proposed changes, suggestions or consideration to text:</u> Change sub-item 6.59 to include the following text: “6.59. Systems and facilities shall be provided for the management and storage of radioactive waste on the nuclear power plant site, or at a suitable dedicated site, for a period of time consistent with the availability of the relevant disposal option.”</p> <p>Interpretation required: <i>None</i>.</p> <p><u>Justification for proposed modification and/or interpretation:</u> Similarly to Requirement 12, this requirement as currently written can also be interpreted as applying only to a single nuclear power plant. SMRs by design could be built in larger numbers in a geographic area and therefore could enable a fleet solution to be derived for the effective and safe management of waste and the decommissioning process. This may enable consideration to be given to the construction of a single facility that is built solely for that purpose. Such a fleet facility would have greater throughput of waste and therefore would offer a greater opportunity for the application of advanced processing technology to reduce environmental impact.</p> <p>In addition, alternate power sources may not be required to make the design of the SMR robust against Design Extension Conditions.</p>
New Requirement 41A, Interactions between the Heat Delivery System and the Plant	<p><u>Proposed changes, suggestions or consideration to text:</u> The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the heat delivery system between the plant and a coupled process heat facility if present.</p> <p><u>Justification for addition:</u> SMRs provide greater opportunity for nuclear power plants to support industrial facilities that utilize heat or both heat and electricity. Analogous to Requirement 41, which addresses the potential impact of grid disturbances on reactor safety, this proposed requirement addresses potential disturbances from the process heat user. An example is that the shutdown of a coupled desalination plant would represent a loss of load to the reactor plant.</p>

## 6. CONSIDERATIONS FOR FUTURE WORK

In regard to future work, the participants recommended the following:

- A future revision of SSR-2/1 to incorporate considerations outlined in Section 5 of the report;
- Further review of the SSR-2/1 requirements to high temperature gas reactors through the implementation of additional meetings;
- A review of the U.S. NRC 10CFR50 Appendix A requirements for advanced non-light water reactors;
- Development of an IAEA technical report to document the outcomes of this project.

## ACKNOWLEDGEMENTS

FLAUW, Yann	France
FLOWER, Alison	United Kingdom
INGERSOLL, Daniel	United States of America
KANG, Han Ok	Republic of Korea
MOOR, Steve	United Kingdom
SONG, Danrong	People’s Republic of China
RICKMAN, Robin	United States of America

## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA-SSR-2/1, IAEA, Vienna (2016).

## **DESIGN SAFETY CONSIDERATIONS FOR WATER-COOLED SMALL MODULAR REACTORS - INCORPORATING LESSONS LEARNED FROM THE FUKUSHIMA DAIICHI ACCIDENT**

M. SUBKI  
International Atomic Energy Agency  
Vienna, Austria  
Email: m.subki@iaea.org

SUSYADI  
National Nuclear Energy Agency of Indonesia (BATAN)  
Jakarta, Indonesia  
Email: susyadi@batan.go.id

K.B. PARK  
Korea Atomic Energy Research Institute (KAERI)  
Seoul, Republic of Korea  
Email: kbpark2@kaeri.re.kr

M.E. RICOTTI  
Politecnico di Milano (POLIMI)  
Milano, Italy  
Email: marco.ricotti@polimi.it

C. ZELIANG  
University of Ontario Institute of Technology (UOIT)  
Oshawa, Canada  
Email: Chireuding.Zeliang@uoit.ca

### **Abstract**

The IAEA has a project to help coordinate Member State efforts in the development and deployment of small modular reactor (SMR) technology. This project aims simultaneously to facilitate SMR technology developers and potential SMR users, particularly States embarking on a nuclear power programme, in identifying key enabling technologies and enhancing capacity building by resolving issues relevant to deployment, including nuclear reactor safety. The accident at the Fukushima Daiichi nuclear power plant was caused by an unprecedented combination of natural events: a strong earthquake, beyond the design basis, followed by a series of tsunamis of heights exceeding the design basis tsunami. Consequently, all the operating nuclear power plants and advanced reactors under development, including SMRs, have been incorporating lessons learned from the accident to assure and enhance the performance of the engineered safety features in coping with such external events. This paper presents technology developers and users with common considerations, approaches and measures for enhancing the defence in depth and operability of water cooled SMR design concepts to cope with extreme natural hazards. Indicative requirements to prevent such an accident from recurring are also provided. At first, a review of engineered safety feature design of SMRs is provided, covering the trip and shutdown system, residual heat removal system, safety injection system, containment system and severe accident mitigation features. Afterwards, countermeasures to address the lessons learned from the Fukushima Daiichi accident will be discussed from the viewpoints of design and siting, on-site and off-site emergency preparedness and responses, and nuclear safety infrastructures. It is concluded that water cooled SMR designs have variations in safety system designs that may come from the reactor attributes such as design and safety characteristics, power level, and type of safety system (active, passive or hybrid of active and passive) to cope with accidents. They also have the potential to duly adapt to and cope with a variety of extreme natural hazards (e.g. simultaneous and multiple external hazards). The study suggests that the IAEA should develop relevant safety standards to incorporate SMR specific design features and special condition, as the current safety standards are applicable primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation. The paper reports Member States accomplishment in discussion design safety considerations for water-cooled SMRs incorporating lessons learned from the Fukushima Daiichi accident published in 2016 as IAEA-TECDOC-1785.

## 1. INTRODUCTION

Substantial works of developments of small and medium-sized or modular Reactors (SMRs) technology are on-going in several countries. Their motives include: fulfilling the need for flexible power generation for a wider range of users and applications; replacing the ageing fossil fuel-fired power plants; enhancing safety performance through inherent and passive safety features; offering better economic affordability; suitability for non-electric applications; options for remote areas; and synergetic energy systems that combine nuclear and renewable energy sources [1]. Some SMRs are designed to be deployed as multi-module power plants, where modularity is achieved by integrating major components of the reactor coolant system inside the reactor pressure vessel – in the same compartment with the reactor core and internals. Moreover, transportable nuclear power plant (TNPP), including floating and marine-based SMRs, are also being developed.

The Fukushima Daiichi accident informed many valuable lessons on both technical and economic impacts in utilizing nuclear energy. The accident has disclosed various existing design weaknesses and vulnerabilities, especially when combination of unprecedented natural phenomena occurs. Realizing that other unprecedented site/region-specific events could disrupt reactor operation in the same scale or more than what happened in the Fukushima Daiichi accident, not necessarily a large tsunami, nuclear community needs to take lessons from the accident and transform them into appropriate design enhancements, actions, and other countermeasures in water cooled reactors, both those in operations and near term deployable designs.

This paper presents and discusses design safety considerations on appropriate and practical countermeasures to incorporate and address the lessons learned from the Fukushima Daiichi accident to enhance the design of engineered safety systems of water cooled SMRs currently under development.

## 2. OVERVIEW OF THE FUKUSHIMA DAIICHI ACCIDENT

The Fukushima Daiichi accident on March 11, 2011 demonstrated that extreme natural hazards have the potential to invalidate or impair multiple levels of defence in depth (DiD). The earthquake and the tsunami impacted on multiple units at the Fukushima Daiichi NPP and caused widespread destruction of buildings, doors, tanks, water intakes, roads and other site infrastructures which lead to the loss of emergency core cooling capability and eventually loss of the ultimate heat sink from the sea. By design, the Fukushima Daiichi nuclear power plant provided equipment and systems for the first three levels of DiD: (1) equipment intended to provide reliable normal operation; (2) equipment intended to return the plant to a safe state after an abnormal event; and (3) safety systems intended to manage accident conditions. The design bases were derived using a range of postulated hazards; however, external hazards such as tsunamis were not fully addressed. Consequently, the flooding resulting from the tsunami simultaneously challenged the first three protective levels of DiD, resulting in common cause failures of equipment and systems at each of the three levels [2].

## 3. REVIEW OF ENGINEERED SAFETY FEATURE DESIGN OF SMALL MODULAR REACTORS AND ADVANCED REACTORS

Engineered safety feature (ESF) of nuclear power plant is a set of means to protect the public from radioactive fission products in the event of accidents. Its primary functions are to localize, control, mitigate and terminate the consequences of postulated accidents and maintain radiation exposure levels below allowable limits. Various designs and concepts of ESFs are used in different reactors and there are similarities among them. In advanced SMRs the technologies of ESF can be characterized as follows:

- Improved trip and safety shutdown systems. A new design is introduced recently for integral PWR type SMRs where the CRDM is placed inside the vessel to eliminate penetration and the consequences of their failure. This technique inherently removes possibility of rod ejection accident and the consequent LOCA as penetrations in the reactor vessel closure head are eliminated.
- Passive residual heat removal system. Some SMR designs passively remove decay heat through pairing the steam generators (SGs) with heat exchangers immersed in a water pool. Steam produced by decay heat in the SG is routed to the heat exchangers where it is condensed. The condensate flows back to the SG through SG feed water inlet.

- Passive safety injection system. Several methods are implemented in advance SMRs including Safety injection using pressurized tank, Safety injection using recirculation valves (in NuScale), and Gravity driven safety injection system
- Improved containment system. Containment system has three main functions: (a) Confinement of radioactive substances in operational states and in accident conditions, (b) Protection of the plant against extreme natural hazards and human induced events, (c) Radiation shielding in operational states and in accident. Several approaches are used in SMR designs, among others are pressure suppression containment system, concrete containment with spray system and submerged metal containment;
- Enhanced severe accident mitigation features. Several strategies are implemented to deal with severe accidents. The approaches are in-vessel retention system, filtered containment venting system and the use of passive auto-catalytic hydrogen re-combiners as hydrogen control devices. Some reactor designs combine the hydrogen control device with pre-inerting of containment atmosphere with nitrogen to remove oxygen.

#### 4. DEFENCE IN DEPTH IN SMALL MODULAR REACTORS

According to the IAEA publication ‘Defence in Depth in Nuclear Safety, INSAG-10, a report by the International Nuclear Safety Advisory Group’ [3], the DiD concept is structured in five (5) levels in which should one level fail, the subsequent level comes to play to deal with the reactor conditions and protects the overall system. The five levels of defence are: (1) Prevention of abnormal operation and system failures, (2) Control of abnormal operation and detection of failures; (3) Control of accident within the design basis; (4) Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents; (5) Mitigation of radiological consequences to protect people and environment against significant releases of radioactive materials. Each level of DiD should be independent of the others and failure in one level should not impair the functionality of other levels.

#### 5. COUNTERMEASURES TO ADDRESS THE LESSONS LEARNED FROM THE FUKUSHIMA DAIICHI ACCIDENT IN THE DESIGN OF WATER COOLED SMALL MODULAR REACTORS

The basis for the development of this paper is international experts’ discussion result on the lessons learned from the Fukushima Daiichi accident which was produced through a series of Consultancy Meetings in the IAEA headquarter [1]. The lessons were compiled and integrated from those have been previously identified, collected and published by the fact finding teams of several organizations/institutes including reactor designers. Experts from various organizations collected and identified as many as 94 individual lessons and recommendations on Fukushima Daiichi Accident, which are grouped into integrated lessons learned. The experts then provided technical considerations and countermeasure options on how to enhance the performance of ESFs of water cooled SMRs.

##### 5.1. Design and Siting

###### 5.1.1. *Strengthen measures against extreme natural hazards and consequential effects*

The combination of two or more natural hazards can result in unprecedented impacts to the reactor facility. The Fukushima Daiichi accident which underwent large earthquake and subsequent tsunami revealed several lessons for the design of future reactors. The following are some of the SMR design guidelines based on the lessons learned:

- Earthquake exceeding the design basis did not cause any known significant damage.
- Earthquake exceeding the design basis causing loss of off-site power source became the initiating event for accident scenario.
- Optimizing for earthquake made some equipment vulnerable to tsunami (e.g., locating EDGs underground).
- Extensive tsunami and subsequent hydrogen explosion damage and debris created significant logistical difficulties and inhibited response actions.

— Repeated aftershocks and tsunami threats stopped recovery work on occasions.

The following Table 1 summarises the strengthening measures against natural hazards and consequential effects.

TABLE 1. STRENGTHENING MEASURES AGAINST EXTREME NATURAL HAZARDS AND CONSEQUENTIAL EFFECTS [1]

Defence in Depth level	Critical issues addressed	Option for countermeasures	Considerations for water cooled SMR	Relevant safety requirements
Prevention (1)	Natural hazards	Ensure that all types of natural hazards are considered in the design.	Natural hazards include earthquake, tsunami, external flood, high winds (typhoon, cyclone, hurricane and tornado), forest fire, snow, ice storm, extreme cold weather, dam break, volcano, and sand storm. • The set and magnitude of natural phenomena should be specific to the site. The criteria should include return cycle of the worst event which can be common to all SMR sites in that area.	IAEA Safety Standards Series Specific Safety Requirements No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design Requirement 17 and relevant Paragraphs.[4]
Prevention (1)	Magnitude of hazards	Ensure that trends and uncertainties are considered in determining the magnitude of natural phenomena which should be mitigated.	The type and cause of natural hazards is site specific but it is better to consider large margin (highest in the region) depending on the site characteristics of the plant.	
Control of accidents within DB (3)	Safety assessment	Include all extreme natural hazards in safety assessment.	• Perform periodic reassessments especially if extreme natural hazards occur in the plant site.	
Control of accidents within DB (3)	Safety systems	Ensure that cliff edge effects are considered and addressed.	Cliff edge effects, where an incremental increase in magnitude causes a disproportionate increase in consequences	

### 5.1.2. Consider issues concerning multiple unit sites

The Fukushima Daiichi accident indicated that multiple reactor units in one site face the followings:

- Unexpected problems
- Unexpected aftershock challenges
- The need to respond to all units concurrently strained all resources on-site.

As the above findings reveal, it is recognized that the issues concerning multiple reactor sites and multiple sites must be addressed. The current design of SMRs typically offers multiple reactor modules in one plant which ranges from two (2) to twelve (12) modules. So it is important to consider the issues of countermeasures shown in the Table 2.

TABLE 2. ISSUES CONCERNING MULTIPLE UNIT SITES [1]

Defence in Depth level	Critical issues addressed	Option for countermeasures	Considerations for water cooled SMR	Relevant safety requirements
Prevention 1	Common cause failure	Ensure that the common cause failure and related accident management concerns are considered in the design.	Multiple unit threat is particularly applicable to modular reactors. Some SMRs are proposed in multiple units. Regulatory body should require safety assessment for all units on the site as a whole. • Provide cross connection between units with the reliable isolation capability.	Requirement 33 and relevant Paragraphs [4]
Control of accidents within DB (3)	Safety systems	Ensure that countermeasures can be carried out for a unit where meltdown occurs and accident dose rate increases beyond analysis limits.	Enhance the containment hydrogen control, using cooling, venting and filtering. • Provide shielding, convenient access and remote operations of countermeasures.	

### 5.1.3. Enhance off-site and on-site electricity supplies

Reliance on active systems for safety functions has been greatly reduced in SMRs designs. Passive cooling systems with a long grace period for DBAs provide improvement over existing reactor designs. However, attention should be paid to the supply of power, especially for severe accident management where the lighting and monitoring systems are needed to cope with the situation. In order to deal with the above facts, some options of countermeasures to enhance off-site and on-site power are described in Table 3.

TABLE 3. ENHANCED OFF-SITE AND ON-SITE ELECTRICITY SUPPLIES [1]

Defence in Depth level	Critical issues addressed	Option for countermeasures	Considerations for water cooled SMR	Relevant safety requirements
Prevention (1)	Equipment readiness	Prepare equipment required to respond to a long term loss of all AC and DC power	The equipment should be conveniently staged, protected, and maintained such that it is always ready for use if needed	Requirement 68 and relevant Paragraphs [4].
Prevention (1)	Protection of EDGs (to be used for safety functions)	Protect EDGs from all extreme natural hazards.	EDGs and associated emergency power supplies should be located at higher elevations considering flooding or their location should be enclosed by water tight and seismically qualified enclosures (e.g., water proof doors and penetrations).	
Prevention (1)	Emergency power supplies	Ensure electricity supplies for safety systems	Use separate redundant DC systems for various safety functions, e.g., for reactor safety monitoring instruments, power system actuation, valves and motors motive power, etc., with complete electrical and physical separation.	

#### 5.1.4. Ensure robust measures for reactor core cooling and ultimate heat sinks

During the Fukushima accident, the EDGs were crippled by tsunami and the successive cooling systems degraded and failed. In Unit 1 the indicators in the control room for IC failed. In Units 2 and 3, the steam-driven systems, namely, RCIC and HPCI kept working for a few days. A loss of core cooling systems and failure to provide core cooling by other means lead to severe core damage. Based on these lessons, the following Table 4 recommends options for the countermeasures.

TABLE 4. ENSURE ROBUST MEASURES FOR REACTOR CORE COOLING AND ULTIMATE HEAT SINK [1]

Defence in Depth level	Critical issues addressed	Option for countermeasures	Considerations for water cooled SMR	Relevant safety requirements
Control of Accident within DB (3)	Safety systems	Confirm the reliability and capability of cooling systems to cool the core after natural hazards occurrences.	Provide at least two success path to cope with the accident using any combination of passive, active, and manually aligned systems. • Provide diversity of heat sink through use of portable heat removal systems	Requirements 47, 51, 52, 53 and relevant Paragraphs [4].
Control of Accidents within DB (3)	SBO	Confirm that SBO can be managed for long time.	Provide passive cooling systems which are able to function for extended or indefinite period. • Consider portable systems for added margin for long term core cooling.	
Control of accidents within DB (3)	Safety systems	Maximize survivability of reactor cooling capabilities [6].	The status of all modes of core cooling should be available in control room under all plant conditions	

#### 5.1.5. Enhance design of safety-related structures, systems and components

Reactor design should guarantee that all safety related structures, system and components (SSCs) survive in all accident conditions. They must be accessible through remote control, and if it fails, through manual operation. In the Fukushima Daiichi accident, several safety related SSCs lost functions due to the failure of remote control after loss of all power. In SMRs such failures of safety related structures, systems and components should be prevented or accommodated with compensatory measures. The following Table 5 explains some considerations.

TABLE 5. ENHANCING DESIGN OF SAFETY-RELATED STRUCTURES, SYSTEMS AND COMPONENTS [1]

Defence in Depth level	Critical issues addressed	Option for countermeasures	Considerations for water cooled SMR	Relevant safety requirements
Prevention (1)	SSC design	Protect SSCs from extreme natural hazards.	Provide design solutions to protecting SSCs from all hazards (e.g., flooding, Volcanic ash, desert sand).	Requirements 45, 46, 48, 49, 55, 58 and relevant Paragraphs [4].
Prevention (1)	SSC design	Prevent primary containment vessel (PCV) damage caused by elevated temperature.	Enhance the PCV cooling system (e.g., by passive system, followed by pump supplied spray system for extended service). • Provide diverse cooling systems for containment and provision for connecting portable cooling equipment.	
Prevention (1), Control of accidents within DB (3)	SSC design	Exploit positive features of SMR in the design of safety related SSCs	• Plant designs should consider installation of air-cooled EDGs and cross-connections between units to allow sharing of AC and DC power, fresh- and seawater, and compressed air systems during emergencies.	

#### 5.1.6. Ensure measures for prevention and mitigation of hydrogen explosions

The explosion damaged the reactor buildings of Units 1, 3 and 4. It was suspected that hydrogen leakages occurred from the primary containment to reactor building through several passages such as top head manhole, top head flange, piping penetration, airlock for personnel, suppression chamber manhole, electric wiring penetration, equipment hatch, vent tubes, etc. Extensive damage and debris from the explosion created significant logistical difficulties and inhibited response actions. The design needs to put more attention on these matters and must ensure measures for prevention and mitigation of hydrogen explosions

#### 5.1.7. Enhance containment venting and filtering system

The BWR venting system is part of containment system which plays an important role to control the pressure of dry well and wet well during abnormal conditions. As venting is an important aspect in coping with the Fukushima Daiichi type accident, the following considerations given in Table 6 are presented to deal with this type of accident.

TABLE 6. CONSIDERATIONS TO ENHANCE THE CONTAINMENT VENTING AND FILTERING SYSTEM [1]

Defence in Depth level	Critical issues addressed	Option for countermeasures	Considerations for water cooled SMR	Relevant safety requirements
Mitigation of severe accidents (4)	Vent design	Ensure that the vent design is hardened and capable to allow safe depressurization	The vent system should be constructed to accommodate a permissible flow of steam/air mixture. The system should be able to reduce pressure inside the reactor before core uncover	Requirement 73 and relevant Paragraphs [4]



Defence in Depth level	Critical issues addressed	Option for countermeasures	Considerations for water cooled SMR	Relevant safety requirements
			<ul style="list-style-type: none"> <li>Plant designs should support timely venting of primary containment even with a loss of power and motive force, such as compressed air.</li> </ul>	
Mitigation of severe accidents (4)	Radioactive Release control	Avoid radioactive release during venting.	Retrofit the vent system with radioactivity filters to reduce the pressure and hydrogen level without releasing large amounts of fission products	

## 6. CONCLUDING REMARKS<sup>1</sup>

Many water cooled SMR designs and technologies are under development offering simplified design and flexible deployment options. The issues and lessons learned from the Fukushima Daiichi event are being incorporated into SMR design development. Water cooled SMR designs for near term deployment have variations in ESF designs that may come from the reactor attributes such as design and safety characteristics, power level, and type of safety system (active, passive or hybrid) to cope with accidents. They also have the potentialities to duly adapt to and cope with a variety of extreme natural hazards (e.g. Fukushima-like or simultaneous and multiple external hazards). This paper presents and discusses design safety considerations on appropriate and practical countermeasures to incorporate and address the lessons learned from the Fukushima Daiichi accident to enhance the design of engineered safety systems of water cooled SMRs currently under development. New nuclear power plants, including SMRs, are to be designed, sited and constructed consistent with the objective of preventing accidents in the commissioning and operation. Should an accident occur, the plants shall be able to prevent and mitigate possible releases of radionuclides that may cause long term off site contamination. There is a need of IAEA role in SMR design safety review to provide advice regarding the design's ability to meet the IAEA Fundamental Safety Principles. It is also suggested that the IAEA should develop relevant safety standards to incorporate SMR specific design features and special condition, as the current safety standards are applicable primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation.

## ACKNOWLEDGEMENTS

ALAMGIR, Md.	United States of America
ARITOMI, Masanori	Japan
ATIQUÉ, Muhammad	Pakistan
BYLOV, Igor	Russian Federation
GIMENEZ, Marcelo Oscar	Argentina
JILANI, Ghulam	Pakistan
KIM, Manwong	Republic of Korea
MARQUINO, Wayne	United States of America
NAYAK, Arun Kumar	India
YAMADA, Katsurmi	International Atomic Energy Agency

<sup>1</sup> The opinions expressed in this paper — and any recommendations made — are those of the participants and do not necessarily represent the views of the IAEA, its Member States or the other cooperating organizations.

## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Safety Considerations for Water Cooled Small Modular Reactors Incorporating Lessons Learned from the Fukushima Daiichi Accident. IAEA-TECDOC No. 1785, IAEA, Vienna (2016).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, The Fukushima Daiichi Accident, Report by the IAEA Director General. IAEA, Vienna (2015).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, INSAG -10 . Defense in Depth in Nuclear Safety. A report by the International Nuclear Safety Group. International Atomic Energy Agency, IAEA, Vienna (1996).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design Specific Safety Requirements. IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).



CONTRIBUTIONS TO HARMONIZATION OF APPROACHES AND  
METHODS BY INTERNATIONAL FORUMS

**Chairperson**

**S. CHEN**  
China



## THE EUROPEAN UTILITY REQUIREMENTS FOR ADVANCED LIGHT WATER REACTORS (EUR): RECENT ACHIEVEMENTS AND NEW CHALLENGES

G. JACQUARD  
EDF  
Villeurbanne, France

E. VIEILLETOILE  
EDF  
Villeurbanne, France  
Email: emmanuel.vieilletoile@edf.fr

### Abstract

Since 1991, the European Utility Requirements (EUR) organisation has been actively developing and promoting harmonised technical specifications for the new mid- and large-size LWR designs to be proposed by the Vendors in Europe. The EUR Document consists of a comprehensive set of requirements covering the whole Nuclear Power Plant (NPP). It encompasses all aspects (safety, performance, competitiveness) and all parts of a NPP (nuclear island and conventional island). The Document can be used by the Utilities (guide for design assessment, technical reference for call for bids) and by the Vendors, as a technical guide. The harmonisation which is sought by the EUR aims at delivering the safest and most competitive designs based on common rules shared all over Europe. Fourteen nuclear operators across Europe are members of the Organisation.

After the publication of the Revision D of the EUR Document (October 2012), the EUR organisation has been extremely active. The main results obtained during the last four years and the new challenges for the coming years (roadmap 2016-2018) are presented in the three following fields.

First, the revision of the EUR Document, in order to maintain it at a state-of-the-art level, remains the highest priority for the Organisation. Regarding the new revision E of the EUR Document [1], issued early 2017, significant updates are implemented in many fields among which: revised safety requirements taking into account the most recent European and international safety standards issued by WENRA and IAEA, the lessons learnt from the Fukushima accident, including re-evaluated Seismic and External Natural Hazards approach and the most recent international standards, for example for Instrumentation & Control.

The assessment of new designs is the second main technical activity of the EUR organisation. The MHI EU-APWR design has been assessed against the revision D between 2012 and 2014. New design assessments are in progress (namely Korean KHNP's EU-APR and Russian AEP's VVER TOI) and are planned to be completed in 2017. A new applicant is in the file.

The third challenge is the interaction between the EUR and the other stakeholders, in particular the other international organisations (ENISS, WNA/CORDEL, WENRA, IAEA, EPRI/URD).

### 1. INTRODUCTION

The development, the design and the licensing of the existing Generation II Light Water Reactor (LWR) plants in Europe had been performed on a national basis with little interaction between countries. To overcome this weakness, in 1991 a group of five major European electricity producers formed an organisation to develop the European Utility Requirements (EUR) Document. The EUR organization nowadays gathers fourteen Utilities (see Figure 1) which represent major European electricity producers operating a nuclear fleet of more than a hundred LWRs. Some of them have already started, are building or planning to build new reactors.

The early drafts of the EUR Document were produced in 1992, in coordination with the development of the Utility Requirements Document (URD) in the US, which was undertaken by the Electric Power Research Institute (EPRI). Indeed, at that time, the EUR utilities were also contributing to the US Advanced Light Water Reactor (ALWR) program, and more specifically to the development of the URD.

The focus of the EUR organisation is the development of common specifications for new Gen III designs to be proposed by Vendors in Europe and their promotion at the international level. The European Utilities involved in the EUR organisation aim at harmonising and stabilising the conditions in which the LWR NPPs to be built in Europe will be designed, built, commissioned, operated and maintained.

EUR Member	Country
CEZ	CZECH REPUBLIC
EDF	FRANCE
EDF Energy	UK
ENERGOATOM	UKRAINE
FORTUM	FINLAND
ENGIE/TRACTEBEL	BELGIUM
GENENERGIJA	SLOVENIA
HORIZON	UK
IBERDROLA	SPAIN
MVM PAKS II	HUNGARY
NRG	NETHERLANDS
ROSENERGOATOM	RUSSIA
TVO	FINLAND
VGB PowerTech	GERMANY

FIG. 1. Members of the EUR organisation as of January 2017.

The harmonisation of the requirements is sought in the following fields:

- safety approaches, targets and assessment methods,
- design conditions, design objectives and criteria for the main systems and equipments,
- equipment specifications and standards,
- information required for the assessment of safety, reliability and cost, and some of the corresponding criteria,

allowing the development of standard designs that can be built and licensed in several European countries with only minor variations.

As a general objective, the EUR organization promotes the development of NPPs providing robust behavior and sufficient autonomy with respect to operator actions, as well as for water and power supplies. The EUR Document requires the NPP to be designed so as to have a low environmental impact on its surrounding environment and on the population by minimizing radioactive and chemical releases in all normal and accident conditions.

The EUR Document is endorsed by the major European electricity producers and is considered as the reference technical document for developing new NPPs and for the bidding of new Generation III projects. It has already been used as a technical basis for bidding purposes in several countries in Europe but also outside Europe.

## 2. THE EUR DOCUMENT

The EUR Document [1] provides a comprehensive set of requirements for Generation III NPPs written by the Utilities themselves, i.e. potential investors in the new designs proposed by the Vendors. The requirements are based on the international design and operation experience which has been accumulated for more than four decades.

The EUR Document covers the entire plant up to the grid interface. It is therefore the basis for an integrated plant design (i.e. Nuclear Island and Power Generation Plant). The EUR Document emphasizes those areas which are most important for the optimisation of the design with respect to safety, performance, constructability and economics.

The Document applies to both Pressurised Water Reactors (PWRs) and Boiling Water Reactors (BWRs). Only LWR plants are dealt with. Other types of plants are not considered to have shown sufficient operating experience to be built, licensed and operated in Europe in the short term, and only a very few projects of non-LWR plants are scheduled in the future in Europe.

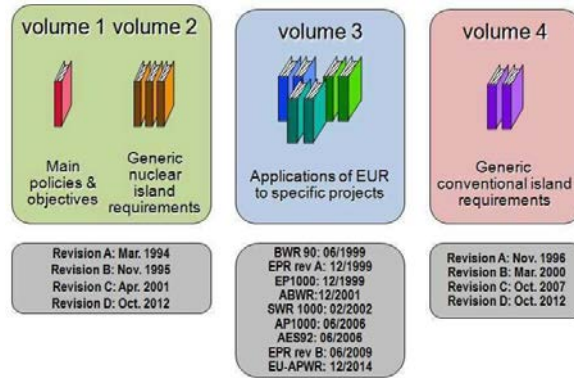


FIG. 2. The EUR Document.

The EUR Document [1] is structured into four volumes (see Fig. 2):

- Volume 1 “Main policies and objectives” including three chapters: chapter 1.1 “Introduction to EUR” presenting the organisation’s objectives, chapter 1.2 “EUR policies” presenting the key policies driving the EUR requirements and chapter 1.3 “EUR synopsis” providing an overview view of the Document itself.
- Volume 2 “Generic and Nuclear Island requirements” contains all the generic requirements and preferences of the EUR utilities for the Nuclear Island, and common requirements for Nuclear Island and Power Generation Plant. This volume contains more than 4000 requirements. The EUR policy is to have a core of strong generic requirements expressed as objectives or functions as far as possible. Several of these requirements are kept open, i.e. they provide only a design methodology and objectives that can be implemented in several ways by the plant designer. The structure of the current Volume 2 is described on Figure 3.
- Volume 3 “Application of EUR to specific designs” consists of a number of subsets, each one being dedicated to a specific design that is of interest to the participating utilities and that has been assessed by the organisation against the EUR requirements. Each subset contains a description of a standard Nuclear Island, a summary of the analysis of compliance vs. the EUR Volumes 1 and 2 and, where needed, design dependent requirements and preferences of the EUR Utilities. The list of designs that have been assessed as of the publication of this paper is shown on Figure 2.
- Volume 4 “Specific Power Generation Plant requirements” contains the generic requirements (more than 1000) related to the Power Generation Plant.

EUR Volume 2: Generic and Nuclear Island Requirements	
Chapter 2.1	Safety requirements
Chapter 2.2	Performance requirements
Chapter 2.3	Grid requirements
Chapter 2.4	Design Basis
Chapter 2.5	Codes and standards
Chapter 2.6	Material – related requirements
Chapter 2.7	Functional requirements: components
Chapter 2.8	Functional requirements: systems & processes
Chapter 2.9	Containment system
Chapter 2.10	Instrumentation & Control and Human – machine interface
Chapter 2.11	Layout
Chapter 2.12	Design process and documentation
Chapter 2.13	Constructability & commissioning
Chapter 2.14	Operation, maintenance and procedures
Chapter 2.15	Quality assurance
Chapter 2.16	Decommissioning
Chapter 2.17	PSA methodology
Chapter 2.18	Performance assessment methodology
Chapter 2.19	Cost assessment information requirements
Chapter 2.20	Environmental impact

FIG. 3. Structure of Volume 2 of the EUR Document.



The EUR Document has been regularly updated in order to accommodate the evolution of the regulatory and industry background as well as to take into consideration the feedback of experience from design, licensing, construction and operation. The Document has been published in successive revisions (see Figure 2).

The Revision D of the EUR Document has been recently used as a basis for bidding processes for newbuild projects in Europe, for example in Hungary.

### 3. CONTENT OF EUR REVISION E

One of the primary objectives assigned to the EUR organization in the 2013-2015 roadmap issued in March 2013 was to launch a new major revision of the EUR Document. In order to define the technical scope of this project, the Utilities prepared during the second half of 2013 a set of position papers on 15 technical fields for which they identified a need to revise the EUR Document. These high-level position papers were used as a support for the EUR Steering Committee to discuss the proposed orientations for changes. Based on this preliminary work, the Steering Committee decided during the first Quarter of 2014 the final technical scope for the Revision E Project which was officially launched in April 2014.

For each of the main technical fields retained for the Revision E Project, Topical Working Groups (TWGs) were launched with experts coming from the different EUR utilities. The main technical updates for the EUR Revision E Project are summarised below for each field:

- Safety requirements: the major objective of Revision E Document here was to revise in depth the Rev. D Chapter 2.1 “Safety Requirements” by working at the same time on the structure and on the technical contents of the chapter.
  - The revision of the structure of the chapter results in a document which is more easily usable for bidding and licensing purposes. The new chapter systematically proposes functional requirements which are organized in a structure similar as other international standards (in particular IAEA SSR-2/1).
  - Regarding the technical changes, the major ambition was to derive EUR requirements which are in line with the newest international safety standards, in particular the recent versions of IAEA and WENRA documents [3-6]. The new EUR Chapter 2.1 gives guidance on how the IAEA and WENRA high-level requirements can be interpreted and applied in the European context. Indeed, the first technical task of the Safety TWG was to write down more detailed technical position papers on the main Safety Objectives proposed by WENRA [5].
  - Regarding the Safety Classification, a dedicated TWG was also set up in 2014 and has been working on the revision of the safety classification requirements in the EUR Document. The work was mainly based on two kinds of inputs: the most recent international references, in particular the IAEA and IEC standards [7-8] and the recent licensing experience gained from the new build projects in Europe.
  - All available lessons learned from the Fukushima accident were examined by the Utilities and integrated when valuable in the Revision E EUR Document Chapter 2.1 (safety requirements) and other connected chapters. The aforementioned IAEA and WENRA sources already provided significant technical inputs for this work.
  - Radiological releases: in addition to the Criteria for Limited Impact (CLI) set in the EUR Rev. D (Appendix B of Chapter 2.1), new EUR Safety Objectives have been introduced in light of the O2 and O3 WENRA Safety Objectives. Furthermore, the assumptions and rationale for the proposed EUR criteria (doses and/or distances) have been updated and clarified.
- Instrumentation and Control (I&C): the Rev. E Document provides a major update of chapter 2.10 (I&C) which had not been revised in detail for years. The new safety standards already mentioned take into account more specific I&C standards [7, 8] which have been recently or will soon be issued by international organisations (e.g. [9]). The updated chapter endorses these key high level documents and specifies Utility requirements regarding the availability, maintenance and more generally all aspects not related to safety but which are of primary importance to the Utility. It emphasizes the importance of

keeping the architecture simple. Lessons learned from the recent licensing processes in Europe have been taken into account.

The other main technical fields for which Topical Working Groups have been set up, and have delivered significant updates for the Revision E, are mostly:

- Seismic Approach,
- Probabilistic Safety Assessment,
- Layout,
- Grid connection,
- Pipe Break preclusion.

In addition to the technical changes listed above, the overall structure of volumes 2 and 4 has been significantly improved, in order to ease the legibility and also to merge requirements which are common to the nuclear island and the conventional island. Requirements which are specific to the Conventional Island are kept in Volume 4, whereas common requirements are grouped in Volume 2. Relevant labels are added into Volume 2 requirements so as to identify nuclear island specific requirements.

#### 4. OTHER RECENT ACHIEVEMENTS

##### 4.1. The 2016-2018 EUR Roadmap

After roadmap 2013-2015, the EUR Steering Committee decided to setup a new roadmap for the next three years. This new roadmap was worked out within a few months and has been issued after approval by all the EUR members in June 2016.

This document summarises the vision of the EUR members and their main priorities for the future. The roadmap includes an ambitious action plan for the period 2016-2018 for which the EUR members committed to work actively by providing sufficient in-kind resources.

Four major objectives are defined:

- Enhance impact of EUR organisation, by developing its influence on Vendors and Regulators through, and in collaboration with, European nuclear industry forums (ENISS, FORATOM, CORDEL...);
- Issue EUR Document Rev. E, so that it remains a major reference technical document for developing new NPPs and harmonising new projects in Europe;
- Continue with best endeavours to respond to new reactor design assessment requests from Vendors, who are interested in getting a sound review of their design versus an internationally recognized reference;
- Propose position papers for a potential future revision by analyzing feedback from revision E and assessments, and
- identifying innovations which could improve reactor competitiveness in the future.

##### 4.2. Performance of new design assessments

From October 2012 to October 2014, the EUR Organisation performed the assessment of the Japanese Mitsubishi Heavy Industries (MHI) EU-APWR design. This was the first time that a design was assessed against the Revision D of the EUR Document.

The EU-APWR is an Advanced PWR, 1700 MWe class, 4-loops, 14ft active core fuel length that MHI has developed for the European market. The EU-APWR is an evolution of the Advanced PWR currently under the licensing process in Japan. MHI modified the design applying safety and economical improvements in order to comply with the EUR requirements: 4 active safety trains, some passive features, a single containment with liner and a core catcher.

The overall results of the assessment process indicate the good compliance of the EU-APWR Standard Design with EUR requirements.

In October 2014, the EUR Steering Committee approved the final technical report for this assessment and Subset H of the EUR Volume 3 was issued in January 2015 [10].

More details on the assessment methodology and the technical results can be found in [11-12].

Taking advantage of this design assessment exercise, the EUR organisation also worked in 2013 on the optimisation of the EUR assessment process itself. This work aimed at improving the efficiency of the next design

assessments and in particular to minimise their duration. The preliminary work which has to be performed by the vendor before launching the assessment by the EUR utilities has been clarified. The different steps of the preparation phase and of the assessment phase itself have been explicitly described in a EUR document titled “Generic Assessment Principles” [13]. This document can be circulated and commented to the Vendors right from the very preliminary steps of the assessment. In addition, a “Standard Project Manual” has been developed in order to provide both the team of Utilities and the Vendor with a detailed basis for deriving their specific Project Manual.

Two design assessments are ongoing now against EUR Rev D Document:

- EU-APR, designed by South Korean KHNP. This is the European version of APR1400, with enhanced level of safety. 8 units of APR1400 are under construction in South Korea and in United Arab Emirates. EU-APR is a 1,400 MW PWR, 2 loops with 4 active safety trains, some passive features, a double containment with liner and a core catcher. Eight EUR Utilities are participating to the assessment project, which began in September 2015, and is scheduled to be completed by mid-2017.
- VVER TOI, designed by AEP (Atom Energo Proekt Moscow). This is a new design of GEN III VVER, and a simplified evolution of AES-92 and AES-2006. Several AES-92 and AES-2006 have been commissioned or are under construction in Russia, India and Belarus. VVER TOI is scheduled to be constructed soon in Russia. VVER TOI is a 1,250MW PWR, 4 loops with 2 active trains and a full set of passive features, a double containment with liner and a core catcher. Five EUR Utilities are participating to the assessment project, which began in November 2015, and is scheduled to be completed by end 2017.

#### 4.3. Communication and interaction with stakeholders

Being an internationally recognised organisation, the EUR includes in its roadmap for the period 2016-2018 an active communication plan in order to maintain a strong influence in the field of New Nuclear Projects.

- One of them ain objectives of the communication plan is the promotion of the EUR Documents other remains an international reference used by both designers and utilities for their new build projects.
- For training and dissemination purposes, the EUR organisation proposed a three-day technical course on the Revision D for its members. This training session was hosted by MVM in Paks, Hungary, in March 2014. New training sessions will be organised in the future for Revision E and some of them could be open to non EUR members.
- The external communication was also improved with a reinforced presence in international nuclear engineering conferences. The website of the EUR organization [14] provides the EUR members, the external stakeholders and the public with clear and easy accessible information on the EUR.
- Keeping a very active interaction with other international stakeholders is also one of the main priorities of the 2016-2018 roadmap.

The EUR organisation coordinates with the European Nuclear Installations Safety Standards initiative (ENISS [15]) which was launched in 2005 within FORATOM in order to strengthen the interaction between the European nuclear industry and the WENRA association.

The EUR also interacts with the working group on the Cooperation in Reactor Design Evaluation and Licensing (CORDEL) which was created in 2007 under the auspices of the World Nuclear Association (WNA). This group shares the same objectives as the EUR organisation in terms of harmonisation and standardisation of the designs and licensing processes [16].

The strong need for interaction between the EUR, ENISS and CORDEL was reaffirmed through a joint statement signed in September 2012 by the three chairmen of the organisations. EUR, ENISS and CORDEL committed to inform themselves mutually of their activities. ENISS has clearly the lead for the interaction with the WENRA organisation. ENISS provides WENRA with the comments coming from the Utilities, which usually have been prepared jointly with the EUR organisation (at least for the topics related to new NPP designs). Both ENISS and CORDEL have a seat as observers at the Nuclear Safety Standards Committee (NUSSC) of the IAEA and therefore can promote the views of the nuclear industry in this important organisation.

The EUR and the EPRI/URD also regularly communicate with each other. As stated above, the very early drafts of the EUR Documents were worked out in close connection with EPRI/URD. Since then, several comparison exercises were performed by the EUR organisation at the different stages of development of the EUR

Document. The most recent detailed comparison was performed in 2010 by the EUR organisation. At that time, the URD Revision 10 and the EUR Revision C were compared. The output of this comparison work was one of the important technical inputs for the preparation of the Revision D project. More recently, when preparing the technical scope of the Revision E Project, EUR and URD exchanged some technical information regarding the integration of the Fukushima lessons learnt into the Utility requirements.

A strong connection of EUR organisation with IAEA is assured by having a EUR seat as “corresponding member” in some IAEA working groups such as NUSC. This enables EUR to be aware as soon as possible of the trends and of the new Regulatory issues and able to interact with their development.

## 5. CHALLENGES TO COME

In accordance with the EUR 2016-2018 roadmap presented in a previous section, the EUR organisation is now facing new challenges for the coming years:

- To issue the Revision E of the EUR Document in 2017, to communicate and develop training course on it in order to promote its use. This major revision is of prime importance for the future new build projects in Europe;
- To perform new design assessments as the Vendors keep submitting applications to the EUR Organisation. At the date of the paper, the two design assessments expected to be completed in 2017 are the EU-APR from South Korean KHNP and the VVER-TOI from Russian AEP. Other Vendors are in contact with EUR organisation in order to perform assessment of their design against EUR Revision E;
- To keep improving nuclear industry through its requirements by preparing the scope of a new revision and identifying innovations, which could improve reactor competitiveness in the future. Driven by the interest of the nuclear industry, the work and promotion of the EUR requirements within Europe and worldwide will continue.

## 6. CONCLUSION

This paper has summarised the main results obtained by the EUR organisation over the last years. The development of the safest and the most competitive designs remain the highest priority for new nuclear build projects all over the world and in Europe in particular. In order to achieve this goal, the EUR organisation will keep on developing harmonized and standardized Utility requirements, which are based on a solid design, licensing and operating experience throughout Europe.

## REFERENCES

- [1] European Utility Requirements for LWR Nuclear Power Plants – Vol. 1, 2, 4, Rev. E, EUR Organisation (2017).
- [2] DE FRAGUIER, E., et al., The European Utility Requirements (EUR): a great achievement and still on its way, Paper ICONE21-16914, Proceedings of the ICONE 21 Conference, July 29-August 2, 2013, Chengdu, China.
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Standard Series, Specific Safety Requirements, No SSR-2/1, Safety of Nuclear Power Plants: Design (Rev.1), IAEA, Vienna (2014).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Standard Series, Specific Safety Requirements, No SSR-2/2, Safety of Nuclear Power Plants: Commissioning and Operation (Rev.1), IAEA, Vienna (2014).
- [5] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, Safety of New NPP Designs, a study by the Reactor Harmonisation Working Group, WENRA (2013), <http://www.wenra.org>
- [6] Safety Reference Levels for Existing Reactors, Update in relation to lessons learned from TEPCO Fukushima Daiichi accident, September 2014, WENRA organisation, <http://www.wenra.org>
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Structures, Systems and Components in Nuclear Power Plants, IAEA-SSG-30, IAEA, Vienna (2014).
- [8] Nuclear Power Plants – Instrumentation and Control important to Safety: General Requirements for Systems, IEC 61513 ed.2, 2011; Classification of instrumentation and control functions, IEC 61226, 2009.
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA-SSG-39, IAEA, Vienna (2016).

- [10] European Utility Requirements for LWR Nuclear Power Plants – Volume 3, Subset H – EUR Compliance Assessment of the MHI EU-APWR Design (restricted access), EUR Organisation (2015).
- [11] BALLARD, A., et al., Evolution of the EU-APWR design in order to satisfy the EUR, Paper ICONE23-1120, Proceedings of ICONE 23 Conference, Chiba, Japan, May 17-21, 2015.
- [12] FACCIOLO, L., et al., 2015, The EUR compliance analysis of the EU-APWR standard design: assessment process, methodology and main results, Paper ICONE23-1123, Proceedings of ICONE 23 Conference, Chiba, Japan, May 17-21, 2015.
- [13] European Utility Requirements, EUR Generic Assessment Principles, Version 1.0, June 2014.
- [14] European Utility Requirements, EUR Organisation Website, <http://www.europeanutilityrequirements.org>
- [15] European Nuclear Installations Safety Standards Initiative (ENISS), <http://www.eniss.eu>
- [16] WORLD NUCLEAR ASSOCIATION, Cooperation in Reactor Design Evaluation and Licensing (CORDEL), WNA Annual Report 2011-2012.

## MULTINATIONAL DESIGN EVALUATION PROGRAMME: 10 YEAR-ACHIEVEMENTS

J. COLLET  
ASN  
Montrouge, France  
Email: julien.collet@asn.fr

A. LORIN  
NEA  
Boulogne-Billancourt, France

### Abstract

The Multinational Design Evaluation Programme (MDEP) celebrated recently the 10<sup>th</sup> anniversary of its creation. In the past ten years, MDEP's reputation as an effective organisation for leveraging the resources and experiences of multiple nations for regulatory review of new reactors has grown significantly. As a result, the portfolio of new reactor designs that are being addressed has increased from two to five, with a possibility of adding more new reactor designs. Presently, the five design specific working groups activities are supported by three issue specific working groups. MDEP's membership has grown from the original 10 national regulators to 15.

Over the past 10 years, 25 common positions and 13 technical reports have been published by MDEP. In 2016, two generic common positions were issued at the level of the Steering Technical Committee: one on First Plant Only Tests and one addressing Fukushima Daiichi Nuclear Power Accident.

In 2015, the Policy Group extended the cooperation period from the end of 2017 to the end of 2022, focusing on its core mission of collaborating on new reactor design-specific activities. The scope of MDEP has been extended in 2016 to incorporate commissioning and early phase operation as an MDEP area of cooperation. MDEP maintains the cooperation with its main stakeholders, namely the industry representatives and other international organisations.

## 1. INTRODUCTION

MDEP is a multinational initiative that develops innovative approaches to leverage the resources and knowledge of national regulatory authorities who are, or will shortly be, undertaking the review of new reactor power plant designs. MDEP is primarily focused on design evaluation, but also includes inspection activities and generic issues.

## 2. BACKGROUND

### 2.1. Inception and membership of a first of a kind programme

In the early 2000's, nuclear regulatory organisations from Finland and France were shaping bilateral co-operation on the matter of design review of a new type of reactor, the EPR. In 2004, a first informal discussion among several experienced nuclear regulators took place in Paris. In March 2005, a second informal discussion was held in Washington DC, including the OECD Nuclear Energy Agency (NEA), the Generation IV International Forum (GIF), the US Department of Energy and the International Atomic Energy Agency (IAEA). In July 2005, the US NRC formulated a proposal of initiative on multinational co-operation on new reactor design reviews. Several meetings led to the drafting of project plans, of a working approach and, finally, of terms of reference mid-2006. In September 2006, the first "Policy Group" meeting to approve the project took place. In January 2007, MDEP was launched for a two-year pilot project. At that time, members included regulatory authorities from Canada, China, Finland, France, Japan, Korea, Russia, South Africa, United Kingdom and the United States. The IAEA has also taken part in the work of MDEP since the inception and the NEA was designated to fulfil the Technical Secretariat function in support of MDEP. Since then, MDEP membership has expanded to 15 by adding regulators from India and the United Arab Emirates in 2012, Sweden and Turkey in 2013, and lastly Hungary in 2015.

A key concept throughout the work of MDEP is that national regulators retain sovereign authority for all licensing and regulatory decisions.

## 2.2. An organisation with reactor design evaluation at its core

MDEP is governed by a Policy Group (PG), made up of the heads of the participating regulators. Succeeding to Mr André-Claude Lacoste (France, ASN) and to Ms Allison M. Macfarlane (USA, NRC), the PG chairmanship was transferred to the Director General of the Finnish nuclear regulator, STUK, in January 2015. The PG provides guidance to the Steering Technical Committee (STC) on the overall approach. The STC consists of senior staff representatives from each of the participating national safety authorities, plus a representative from the IAEA. The STC, chaired by the Deputy Director General of the French nuclear regulator, ASN, manages the design-specific and issue-specific working groups, approving their programme plans.

Five Design Specific Working Groups (DSWGs) are facilitating the MDEP goal of enhanced co-operation. The EPR Working Group (EPRWG) held its first meeting in 2008. It consists of the regulatory authorities of China, Finland, France, India, Sweden, the United Kingdom and the United States. The AP1000 Working Group (AP1000WG) was established in 2009 and consists of the regulatory authorities of Canada, China, Sweden, the United Kingdom and the United States. The APR1400 Working Group (APR1400WG) was created in 2013 and includes the regulatory authorities of Korea, the United Arab Emirates and the United States. The VVER Working Group (VVERWG) was initiated in 2014 and includes the regulatory authorities of China, Finland, Hungary, India, Russia and Turkey. The ABWR Working Group (ABWRWG) was the last group, created in 2014, and includes the regulatory authorities of Japan, Sweden, the United Kingdom and the United States. The DSWGs have been successful in sharing information and experience on the safety design reviews with the purposes of enhancing the safety of the design and enabling regulators to make timely licensing decisions, and of promoting safety and standardisation of designs through MDEP co-operation.

The five DSWGs are supported by three Issue Specific Working Groups (ISWGs): the Vendor Inspection Co-operation Working Group (VICWG), the Digital Instrumentation and Controls (I&C) Working Group (DICWG) and the Codes and Standards Working Group (CSWG). As these groups' activities are cross-cutting and can support any design review, the 15 MDEP members take part to the ISWGs. In addition to that, the DSWGs have established Technical Expert Subgroups to provide them with design-specific expertise on topics of their needs. The current structure of MDEP is as follows:

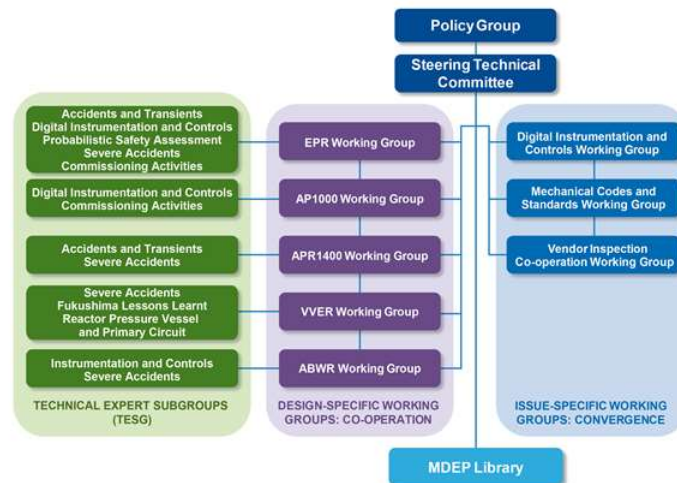


FIG. 1. Organisational structure of the Multinational Design Evaluation Programme Chart as of March 2017.

## 2.3. MDEP stakeholders

MDEP strives to maintain an awareness of, and interactions with, other organisations that are implementing programmes to facilitate international co-operation on new reactors. Interactions are focused on ensuring that MDEP does not duplicate efforts, benefitting from the outputs of these organisations, and communicating its activities and results to other organisations.

MDEP established and maintains high-level relationships with the IAEA, Western European Nuclear Regulators Association (WENRA), the NEA Committee on Nuclear Regulatory Activities (CNRA), the World Nuclear Association's Working Group on Cooperation in Reactor Design Evaluation and Licensing (CORDEL)

and GIF. It is worth highlighting that one of the aims pursued in the creation of CORDEL was to set up an industry counterpart and interlocutor to MDEP.

Working groups have established the necessary interfaces both within and outside of MDEP. The DSWGs are in contact with the vendor(s) and Owners and Operators Group (OOG) of the design they review. In addition to IAEA, the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronics Engineers (IEEE) are represented at the DICWG meetings. The DICWG members jointly review and comment on proposed IEC, IEEE and IAEA standards that are relevant to the regulatory review of digital I&C systems. The CSWG is working closely with standards development organisations (SDO) and CORDEL to converge code requirements related to pressure boundary components and to reconcile code differences.

To ensure that efforts are not duplicated between the groups, the MDEP scope is focused on short-term activities related to specific design reviews being conducted by the member countries, and efforts to harmonise specific regulatory practices and standards.

## **2.4. A five-year renewed mandate to sharpen goals and scope of activities**

The main objectives of the MDEP effort are to enable increased co-operation and establish mutually agreed upon practices to enhance the safety of new reactor designs. The enhanced co-operation among regulators enables to improve the effectiveness and efficiency of the regulatory design reviews, which are part of each country's licensing process. The goal of MDEP is not to independently develop new regulatory standards, but to build upon the similarities already existing, and existing harmonisation in the form of IAEA and other safety standards.

MDEP members work together and weigh each word to develop common positions on topics of common concern. Common position papers are approved by all member regulators in the working group. Working groups also develop technical reports to document different views on a topic. In addition to the work performed within the working groups, MDEP has provided each regulator with peer contacts who share information, discuss issues informally, and disseminate information rapidly.

MDEP has made improvements in communicating information regarding the members' regulatory practices through the development of an MDEP library, managed by NEA, which serves as a central repository for all documents associated with the programme.

Based on the value gained by the MDEP members during the five first years of the programme, it was extended for another five-year period in 2012 by the PG. Based on a thorough evaluation of data collected from member regulators in 2014, the PG made another decision to extend the co-operation period from the end of 2017 to the end of 2022, focusing on its core mission of collaborating on new reactor design-specific activities. At the same time, it decided that issue-specific working groups will be terminated in MDEP with the aim of continuing the work under NEA so as to benefit more member countries.

In addition to the original objectives of the programme, the lessons learnt from the Fukushima Daiichi nuclear power plant accident are being appropriately incorporated into MDEP activities in the DSWGs' programme plans. Recently, although the PG has determined that the full operational stage should not be included in the scope of MDEP, the scope has been expended to commissioning and early phase operation of about one year.

## **3. ACHIEVEMENTS**

Accomplishments to date provide confidence that the MDEP membership, structure and processes offer an effective method of accomplishing increased co-operation in regulatory design reviews. All published MDEP documents are available in the MDEP website [1].

### **3.1. STC undertakes special projects**

#### *3.1.1. Safety goals and self-assessment*

In 2011, the STC published a paper that reviews the high level goals used in MDEP countries and the relevant work of international groups. This paper was supplemented by a common position shared with IAEA on Safety Goals.



The STC also regularly reviews its processes to identify lessons learnt and improvements. In 2013, the STC issued a self-assessment report based on more than 100 survey collected.

### 3.1.2. *Fukushima Daiichi nuclear power plant accident lessons learnt and Vienna declaration*

Lessons learnt from the Fukushima Daiichi nuclear power plant accident are discussed by all of DSWGs and have been incorporated in their programme plans. MDEP recognises that other ongoing international initiatives are focused on operating plants. Therefore, MDEP considers important to address such issues for new reactors. The five DSWGs have completed their evaluation and published their findings(?) in a common position. These papers identify common approaches to address potential safety improvements as related to lessons learnt. Thus, the STC developed an integrated MDEP common position on the lessons learnt from Fukushima Daiichi nuclear power plant accident that integrates the common positions from all five DSWGs into a single MDEP position paper. This common position was published in September 2016 [2]. It includes a high-level statement on Vienna declaration identifying topics that may be addressed by design-specific working groups.

### 3.1.3. *First Plant Only Tests*

In 2014, the EPRWG initiated the draft of a common position addressing First Plant Only Tests (FPOT) on the EPR design. The aim of the common position is to provide guidance for licensees wishing to credit a test conducted during commissioning of the first unit of a design to characterise the performance and behaviour of a system or component on follow-on units constructed in another country. The member countries' requirements for crediting FPOT described in the appendices of the draft common position were found to be applicable to all designs. As a consequence, the draft EPR common position was reviewed by the other DSWGs and turned into a generic MDEP common position. This common position was published in May 2016 [3]. Its appendices provide an early insight to the licensees on what requirements they will have to fulfil to make a FPOT acceptable. The first implementation of FPOT is well underway with the EPR Taishan unit 1 reactor pressure vessel internals vibration FPOT.

## 3.2. **Design Specific Working Groups accomplishments**

In addition to the work mentioned above, the DSWGs have published ten common positions and several technical reports during the ten past years. To be noted is for instance the AP1000WG common position on squib valve design or the EPRWG common positions on the DI&C design of the EPR or on the EPR containment mixing (cf. paper addressing this issue), containment heat removal system in accident conditions or in-containment refueling water storage tank pH control in accident conditions.

## 3.3. **Issue Specific Working Groups accomplishments**

The Vendor Inspection Co-operation Working Group achieved its generic goals with the completion of a number of common positions and technical reports on quality assurance/quality management criteria, vendor inspection good practices and multinational vendor inspection. The working group also established a protocol for joint or witnessed vendor inspection. The VICWG has performed numerous joint or witnessed inspections since its creation and two multinational vendor inspections, the last one having been performed at the Areva Le Creusot plant. The VICWG is also interfacing with standards development organisations to encourage and explore harmonisation of quality standards.

The Digital Instrumentation and Controls Working Group has issued twelve common positions so far based on the existing standards, national regulatory guidance, best practices, and group inputs using an agreed upon process and framework. These common positions describe methods and evidence that all DICWG member countries find acceptable to support safety justification for digital I&C systems. The DICWG common positions published are mentioned in the figure below and have been classified according to I&C architecture and design; quality and verification & validation; and hazards and reliability categories [4].

	I&C Architecture and Design	Quality and V&V	Hazards and Reliability
CP 01 (CCF)			✓
CP 02 (Software tools)		✓	✓
CP 03 (V&V)		✓	✓
CP 04 (Comm. Independence)	✓		✓
CP 05 (Hardware Description Language)	✓		
CP 06 (Simplicity)	✓		
CP 07 (Industrial Digital Device)	✓		
CP 08 (Impact of Cyber Security)	✓		✓
CP 09 (Overall Architecture)	✓		
CP 10 (Hazard ID. & Control)			✓
CP 11 (Pre-installation & Initial testing)		✓	
CP 12 (Auto. Test as Surveillance test)	✓	✓	✓
CP 13 (Spurious Actuation)			✓

FIG. 2. MDEP DICWG common positions relationships.

The Codes and Standards Working Group is working closely with standards development organisations to converge code requirements related to pressure boundary components and to reconcile code differences. The working group has successfully completed its goal and mandate to achieve some harmonisation and identify the challenges in harmonising codes and standards. The group has encouraged and pushed the industry and the SDOs to move forward and work co-operatively. The working group has finished its work, with its only outstanding mandate of continuing to interact with the industry. Amongst CSWG's products found to be helpful are the Pressure boundary code comparison (with industry cooperation) and technical reports on the regulatory frameworks for pressure-boundary codes and standards, on the lessons learnt on achieving harmonization, on the fundamental attributes for pressure boundary components and on the essential performance guidelines for pressure boundary components.

#### 4. PERSPECTIVES AND CONCLUSION

MDEP achievements have proven to be significantly beneficial to MDEP members.

For this reason, the programme is continuing on beyond 2017. The design-specific working groups will continue co-operation and exchanging feedback on design issues through the construction and commissioning phases and will incorporate feedback from operating experience as it pertains to design. As the current issue-specific working groups are completing the goals and activities specified in their programme plans, transfer of their generic activities to the NEA is being worked out. Completion strategies that include products, schedules and recommendations for ensuring the continuation of the interactions among the regulators, and between regulators and external stakeholders when these activities are transferred, are being developed. As for DSWGs, the programme is open to considering adding more new reactor designs if regulators from at least three countries express interest in working together.

At the important milestone of its 10<sup>th</sup> anniversary, MDEP is hoping to gather feedback on its current activities and discuss its future. To this end, MDEP is organising its fourth MDEP conference to be held in September 2017 in London, United Kingdom [5]. The event will provide a forum for MDEP stakeholders (including industry representatives, standard development organisations and other international organisations) to share the results of their engagement with the programme and to deliver presentations on ongoing activities related to new reactor licensing.

#### REFERENCES

- [1] OECD NUCLEAR ENERGY AGENCY, Multinational Design Evaluation Programme, <http://www.oecd-nea.org/mdep/>
- [2] NUCLEAR ENERGY AGENCY, MDEP Common Position CP-STC-02, Common Position Addressing Fukushima Daiichi Nuclear Power Accident.
- [3] NUCLEAR ENERGY AGENCY, MDEP Common Position CP-STC-01, Common Position addressing First-Plant-Only-Tests (FPOT).

- [4] NUCLEAR ENERGY AGENCY MULTINATIONAL DESIGN EVALUATION PROGRAMME, MDEP Technical Report TR-DICWG-01, Technical Report on the Relation Structure of the Digital Instrumentation and Controls Working Group (DICWG) Common Positions, October 2016.
- [5] MDEP Fourth Conference on New Reactor Design Activities, <https://www.oecd-neo.org/mdep/events/conf-2017>.

## **SAFETY REINFORCEMENT OF EXISTING INSTALLATIONS**



NATIONAL STRATEGIES TO IMPLEMENT INTERNATIONAL SAFETY  
REQUIREMENTS

**Chairperson**

**M. HIRANO**

Japan



## ENSURING SAFETY REGULATION FOR SUSTAINABLE DEVELOPMENT OF NUCLEAR POWER

D. BHATTACHARAYA

Atomic Energy Regulatory Board, Anushakti Nagar, Mumbai, India-400094

E-mail: diptojoyoti@aerb.gov.in

J. KOLEY

Atomic Energy Regulatory Board, Anushakti Nagar, Mumbai, India-400094

E-mail: jkoley@aerb.gov.in

P.R. KRISHNAMURTHY

Atomic Energy Regulatory Board, Anushakti Nagar, Mumbai, India-400094

Email: prk@aerb.gov.in

### Abstract

Achievement of high safety standard is essential for ensuring sustainability of nuclear power generation. Regulatory requirements for ensuring safety in design is very crucial so that due priority is given to safety during design of NPPs. These requirements need to be changed from time to time in order to refresh the concepts and goals of safety with evolution of technology accommodating innovations, experience from design, construction and operation as well as experience from major nuclear events in the world. Public expectations of safety, socio economic situations and demographic conditions plays a major role in framing safety goals. Large scale contamination of land and crops or relocation of public living in the vicinity of NPPs for indefinite time frame has become unacceptable. AERB recently published 'Safety Code on Design of Light Water Reactor Based Nuclear Power Plants,' stating mandatory requirements for design of light water based Nuclear Power Plants (NPP), intended to ensure the highest level of safety that can reasonably be achieved. New requirements redefined the concept of 'Defence in Depth' by introducing 'Design Extension Conditions' (DEC) in National safety regulation. The code also specifies requirements with respect to public dose for Design Basis Accidents and Design Extension Conditions and provides regulatory approach in the area of beyond design basis including severe accidents as well as extreme/unexpected events.

### 1. INTRODUCTION

Requirement of electricity generation and reliable distribution is increasing day by day in India. India is the 3rd largest power producing country in the world. Nuclear power generation is around 1.8% of the total installed capacity in India. Capacity addition in nuclear sector is continuing and expected to be significant in future. But after accident in Fukushima Daiichi NPP in Japan, ensuring nuclear safety during a design extension condition has gained paramount significance.

Nuclear power plant design considers design basis accidents (DBA) in Defence-in Depth level III. Design of safety systems requires adherence to specific design philosophy like compliance to single failure criteria, redundancy, diversity, common cause failure, fail safe design etc. If same set of rules are applied for systems required to function in Design Extension Conditions (DEC), the design becomes very complex and inappropriate for the purpose. Further this can make nuclear power generation unsustainable. So, making rules for designing systems required during design extension condition is very challenging. Design agencies require specific guidelines for designing systems integrated with main plant design which will be useful to meet the safety requirements during extreme exigencies.

Post Fukushima accident, Indian regulators faced the challenge to set up rules for designing systems needed in DEC conditions (Defence-in Depth level IV). Graded approach followed and design extension condition was subdivided into two parts: Design Extension Condition A (DEC-A) which includes accident without core melt and Design Extension Condition B (DEC-B) which includes accident with core melt. Design requirements are specified for systems those will function during design extension condition. These requirements are philosophically different than design rules applicable for designing safety systems meant for controlling or mitigating design basis accident.



## 2. CHALLENGES IN FRAMING NEW DESIGN RULE FOR SYSTEMS REQUIRING DURING DEC

As per established safety requirement, structures systems and components that will be functional up to DBA (Defence in Depth Level III) should meet single failure criteria. To meet single failure criteria, redundancy is provided in system design. So, concept of multiple safety system trains is applied to address Design Basis Accident which is defined as “Accident conditions against which a nuclear power plant is designed according to established design criteria (including single failure criteria), and for which the damage to the fuel and the release of radioactive material are kept within authorized limits”. When multiple failure takes place, which are independent to each other, it is termed as DEC. Extreme external event causing common cause failure need to be addressed in this case. Providing redundant system equipment may not be enough or sufficient under this condition. Diversity in system with different operating principle than that used for systems required during design basis accident need to be emphasised. Possibility of hook up external means for power supply and cooling water supply, design provision for measurement or monitoring important parameters ensuring nuclear safety, different set of equipment for measurement of off normal parameters expected during accident condition could be the solution.

In certain cases, provision of redundancy may not be possible like provision for retaining and cooling molten corium in subcritical condition. For such systems, ensuring physical integrity and cooling is most important under that prevailing environmental condition which is definitely a challenge.

Extreme external event can cause serious damage to multiple units. In order to cater the safety requirement of multiple units, design provision (hardware) shall exist to bring the units in severe accident safe state ensuring sub-criticality and long term decay heat removal. It is also expected that external aid may not reach the location of power plant promptly. Thus, site of the power plant shall have its own source of power (DG sets and fuel) and cooling water for a reasonable period (at least for seven days) acceptable to regulators.

## 3. MODIFICATION IN NATIONAL REQUIREMENT

Nuclear power plant design has evolved and matured progressively. The nuclear accidents taught valuable lessons to both power plant designers and regulators. It has been understood that more and more development in design and understanding the abnormal operation progression has serious bearing on public domain intervention. It has been realised that suitable design and augmentation in emergency provisions can drastically reduce required action in public domain. In order to reduce the consequence of a severe accident, several regulatory provisions have been made. The philosophy which has been followed is “device design provision in such a way that possibility of a severe accident is very remote and if such accident happens design provisions will be there to reduce the consequence within acceptable limit”. In order to achieve the goal of this philosophy regulatory requirements are framed.

### 3.1. Rearrangement of Defence in Depth

In the design code for the light water reactor (AERB/NPP-LWR/SC-D) the concept of design extension condition is included. Design extension condition has been subdivided into ‘DEC-A’ where it is expected that some fuel failure may take place but gross fuel failure or core melt can be avoided by means of design provisions other than safety systems provided for design basis accident. In ‘DEC-B’, gross fuel failure and core melt is considered. In this level the main target is to prevent re-criticality of the molten corium and ensure containment function. Accident sequence leading to large release or early release need to be practically eliminated. The entire regime of condition is given in Fig. 1.

In order to bring design extension conditions within design basis and make provisions for systems to be available during DEC-A condition, concept of Additional Safety Systems (ASS) are introduced. The additional safety systems are those systems which are required to cool the nuclear fuel but different than safety system provided for nuclear fuel during design basis accident like Emergency Core Cooling System. Additional safety system may not meet the redundancy criterion but must meet diverse principle of action. Designers need to establish that in case of multiple failures, the additional safety system can prevent large scale fuel failure.

Operational states		Accident conditions		Conditions practically eliminated
NO	AOO	DBAs	Design Extension Conditions	
		Design Extension Conditions		
		No core melt	Severe Accidents (core melt)	
Included in the design basis				Beyond design basis

FIG. 1. The entire regime of condition.

In order to prevent re-criticality of molten corium and containment failure in DEC-B condition, concept of Complementary Safety Features (CSF) is introduced. Again the complementary safety features may not meet the redundancy principle but should be able to meet the requirement of controlling the fission chain reaction, cool the molten corium in limited way and ensure containment function to prevent large and early radioactivity release. The systems required at different plant condition are given in Fig. 2.

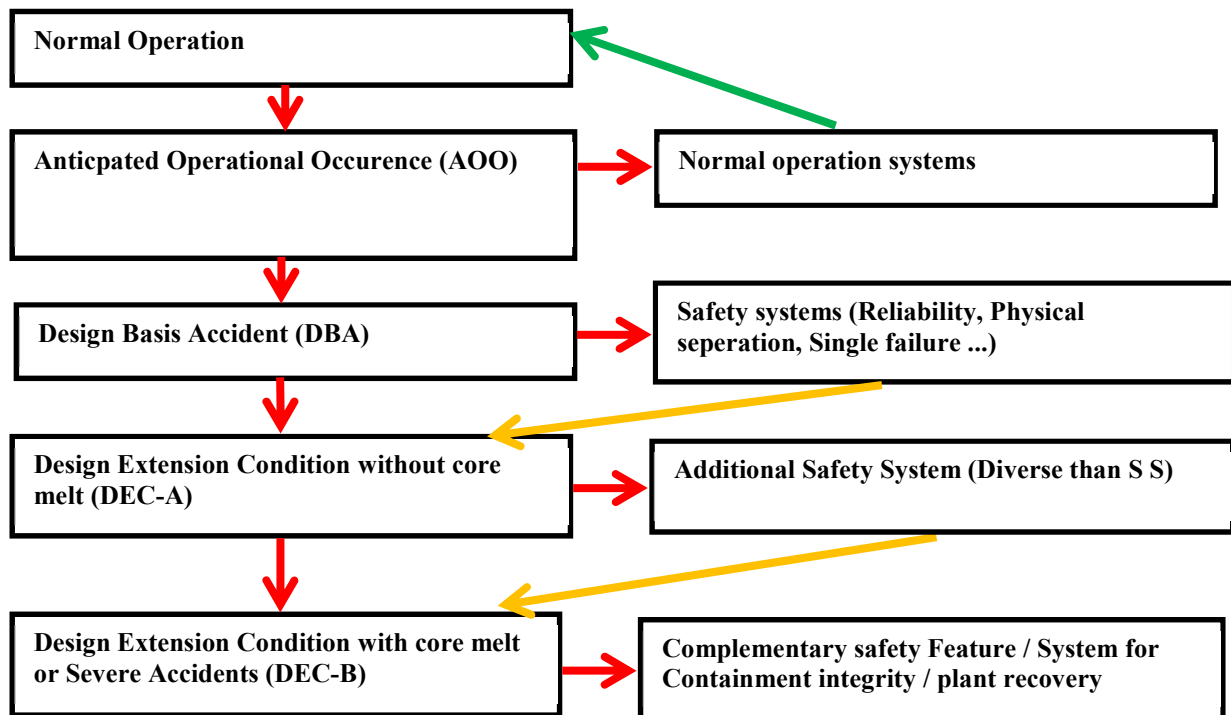


FIG. 2. The systems required at different plant condition.

### 3.2. Dose criteria for design of systems and emergency actions

During normal operation and Anticipated Operational Occurrences dose criteria for the member of public is fixed to  $\leq 1$  mSv/year. For design basis accident (DBA) in a NPP, the design should be such that there shall not be any need for offsite countermeasures (i.e. no need for prophylaxis, food control, shelter or evacuation) involving public, beyond exclusion zone (1.6 km for older plant and minimum 1.0 km for newer plants). In such

cases the design target for effective dose calculated using realistic methodology shall be less than 20.0 mSv/ year following the event. This target is fixed so that in a long window period the cumulative dose does not cross 100 mSv for a member of a public (to avoid possibility of deterministic effect).

For accidents without core melt within design extension conditions (multiple failures and rare external events) there shall be no necessity of protective measures in terms of sheltering or evacuation for people living beyond Exclusion Zone. Required control on agriculture or food banning should be limited to a small area and to one crop. However, the design target for effective dose, with such interventions considered, remains same as for DBA i.e. 20.0 mSv/ year following the event.

In case of severe accident i.e. accidents with core melt within design extension conditions (DEC-B), the release of radioactive materials should not lead to a situation requiring permanent relocation of population. Though there is no dose criteria for DEC-B condition but the requirement for offsite interventions should be limited in area and time which is considered as severe accident mitigation goal. Indian utility has proposed that in case of severe accident with core melt the target radioactivity release should be limited to 100 TBq of Cs-134 and Cs 137. To achieve this safety goal, ensuring containment function is essential. Two such possibilities which can threat the containment integrity are hydrogen explosion within the containment and over pressurization (beyond design limit) of the containment following an accident sequence. Such possibilities shall be controlled by design provisions.

### 3.3. Practically Eliminated Events

The design of nuclear power plant shall be such that accident sequence that could lead to large or early releases of radioactivity are practically eliminated. All abnormal situations and event progression shall be analyzed and any possible combination of events that can significantly increase the likelihood of releasing large quantity of radioactivity shall be avoided by design provision. Design extension conditions those cannot be practically eliminated shall be controlled by adopting only protective measures those are of limited scope in terms of area and time for protecting the public from over radiation exposure. Design shall be such that sufficient time will be available to implement the required counter measures.

### 3.4. Reinforcing and enhancing further safety

If a design meets the above requirements, with a high degree of confidence it can be stated that severe accident due to internal events can be avoided. However, possibility of extreme external natural event cannot be ruled out. National requirement states that designers / utility shall provide means to mitigate the consequence of an unexpected events by a diverse and flexible accident response capability. Flexible accident management capability can include portable and mobile backup provisions to permanently installed plant safety systems and smart operators with given flexibility to respond as necessary. It is expected that the designers shall provide alternate and diverse means for nuclear fuel cooling, sufficient availability of cooling water, backup power supply for critical parameter monitoring and enhanced onsite emergency response capability.

## 4. CONCLUSION

In order to meet the challenge of climate change and sustainable development, power generation from nuclear fuel is inevitable. The risk of nuclear accident can be reduced by suitable design provisions and emergency response provisions by the operators. Large scale acceptability of Nuclear power by public is possible if suitable regulation is implemented and nuclear power generation can be rendered very low risk other than due to extreme external events which are not considered in design.

## REFERENCES

- [1] ATOMIC ENERGY REGULATORY BOARD, "Site Evaluation of Nuclear Facilities", AERB/NF/SC/S (Rev.1), AERB, Mumbai (2014).
- [2] ATOMIC ENERGY REGULATORY BOARD, "Design of Light Water Reactor Based Nuclear Power Plants", AERB/NPP-LWR/SC-S, AERB, Mumbai (2014).

## ANALYSES OF DEC FOR NPP'S IN THE CZECH REPUBLIC AND THEIR IMPLEMENTATION INTO SAR

P. KRÁL

Nuclear Research Institute (UJV) Rez  
Husinec-Rez, Czech Republic  
Email: pavel.kral@ujv.cz

J. KRHOŮNKOVÁ

Nuclear Research Institute (UJV) Rez  
Husinec-Rez, Czech Republic

J. MACHÁČEK

CEZ – Temelin NPP  
Temelin, Czech Republic

### Abstract

The paper is devoted to the concept of design extension conditions (DEC) and its application and assessment at the Czech nuclear power plants Dukovany (VVER-440) and Temelin (VVER-1000). Starting from evolution of the DEC concept and the role of EUR, WENRA and IAEA – the current status of the DEC concept and its implementation in the Czech Republic is described. The core of the paper is focused on the deterministic safety analyses of design extension conditions without core melt (DEC-A) in the Czech Republic. All major steps and tasks connected with this part of DEC safety assessment are described – methodology basis, role of probabilistic safety assessment, selection of events, computer tools used and their validation, and finally overview and example of safety analysis and incorporation of DEC analyses results into modified format of Safety Analysis Report (SAR).

### 1. INTRODUCTION

When speaking about safety assessment of design extension conditions, i.e. analyses of events beyond design basis accident, one should distinguish between analyses of DEC without core melt (marked DEC-A in the paper) and analyses of DEC with core melt (marked DEC-B in the paper).

Whereas the later (DEC-B, severe accidents) have been widely assessed and analyzed for at least 2 decades with the accelerator moment of Chernobyl accident, the former (DEC-A, BDBA) were analyzed in the past only partially – typically only the anticipated transient without scram (ATWS) or station blackout (SBO) were analysed and documented in Safety Analysis Report (SAR).

The more systematic work on safety assessment of DEC-A (BDBA) has been started only in the last decade with different starting point and speed in various countries. This effort has been initiated by initiatives and suggestions of European Utility Requirements (EUR) [1], WENRA safety reference levels [7] and IAEA introducing DEC term and concept into the safety standards series [12, 14].

The work on BDBA and DEC safety analyses for Czech NPPs was initiated in 2009 as a consequence of the Periodical Safety Review (PSR) after 20 years of the operation of the Dukovany NPP.

### 2. EVOLUTION OF THE DEC CONCEPT

The term and concept of Design Extension Conditions (DEC) is a new step in evolution of the nuclear safety (see the chronology below). It is a logical follower of previous concept of “design basis” and “design basis accident” supplemented in last decades by analyses of ATWS, SBO and severe accidents (not fully systematic and not reflected in design basis).

Chronology of evolution of basic concept of nuclear safety:

- Worst Conceivable Accident (1940's)
- Maximum Credible Accident (1950's) to
- Design Bases Accident, DBA (from 1960's) to
- Plant Design Envelope, PDE incl. Design Extension Conditions, DEC (2010's)

The term “Design Extension Condition” (DEC) was first introduced in the European Utility Requirements (EUR) in 1992 [1] to define some selected sequences due to multiple failures with the intent to improve the safety of the plant extending the design basis. The DEC are in EUR divided to “complex sequences” and “severe accidents” (corresponding to DEC-A and DEC-B in WENRA terminology).

WENRA published in 2008 document “Reactor Safety Reference Levels” (RL’s) and used firstly the term “design extension” and later in 2014 update of the WENRA RL’s document [7] added clear differentiation between DEC without core melt (DEC-A) and DEC with core melt (DEC-B).

It is worth noting that the evolution of DEC concept was strongly accelerated by the Fukushima accident in 2011 and by following ENSREG activities.

In 2012 the IAEA SSR 2/1 [12] introduced the term and concept of “Design Extension Conditions” into the system of IAEA Safety Standards. The concept of DEC was further elaborated in Revision-1 of IAEA SSR-2/1 (2016) and in other IAEA documents as IAEA SSG-30 (2014), TECDOC-1791 (2016), GSR-Part4 (Rev.1, 2016). DEC will be also an important change in revisions of SSG-2 and GS-G-4.1 guides (to be issued in 2018). Current definition of “design extension conditions” according to Revision 1 of SSR-2/1 (2016) and IAEA Glossary is as follows:

Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process for the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits.

Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with core melting.

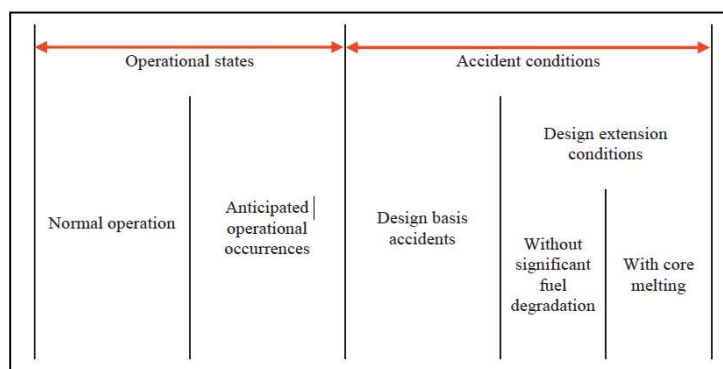


FIG. 1. Plant states including DEC (according to Rev.1 of SSR-2/1, 2016 [12]).

UJV Rez has participated actively both in development of EUR (through CEZ membership, from 2007) and in development and revising of IAEA documents.

### 3. METHODOLOGY BASIS FOR DEC-A ASSESSMENT IN THE CZECH REPUBLIC

Aside the IAEA recommendations and the Czech Atomic Law, the following regulations, directives and reports constitute the legislative and methodological basis for deterministic analyses of DEC-A (BDBA) in the Czech Republic:

SUJB regulation 195/1999, Requirements on Nuclear Facilities for Ensuring of Nuclear Safety, Radiation Protection and Emergency Preparedness, 1995.

SUJB directive BN-JB-1.6, Probabilistic Assessment of Safety, 2010 (currently revised due to new Atomic Law).

SUJB directive BN-JB-1.7, Selection and Assessment of Design and Beyond Design Events and Risks for Nuclear Power Plants, 2010[2] (currently revised due to new Atomic Law).

UJV, Proposal of Methodological Procedure for Performing of Safety Analysis of Beyond Design Basis Accident, UJV Rez, 2010 [3].

Analyses of DEC-A scenarios use best estimate computer codes with combination of realistic initial and conservative (or realistic) boundary conditions. The robust design of VVER reactors and their safety features

enable to fulfil DBA acceptance criteria in most DEC-A cases including radiological consequences. For the most severe conditions comprising multiple failures of safety systems or safety groups providing protection in the level 3a of Defence in Depth (like SBO), the new measures implemented after post-Fukushima Stress tests in the level 3b of DiD provide additional robust protection against evolution of these scenarios into DEC-B (severe accident). The acceptance criteria applied to DEC-A analyses are identical to those applied to DBA analysis with exception of criterion on primary and secondary pressure and radiological consequences.

The computer code used for NPP safety analyses in the Czech Republic must be approved by the regulatory body according to SUJB directive VDS-030.

#### 4. OVERALL APPROACH TO SAFETY ASSESSMENT OF DEC IN THE CZECH REPUBLIC

Introduction of DEC concept into area of safety assessment field in the Czech Republic has different impacts in different subareas like probabilistic analysis, deterministic analyses of DBA andbdba, and deterministic analyses of severe accidents.

Whereas the probabilistic and severe accident analyses were not too much affected by implementation of DEC concept (as the relevant sequences had been analysed before), the deterministic analyses ofbdba (DEC-A) got new strong impulse. And the conceptual and terminological changes in DBA-DEC area are still under evolution.

#### 5. SELECTION OF DEC-A EVENTS TO BE ANALYSED AND DOCUMENTED IN SAR

The basic set of DEC-A (bdba) events to be analysed is specified in BN-JB-1.7[2]. Supplemental events and scenarios could be specified by PSA outcomes and engineering judgement.

It is important to mention that in analyses of DEC (which are often complex sequences or combinations of events and failures) it is logical to transfer from “frequency of initial events” to “frequency of occurrence of scenarios”.

SUJB directive BN-JB-1.7 [2] requires besides the standard set of ATWS analyses the following DEC-A (bdba) events to be analysed:

- Total long-term loss of inner and outer AC power sources;
- Total long-term loss of feed water („feed-and-bleed,, procedure);
- LOCA combined with the loss of ECCS;
- Uncontrolled reactor level drop or loss of circulation in regime with open reactor or during refuelling;
- Total loss of the component cooling water system;
- Loss of residual heat removal system;
- Loss of cooling of spent fuel pool;
- Loss of ultimate heat sink (from secondary circuit);
- Uncontrolled boron dilution;
- Multiple steam generator tube rupture;
- Steam generator tube ruptures induced by main steam line break (MSLB);
- Loss of required safety systems in the long term after a design basis accident.

The whole set of prescribed DEC-A analyses was already performed both for Dukovany NPP (VVER-440) and for Temelin NPP (VVER-1000).

As for the documentation of DEC-A analyses in Safety Analysis Report, the temporary solution was creation of a new subchapter 15.9.1 which contains basic results of all DEC-A (bdba) analyses required by BN-JB-1.7.

The final foreseen solution is introduction of new SAR charter 19, that would contain both DEC-A (bdba without core melt) and DEC-B (severe accident) analyses presented in systematic and integrated way. Then the Chapter 15 will be again intended for analyses of events up to DBAonly.

Analyses of DEC-A events for the Czech NPP's have been done with help of RELAP5 computer code. It is worth noting that RELAP5 has been in UJV Rez validated against experimental data from more than 20 tests carried out at various integral test facilities (ITF) and that approximately half of these tests were modelling events of DEC-A type.

# 6. EXAMPLE OF DEC-A ANALYSIS: SBLOCA IN VVER-1000 WITH FAILURE OF ECCS AND OPERATOR START OF HPSI AT 30 MIN

Analysis of small break loss of coolant accident (SBLOCA) with break D50 mm in cold leg and with failure of start of emergency core cooling systems (ECCS) and operator manual start of high pressure safety injection (HPSI) at 30 min was performed for VVER-1000. Nodalization scheme of VVER-1000 for RELAP5 used and graphical courses of main parameters are shown in Fig.2 – Fig.6 below.

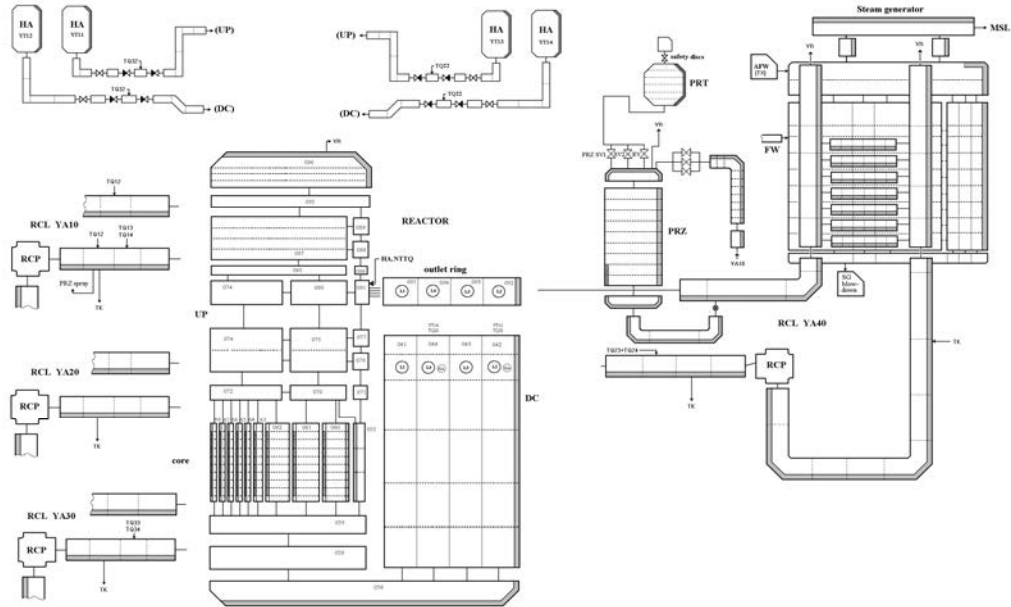


FIG. 2. Nodalization scheme of VVER-1000 for RELAP5 (only primary circuit and 1 of 4 modeled loops depicted).

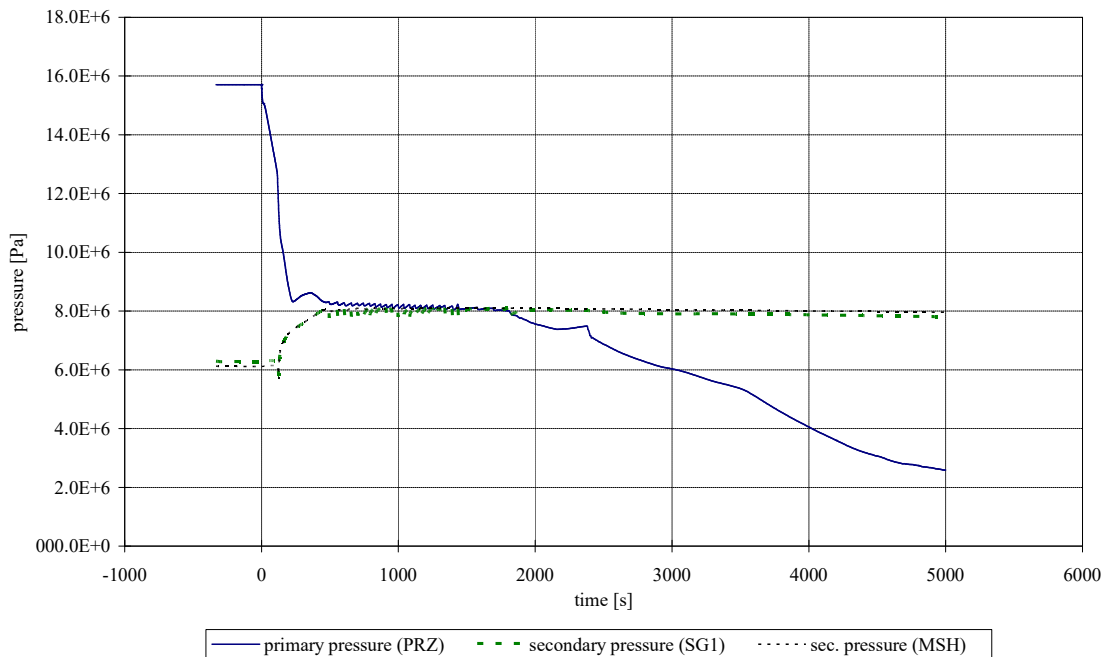


FIG. 3. Primary and secondary pressure (SBLOCAD50mm in VVER-1000 with failure of ECCS).

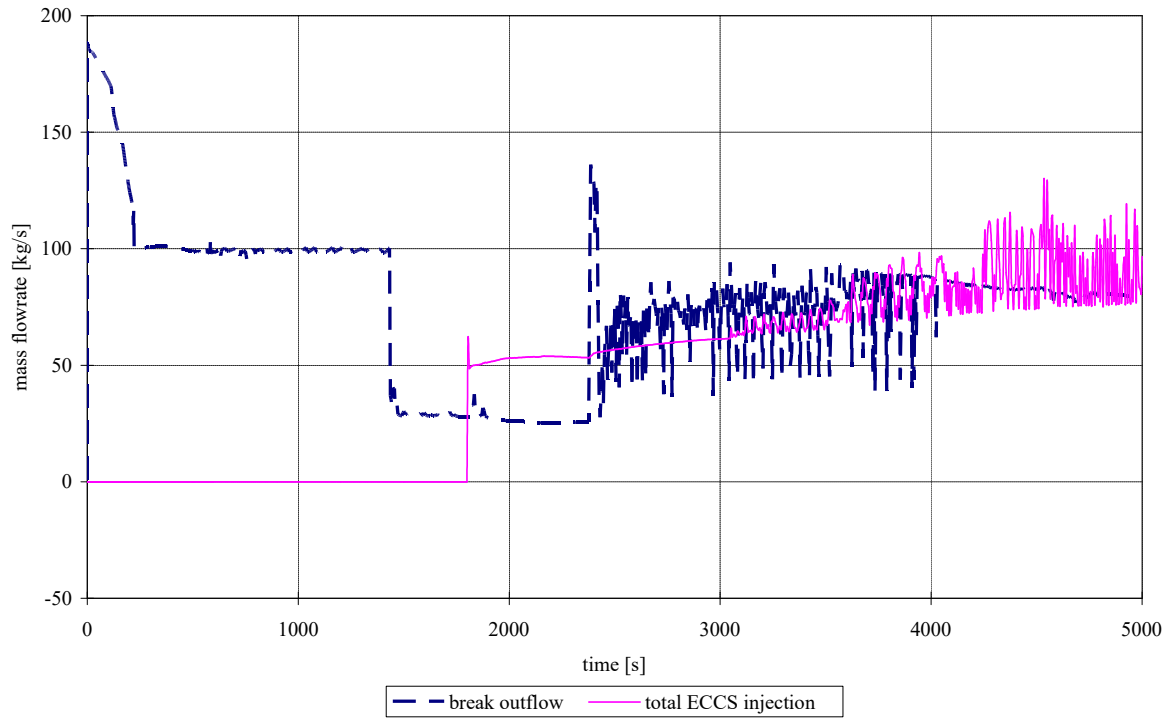


FIG. 4. Break outflow and total ECCS injection (SBLOCA D50mm in VVER-1000 with failure of ECCS).

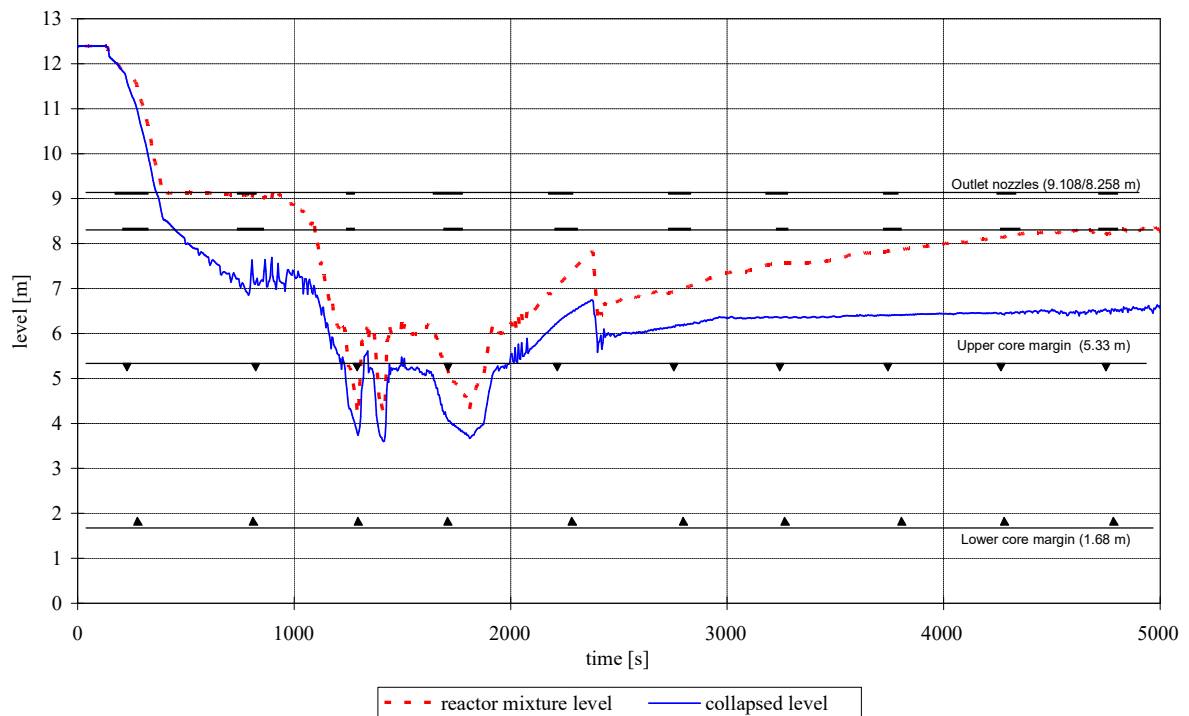


FIG. 5. Reactor levels (SBLOCA D50mm in VVER-1000 with failure of ECCS).

Loss of primary coolant through break D50mm in cold leg and without automatic actuation of ECCS leads to depletion of primary inventory and if not mitigated by operator, core uncover and overheating. However, with respect to high “water volume to power ratio” in VVER-1000, there is sufficient time for operator intervention. In the presented case, operator starts one HPSI pump at 30 min and soon after it the core is quenched and core cooling is restored and stabilized.



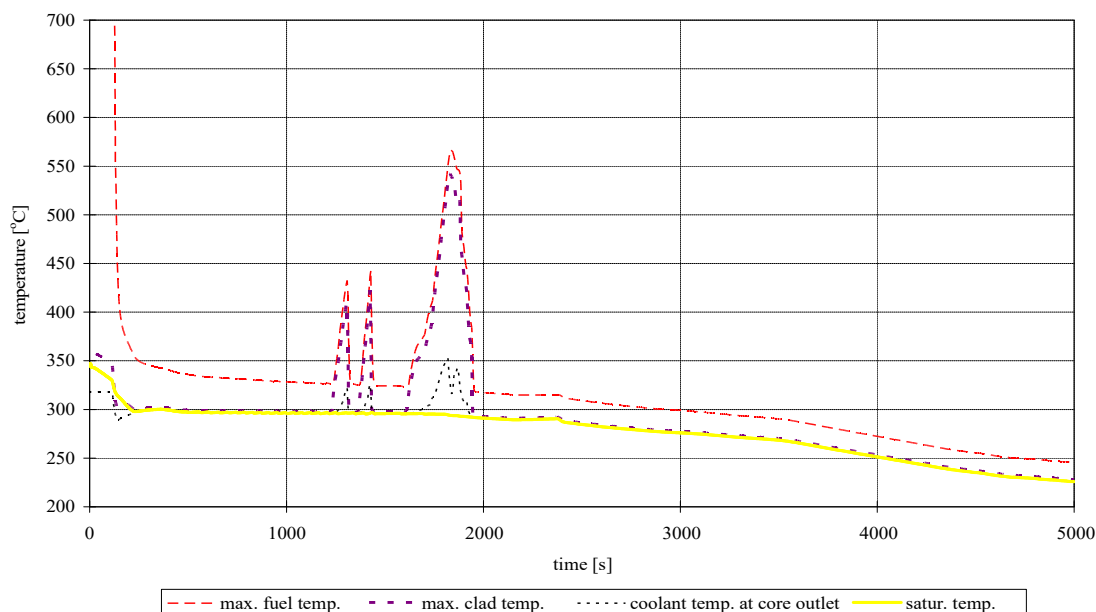


FIG. 6. Reactor core temperatures (SBLOCA D50mm in VVER-1000 with failure of ECCS).

## 7. SUMMARY

The work briefly described in the paper has been focused on the implementation of design extension conditions (DEC) concept to safety assessment of Czech nuclear power plants Dukovany (VVER-440) and Temelin (VVER-1000). The core of the paper is focused on the deterministic safety analyses of the design extension conditions without core melt (DEC-A). All major steps and tasks connected with this part of DEC safety assessment are described – methodology basis, selection of events, computer tools used and their validation, and finally overview safety analyses performed example of results and incorporation of them into modified format of Safety Analysis Report (SAR).

## REFERENCES

- [1] EUR, European Utility Requirements for LWR Nuclear Power Plants, Rev. D, 2012.
- [2] SUJB directive BN-JB-1.7, Selection and Assessment of Design and Beyond Design Events and Risks for Nuclear Power Plants, 2010.
- [3] KRHOUNKOVA, J., KRÁL, P., MACEK, J., Proposal of Methodological Procedure for Performing of Safety Analysis of Beyond Design Basis Accident, Revision 1, UJV Rez, 2010.
- [4] KRÁL, P., Analyses of Beyond Design Basis Scenarios of LOCA with Reduced Availability of ECCS, 2012.
- [5] BENCIK, M., Analysis of Total Long-Term Loss of Inner and Outer AC Power Sources in NPP Temelin, 2015.
- [6] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, Statement and Report on Safety of New NPP Designs, 2013.
- [7] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, Reactor Safety Reference Levels for Existing Reactors, 2014.
- [8] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, Guidance Document Issue F: Design Extension of Existing Reactors, 2014.
- [9] SNETP, Identification of Research Areas in Response to the Fukushima Accident, 2013.
- [10] NUGENIA, Global Vision, 2015.
- [11] OECD NUCLEAR ENERGY AGENCY, Implementation of Defence in Depth at Nuclear Power Plants, 2016.
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Specific Safety Requirements, SSR-2/1 (Rev. 1), IAEA, Vienna (2016).
- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, General Safety Requirements, GSR Part 4 (Rev.1), IAEA, Vienna (2016).

- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA-TECDOC-1791, Considerations for the application of the IAEA Safety Requirements on Design, IAEA, Vienna (2016).
- [15] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA-SSG-30, IAEA, Vienna (2014).
- [16] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, Terminology used in nuclear safety and radiation protection, IAEA, Vienna (2016).

## APPLICATION OF THE CONCEPT OF DEFENCE IN DEPTH TO THE EPR REACTOR DESIGN

E. COURTIN  
AREVA NP  
Paris, France  
Email: etienne.courtin@areva.com

### Abstract

The application of defence in depth has been improved in Generation 3 NPPs in two main directions: the improvement in the core melt prevention for complex sequences and the consideration of core melt situations in the design. This can be illustrated by EPR design.

The plant safety is primarily based on a robust list of design basis conditions (DBC) designed by considering single initiating internal events that challenge the main safety functions. In Gen 3 NPPs these accidents shall include events initiated in the spent fuel pool and also events initiated during any plant shutdown mode.

Design Extension Conditions without significant fuel degradation (DEC-A) are meant to prove core melt prevention capability of the plant in complex sequences. The first step is to build the list of relevant sequences in close link with the probabilistic targets of core melt.

DEC conditions with significant fuel degradation (i.e. core melt, DEC-B) are deterministically postulated in the design. The list of EPR core melt design situations results from the identification of the specific physical phenomena expected to occur during core melt and dedicated systems are designed to address them. The significant fuel degradation situations that cannot be reasonably controlled are demonstrated to be practically eliminated.

This article will explain how the EPR model implements the concept of defence in depth, relying on a very strong main line of defence for DBC, complemented by independent features designed to prevent fuel degradation or limit its consequences.

## 1. INTRODUCTION

The concept of defence in depth is a cornerstone of Nuclear Power Plant Safety. This concept is not new in the NPP design though its application to Generation 3 NPPs leads to extend the understanding of how should each level of defence be implemented in order to meet the stringent safety objectives that are now applicable to new reactors.

The paper develops the application of defence in depth concept to EPR reactor design; it mainly focuses on the methods applied regarding internal events (excluding hazards) in 3<sup>rd</sup> and 4<sup>th</sup> levels of defence in order to achieve European safety objectives (as they are set in ref. [1] and [2]). Note that, even though the objectives are the same in all EPR Projects, the methodology described here after reflects the up to date process and it may differ on the ongoing projects.

## 2. PRINCIPLES

### 2.1. Safety objectives

As a generation 3 nuclear reactor, the EPR model aims at having only limited detrimental impact on the population and the environment, even in case of a postulated core melt situation. The various safety objectives considered in EPR design for different kinds of design conditions are those in force in the Western Europe. Some of these objectives are recalled below, as they are stated in ref. [2].

#### ***Accidents without core melt***

*ensuring that accidents without core melt induceno off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering nor evacuation).*

*reducing, as far as reasonably achievable,*

*the core damage frequency taking into account all types of credible hazards and failures and credible combinations of events;*

***Accidents with core melt***

*reducing potential radioactive releases to the environment from accidents with core melt, also in the long term, by following the qualitative criteria below:*

*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 (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures.*

Compared to former designs, a clear stress is put on two main additional objectives that are: first to prevent core melt with a high confidence and, second, to be able to manage core melt situations in a way that guarantees limited radiological consequences. These two aspects are further developed in the paper.

**2.2. The defence in depth principle**

The defence in depth principle was defined in ref. [4] and the definition of defence in depth levels, as applicable to EPR design, are refined in ref. [3]. There are some differences between IAEA and WENRA definitions of the levels, mainly regarding whether complex sequences without core melt should be considered in level 3 (WENRA) or level 4 (IAEA). However, regardless of these differences, there are major convergences in the international safety approach based on the defence in depth principle and that can be summed up in the following way.

The main basis of nuclear safety are a robust design and a strict plant operation and maintenance; they ensure that normal operation can be carried out without any threat to the nuclear safety (level 1 of defence in depth). This aspect is not further developed in the paper.

Minor deviations from normal operation are corrected, in particular by limitation systems, without any radiological consequences too (level 2 of defence in depth). This aspect is not further developed in the paper.

Safety systems are designed to cope with single initiating events leading to accident conditions. (level 3 of defence in depth)

Multiple failure may affect safety systems, leading to complex accident conditions where core melt should be prevented (level of defence in depth 3b in WENRA or 4 in IAEA)

Regardless of the reliability of the means implemented to prevent core melt, situations with significant fuel degradation should be postulated and dedicated means be implemented to limit the radiological consequences (level 4 of defence in depth).

Independence should be provided between the features credited in each line of defence, as far as reasonably practicable.

The next parts of the paper describe how these principles are implemented in EPR design in order to reach the safety objectives mentioned in § 0.

**3. DESIGN BASIS CONDITIONS**

The aim of this part is not to describe in detail how design basis conditions are defined and addressed as this issue is not a major step forward in the design of new plants compared to Generation 2 NPPs, even though many improvements have been brought in both prevention and mitigation of accidents. In EPR design, "Design Basis Conditions" stand for both Anticipated Operational Occurrences (AOO) and Design Basis Accidents (DBA).

**3.1. Purpose of Design Basis Conditions (DBC)**

Design basis conditions aim at designing the safety systems that are able to compensate for disturbances in the control of the reactor main safety functions. For this purpose, envelope accident sequences are postulated on the basis of single initiating events that directly affect the control of the plant main parameters. Those accidents should be analysed with conservative methods and assumptions in order to bring safety margins in the design and

be able to cope with most of real accident situations that may be slightly different or more complex than the postulated ones.

### 3.2. Improvements in EPR design

The main improvements provided in EPR design regarding the DBC refer to:

- the consideration of shutdown modes as possible initial conditions for accident initiation;
- the consideration of accident situations occurring in the fuel storage pool.

Basically, power operation is the most usual operational mode of the plant and accident analyses address it in priority. However, operation feedback along the years has proved that shutdown modes also lead to specific threats, in particular when RCS or containment are open. In EPR, each plant mode is analysed in order to identify the specific risks and corresponding accident sequences are included in the DBC list. The same conservative analysis rules apply to the DBC initiated in shutdown modes.

The spent fuel pool has the potential to generate radiological releases. Therefore, DBC analysis should not be limited to the reactor itself and should include the risks specific to the pool and also the fuel handling operations. In EPR safety demonstration, accident sequences related to the spent fuel pool are included in the DBC list and conservative analysis rules are also applied. The transient families are mostly associated to the reduction of heat removal capability or uncontrolled pool level decrease.

## 4. DESIGN EXTENSION CONDITIONS: CORE MELT PREVENTION (DEC-A)

### 4.1. Purpose of DEC-A analysis

According to WENRA objective O2 (see § 0), it has to be demonstrated that the overall core damage frequency (CDF) is reduced *as far as reasonably achievable* and WENRA requires this demonstration to be primarily deterministic. From a design point of view, it means that the core damage frequency that can be associated to each Postulated Initiating Event (PIE) should be made low enough thanks to deterministic provisions. Based on former experience, the order of magnitude of an indicative core melt frequency target for a given PIE should be less than  $1\text{E-}7/\text{reactor year}$  in order to meet the generally approved target value of  $1\text{E-}5/\text{r.y}$  for the overall core melt frequency estimated in Level 1 Probabilistic Safety Assessment (PSA).

As the reliability of most active and passive safety systems credited in the DBC analysis is limited, such CDF target cannot be reached for the most frequent PIEs by just crediting the safety systems. Therefore, the aim of DEC-A analysis is to prove that, for any PIE, core melt can be prevented even in complex sequences where a complete failure of a DBC safety system is assumed. Such demonstration relies on diversified features that are able to control the safety functions when failure in safety systems is assumed. In such case, the combined reliability of the safety systems and the diversified systems allows to meet the probabilistic target.

At the design stage, detailed PSA results are not yet available, therefore such evaluation is performed based on decoupled approach. The principle is displayed in Fig. 1.

### 4.2. List of DEC-A

DEC-A analysis are required when there is a need to provide diversified means to control the fundamental safety functions during complex sequences and the efficiency of these means cannot be proved by mere engineering judgment. Two types of complex sequences are considered in the design:

- frequent DBC combined with a common cause failure (CCF) affecting a safety system (including its support systems);
- a common cause failure affecting a safety system used in normal operation (e.g. support systems).

Note that, at the basic design stage, the combination of independent initiating events or simultaneous failure of system without plausible common cause is not considered in the design because the associated frequencies are assumed to be low enough to reject such sequences into the residual risk. This assumption has to be later confirmed by Level 1 Internal Event PSA.

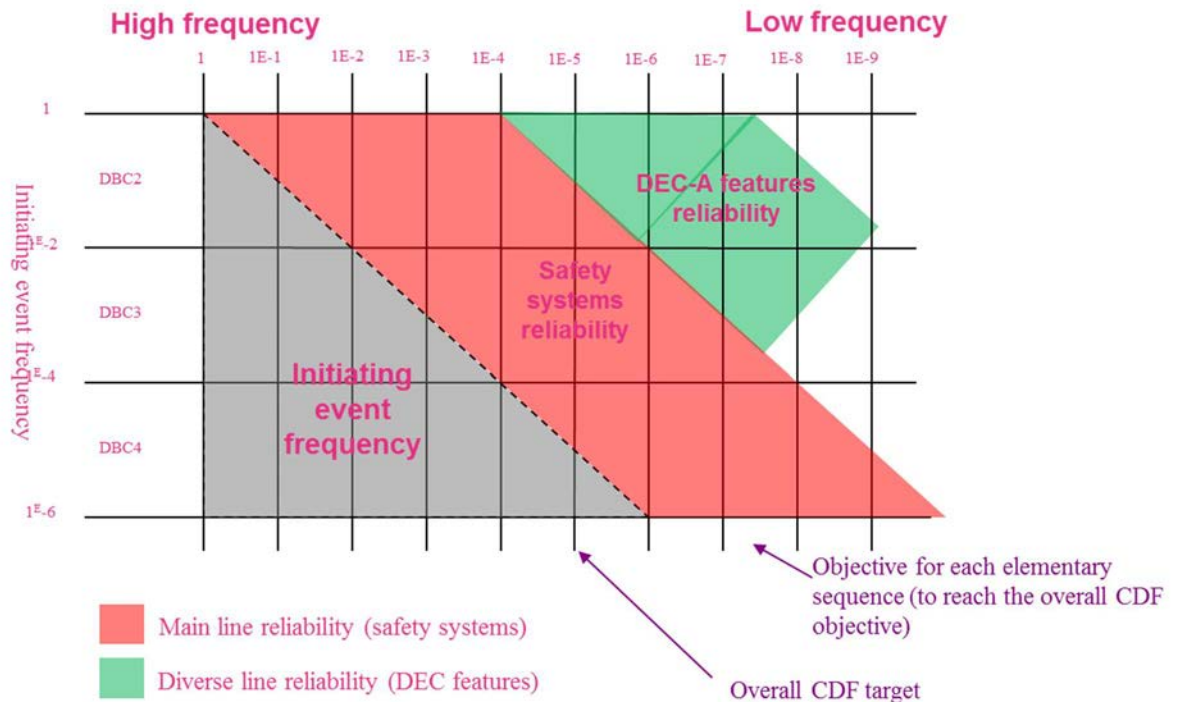


FIG. 1. Role of DEC-A features in the core melt prevention.

The diversity analysis consists in listing all the features credited in frequent DBC (including those used in normal operation, if any) and either postulating a complete failure of the feature by common cause or justifying that such common cause failure is not plausible (for instance because of intrinsic diversity). Then it is analysed whether a diverse mean should be implemented for this feature; there are several possible cases:

- in the frame of DEC-A analysis rules and criteria, the resulting complex sequence remains acceptable regarding the core melt prevention objective without any additional mean;

- the existing DBC features not affected by the common cause failure are able to compensate for the failure provided that they are sufficiently diversified from the feature that was postulated to fail, then no specific DEC-A feature is required;

- a specific reliable DEC-A feature diversified from the safety system that was postulated to fail is required to meet the safety objective.

Eventually the list of DEC-A is built by defining bounding sequences allowing to prove the efficiency of each identified diversified mean in the most challenging plausible complex sequence.

#### 4.3. Systems credited in DEC-A: independence between levels of defence in depth

The demonstration of DEC-A level independency would be straightforward if there were a whole set of diversified systems fully independent from the safety systems and that would be able to fully manage any DEC-A sequence. However, the demonstration is more complex as safety systems can still be credited in a DEC-A analysis because the simultaneous and complete failure of all the components contributing to the DBC line of defence is not plausible. Actually, each DEC-A sequence is characterized by an assumed CCF and any feature not affected by this CCF is considered to be still available. Then the analysis is performed based on both these features and, if necessary, additional DEC-A features that are neither affected by the CCF thanks to adequate diversity.

Eventually the adequate independence of the DEC-A line is proved sequence by sequence and it consists in proving that whatever plausible failure combination is assumed in DBC line, there is still sufficient means available in both the DBC and DEC-A lines to prevent core melt.

## 5. DESIGN EXTENSION CONDITIONS: CORE MELT MANAGEMENT (DEC-B)

### 5.1. Purpose and scope of DEC-B analysis

According to WENRA definition of the 4<sup>th</sup> level of defence in depth applicable in Western Europe (ref. [3]), core melt has to be postulated regardless of the effort made to prevent it in the previous levels of defence in depth. The consequence is that dedicated DEC-B features have to be designed in order to limit the consequences of the accident and fulfil the associated safety objectives (see § 0). The purpose of DEC-B analysis is to prove the appropriate design of DEC-B features.

This design is based on the identification of the main physical challenges for the containment integrity expected to occur during a core melt. A limited number of scenarios are defined in order to characterize each of these challenges and the specific DEC-B features are sized to cope with them.

### 5.2. Systems credited in DEC-B: independence between levels of defence in depth

Basically, only specific features dedicated to DEC-B are credited in DEC-B analysis. No credit can be taken from any system used in normal operation or any safety system (DBC), except some SSCs like the containment itself. Such rule provides assurance of the independence of the 4<sup>th</sup> level of defence compared to the first levels.

Some features may be credited in both DEC-A and DEC-B analysis provided that it does not jeopardize the safety objectives. In practice, it means that, when a DEC-B feature is used in DEC-A, it should be proved that the possible core melt sequence resulting from this DEC-A sequence combined with the failure of the feature, that may lead to unacceptable consequences, has a probability low enough to be rejected in the residual risk.

## 6. PRACTICAL ELIMINATION: A COMPLEMENT TO DEFENCE IN DEPTH CONCEPT

### 6.1. Purpose of practical elimination

According to defence in depth concept, dedicated DEC-B features are implemented in order to limit the consequences of fuel melt. If this last level of defence is correctly implemented, in addition to the prevention means implemented in the previous levels of defence, then it can be considered that the safety objectives are satisfactorily met and it is not necessary to proceed to further demonstration (in particular no requirement to postulate the loss of DEC-B features). Mitigation of fuel melt events mainly relies on the capability to perform efficiently the containment function and, on the contrary, it is impossible to fulfil the safety objectives in conditions where the control of this function is jeopardized, in particular if the containment building integrity is affected.

The aim of the practical elimination concept is to prove that severe accident situations where the containment function would be significantly jeopardized, leading to large or early releases, can "*be considered with a high level of confidence to be extremely unlikely to arise*" (ref. [5]). Note that a mere overshoot of DEC-B criteria is not considered to be necessarily a large or early release. Basically, a situation to be practically eliminated is associated to significant failure of the containment resulting from energetic phenomenon where the containment building would be damaged in a sudden and irreversible way. There are other kinds of containment failures that could also lead to large or early releases but they are either progressive or can be repaired. For these situations it can be considered that additional mitigating measures can be implemented (mostly based on mobile means), and so they are not considered in the practical elimination process.

Eventually the practical elimination process first consists in identifying the severe accident situations that can be associated to energetic phenomenon liable to challenge the containment integrity. Such phenomenon may occur after the fuel melt (such as hydrogen detonation) or before the fuel melt (prompt criticality during heterogeneous dilution). In addition, situations where the implementation of a containment function is not reasonably practicable are also identified and included in the practical elimination process as fuel melt occurring in these specific conditions may obviously lead to large releases (core melt in the spent fuel pool or core melt in the reactor while the containment is open).

## 6.2. Demonstration of practical elimination

Once the situations that have to be practically eliminated are listed, it is necessary to identify the plausible accident sequences that may lead to these specific fuel melt situations. The demonstration of practical elimination is based on the implementation of several independent lines of defence that prevent the energetic phenomena to occur. Demonstration is performed on a case by case basis, depending on the situation that has to be eliminated and the associated credible sequences. In any case, the reliability of the features that are implemented to achieve this demonstration should allow proving with a high confidence that the resulting core melt situation has a very low frequency.

## 7. CONCLUSION

EPR reactor fulfils stringent safety objectives aiming at preventing core melt and inducing no impact to the population and environment in case of accident conditions. In addition, though core melt frequency is very low and according to defence in depth principles, dedicated systems are implemented in order to manage those core melt situations that may occur and guarantee very limited radiological consequences. Eventually some very few situations can be conceived where radiological consequences would not be limited in case of core melt, because of significant failure of the containment due to very energetic phenomena; these situations are proved to be practically eliminated.

The combination of all these analyses provides an explicit demonstration of the fulfilment of defence in depth principles that proves the very high level of safety of EPR reactor.

## REFERENCES

- [1] Technical guidelines for the design and construction of the next generation of NPP with PWR Adopted during the GPR/German experts' plenary meetings held on October 19<sup>th</sup> and 26<sup>th</sup> 2000.
- [2] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, WENRA statement on safety objectives for new nuclear power plants, WENRA (2010).
- [3] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, RHWG report: Safety of new NPP design, WENRA (2013).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of nuclear power plant: design, IAEA- SSR-2/1 rev. 1, IAEA, Vienna (2016).





# SAFETY REINFORCEMENT OF OPERATING REACTORS

**Chairperson**

**K. ARAI**  
Japan



## **WENRA APPROACH WITH RESPECT TO DESIGN EXTENSION OF EXISTING REACTORS**

H. HIRSCH

Austrian Nuclear Advisory Board  
Neustadt a. Rbge., Germany  
Email: cervus@onlinehome.de

B. BECKER

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH  
Cologne, Germany

K. NÜNIGHOFF

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH  
Cologne, Germany

The authors are presenting this paper on behalf of WENRA-RHWG.

### **Abstract**

In 2014, the Western European Nuclear Regulators Association (WENRA) published a revised version of the Safety Reference Levels (RLs) for existing reactors developed by the Reactor Harmonisation Working Group (RHWG). The objective of the revision was to take into account lessons learned of the TEPCO Fukushima Dai-ichi accident.

A major update of the RLs was the revision of Issue F "Design Extension of Existing Reactors" introducing the concept of Design Extension Conditions (DEC).

The revised RLs clearly distinguish DEC not involving a severe accident (DEC-A) and involving a severe accident (DEC-B). They clarify how DEC are to be addressed in safety analysis and provide explicit goals of DEC analysis as well as attributes of the safety analysis of the selected DEC. They address adequate qualification and operability of (mobile) equipment used to manage DEC. The revised RLs also address sites where several reactors are collocated and emphasize the safety of spent fuel storage in DEC. They require independent and diverse heat removal means, one of them being effective after events involving natural hazards more severe than the one used for design basis, and address the availability of I&C, electric power and control room to manage DEC.

This conference contribution discusses WENRA's view on the DEC concept for existing reactors, including the selection process for the design extension conditions and the requirements for ensuring the safety functions, in particular with respect to heat removal and emergency power.

### **1. INTRODUCTION**

With the view to increase harmonization within the countries of the Western European Nuclear Regulators Association (WENRA), WENRA published in 2006 a set of Safety Reference Levels (RLs) for existing reactors. The RLs were updated in 2007 and 2008. The RLs are developed in consensus within the Reactor Harmonization Working Group (RHWG) and approved by the WENRA members. They reflect international safety standards and expected practices in the WENRA countries. It is expected that the RLs are transposed in national regulations and implemented in the nuclear power plants.

In 2014, WENRA published a revised version of the RLs, developed by RHWG [1]. The objective of the revision was to take into account the lessons learned of the TEPCO Fukushima Dai-ichi accident. For this purpose, RHWG reviewed the whole set of RLs, taking into consideration recommendations and suggestions published by ENSREG as a result of the complementary safety assessments ("stress tests") performed in Europe following the TEPCO Fukushima Dai-ichi accident as well as IAEA safety requirements being under updating at that time for the same reason and the conclusions of the 2nd Extraordinary Meeting of the Contracting Parties to the Convention on Nuclear Safety.

As a consequence, a new Issue (Issue T), dedicated to natural hazards, has been established. Issue E (Design Basis Envelope for Existing Reactors) and Issue F (Design Extensions Conditions of Existing Reactors) have been changed significantly. Furthermore, for approximately half of the remaining Issues, there have been limited changes.

The concept of design extension in Issue F has been enhanced and the term design extension conditions (DEC) has been introduced for consistency with the IAEA SSR-2/1 safety standard [2]. The revised Issue F clarifies how DEC to be addressed in safety analysis will be identified and defines explicit goals of DEC analysis as well as attributes of the safety analysis of the selected DEC. Furthermore, new expectations have been formulated for several specific points in Issue F.

In order to provide explanations of the intent of the RLs of Issue F, to contribute to a consistent interpretation and to permit insights into the considerations which have led to their formulation, RHWG developed a Guidance Document for Issue F which was also published by WENRA in 2014 [3].

The RL Issue F is divided in five sections. This division is reflected in the five parts of the following section of the paper.

## 2. MAIN INNOVATIONS IN THE 2014 VERSION OF ISSUE F OF THE WENRA RLS

### 2.1. Objective of Design Extension Conditions (DEC)

Occurrence of conditions more complex and/or more severe than those postulated as design basis accidents (DBA) could not be neglected in safety analysis. These conditions shall be investigated as Design Extension Conditions (DEC) so that any reasonably practicable measures to improve the safety of a plant are identified and implemented. Regarding the treatment of DBA and DEC, there are a number of clear and basic differences concerning the methodology of analysis; technical acceptance criteria and radioactive releases tolerated could also differ, depending on the category of DEC.

The RLs define two categories of DEC:

- DEC A for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved; and
- DEC B with postulated severe fuel damage.

Special efforts shall be implemented with the goal that a severe accident in a spent fuel storage becomes extremely unlikely with a high degree of confidence, since measures for sufficiently mitigating the consequences of a severe accident in spent fuel storages could be difficult to realize.

Extreme unlikelihood with a high degree of confidence is an element of the concept of “practical elimination”. The term “practical elimination” has not been used in the RLs. It is usually applied almost exclusively in the context of severe accidents leading to large or early releases. To demonstrate extreme unlikelihood with a high degree of confidence, probabilistic and deterministic elements both are required.

### 2.2. Selection of DEC

The RLs stipulate that a set of representative DEC shall be derived and justified based on a combination of deterministic and probabilistic assessments as well as engineering judgment. DEC are selected and analysed for the purpose of further improving the safety of the nuclear power plant.

The events which are considered in the selection of the representative DEC should cover a wide range of scenarios, from less demanding to more demanding.

A wide scope of events and combinations of events exceeding the design basis are to be considered at the beginning of the selection process for DEC A – those events, and combinations of events, which cannot be considered with a high degree of confidence to be extremely unlikely to occur, and which may lead to severe fuel damage.

Events occurring during the defined operational states of the plant shall be covered, including events resulting from internal and external hazards, and common cause failures. A non-exhaustive listing of initiating events for DEC A is provided in the Guidance Document for Issue F, including external hazards.

For DEC B, a set of representative severe fuel damage scenarios has to be identified, covering the different situations and conditions which can occur in the course of a severe accident. There will usually be a very large number of possible scenarios which cannot all be captured at the start of a selection process.

### 2.3. Safety analysis of DEC

The selected DEC are subject to DEC analysis. The purpose of this analysis can be

- (1) to review whether the fundamental safety functions can be guaranteed by existing equipment, or
- (2) to identify reasonably practicable measures for enhancing safety.

For (1), conservative or best estimate approaches may be used. In case of (2), best estimate methodology should be preferred to avoid missing reasonably practicable improvements due to an unduly conservative approach. In any case, uncertainties and their impacts have to be taken into account.

Within the analysis of DEC, cliff-edge effects should be identified and a sufficient margin to avoid such effects should be demonstrated wherever applicable. Different kinds of margins may have to be considered, depending on the nature of the DEC. For example, for multiple failure events, the margin could be seen as the capacity of required SSCs to achieve functional capability beyond their design basis, or as the number of additional failures for which it remains possible to avoid severe fuel damage. For certain multiple failures like total SBO, the margin could be expressed in terms of the period of time available for counter-measures. For events related to reactivity or loss of coolant, the margin could be expressed in terms of fuel temperature or enthalpy release. For external hazards within DEC, margins could be expressed in terms of frequency of severity.

When analysing a sequence in the framework of DEC, an end state should be defined and justified for the analysis. For DEC A, this defined end state could be a “safe state” according to IAEA SSR-2/1. In case of DEC B, it is unlikely to reach such a safe state and the defined end state could be a “controlled state after severe accident”. Such a state is characterized by ensured decay heat removal, stabilization of damaged fuel, prevention of re-criticality and confinement ensured to the extent that release of radionuclides is limited.

## **2.4. Ensuring safety functions in design extension conditions**

In DEC A, it is the objective that the plant shall be able to fulfil the fundamental safety functions (control of reactivity, removal of heat from core and spent fuel and confinement of radioactive material).

In DEC B, the objective is that the plant shall be able to fulfil confinement of radioactive material. The other fundamental safety functions are of importance insofar as they are required to support the confinement function. Severe accident management actions to prevent the irreversible loss of confinement which are leading to limited and controlled releases are not considered a loss of the confinement function if they are temporary, associated with specific predefined requirements (e.g. filtering of the releases) and do not lead to unacceptable off-site consequences.

SSCs used for DEC shall be adequately qualified to perform their functions for the appropriate period of time. Plant management under DEC may rely on mobile equipment. Permanent connecting points, accessible under DEC, shall be installed to enable the use of this equipment.

For multi-unit sites, a systematic process shall be used to review all units relying on common services and supplies, to ensure that common resources of personnel, equipment and materials expected to be used in accident conditions are effective and sufficient for each unit at all times.

The NPP shall be autonomous regarding supplies supporting safety functions, for a period of time until it can be demonstrated with confidence that adequate supplies can be established from off site. External hazards exceeding the design basis and related potential damage to infrastructure have to be taken into account.

### **2.4.1. Heat removal functions**

Regarding the removal of the residual heat from the core and the spent fuel, there shall be sufficient independent and diverse means available, including necessary power supplies. At least one of these means shall be effective after events involving external hazards more severe than design basis events.

Either an alternative ultimate heat sink (including a complete chain of systems providing a link to it) or a chain of independent and diverse systems for using the primary ultimate heat sink (if the primary ultimate heat sink is available for all events within the DEC involving external hazards) should be in place. If there is an alternative ultimate heat sink, it should be independent as far as practicable from the primary ultimate heat sink.

The alternative ultimate heat sink or the chain of diverse systems should be able to secure the cooling of core and spent fuel for an extended period of time.

#### 2.4.2. *Confinement functions*

The reference levels on confinement should also be applied to the spent fuel storages, in case severe spent fuel damage has not been demonstrated to be extremely unlikely with a high degree of confidence.

Isolation of the containment shall be possible in DEC. For the shutdown states, special attention needs to be given to situations with an open containment. In this case, timely containment isolation should be guaranteed, or measures to prevent core damage with a high degree of confidence made available. Also, in case of events leading to containment bypass, severe core damage shall be prevented with a high degree of confidence.

The previous version of the RLs already contained the expectations, in Issue F, that pressure and temperature as well as the threats due to combustible gases shall be managed, that containment shall be protected from overpressure, that high pressure core melt scenarios shall be prevented and containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.

A new expectation states that if venting is to be used for managing containment pressure, adequate filtration shall be provided. For multi-unit sites, conditions at other units should be taken into account.

Finally, for the confinement functions, a new RL has been introduced stipulating that in DEC A, releases shall be minimised as far as reasonably practicable. In case of DEC B, any release to the environment shall be limited in time and magnitude as far as reasonably practicable in order to allow sufficient time for protective actions in the vicinity of the plant and to avoid long-term contamination of large areas. These radiological objectives are in line with principles 1 and 2 of the Vienna Declaration on Nuclear Safety [4].

The delay of releases in DEC B can also be important for the implementation of additional measures in the plant (or neighbouring units) to delay releases further or to prevent them altogether.

#### 2.4.3. *Instrumentation and control for the management of DEC*

New expectations concern adequately qualified instrumentation which shall be available for DEC for determining the status of the plant (including spent fuel storage) and safety functions as far as required for making decisions (on-site as well as, in case of DEC B, off-site).

The instrumentation should be able to perform its safety-related functions in DEC environmental conditions. Instrumentation for key parameters should also be able to perform its function for a sufficient period of time in case of total SBO.

An operational and habitable control room (or another suitably equipped location) shall be available during DEC. The other suitably equipped location could be a supplementary control room or a local control panel, if they are adequately equipped and protected.

#### 2.4.4. *Emergency power*

This new section of Issue F stipulates that adequate power supplies during DEC shall be ensured to support the fundamental safety functions. The timeframes defined in the DEC analysis have to be considered and external hazards taken into account.

Furthermore, DC power supply shall be provided with adequate capacity until recharging of batteries can be established or other means are in place.

### 2.5. **Review of the design extension conditions**

Regular assessment of the overall safety of an NPP is required in the Issue “Safety Policy”, in the (new) RL A2.3. A new RL in Issue F emphasizes that this regular assessment has to include the design extension conditions. Furthermore, the design extension conditions shall be reviewed, when relevant, as a result of operating experience and significant new safety information.

The review shall use both a deterministic and a probabilistic approach as well as engineering judgment to determine whether the selection of design extension conditions is still appropriate. Based on the results, needs and opportunities for improvements shall be identified and relevant measures shall be implemented. In accordance with RL A2.3, reasonably practicable measures for improvement which have been identified shall be implemented in a timely manner.

### 3. CONCLUDING REMARKS

WENRA is committed to the improvement of nuclear safety. Bearing this in mind, the WENRA Safety Reference Levels have been significantly updated and expanded taking into account the lessons learned from the TEPCO Fukushima Dai-ichi accident, with the purpose of further improving the safety of nuclear power plants.

Issue F of the RLs (Design Extension of Existing Reactors) is of high importance in this context. Safety considerations for existing reactors need to reach beyond the limitations of the initial design basis, in every respect, including for external hazards.

Furthermore, Issue F emphasizes that the regular assessment of the overall safety of a nuclear power plant, as required in RL A2.3, has to include the design extension conditions. Reasonably practicable measures for improvement which have been identified shall be implemented in a timely manner, in accordance with RL A2.3. The main criterion for the implementation of improvements is reasonable practicability. What is reasonably practicable may change over time. Hence, there also is the need for a regular review of DEC.

Finally, it should be noted that there are significant interactions between some of the Issues of the RLs. Hence, each Issue should not necessarily be considered as self-standing. The RLs need to be considered as a whole set. In particular, the connections between Issue F and Issues E (Design Basis Envelope for Existing Reactors) and T (Natural Hazards) need to be taken into account.

### REFERENCES

- [1] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, WENRA Safety Reference Levels for Existing Reactors – update in relation to lessons learned from TEPCO Fukushima Dai-Ichi Accident, Report, 24 September 2014.
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards, Specific Safety Requirements, SSR-2/1 (Rev. 1, 2016), IAEA, Vienna (2012).
- [3] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, WENRA-RHWG, Issue F: Design Extension of Existing Reactors – Guidance for the WENRA Safety Reference Levels for existing Reactors in their update in relation to lessons learned from the TEPCO Fukushima Dai-Ichi Accident, Guidance Document, 29 September 2014.
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna Declaration on Nuclear Safety, INFCIRC/872, IAEA, Vienna (2015).



# **SAFETY PRINCIPLES AND DEFENCE-IN-DEPTH CONCEPT IMPLEMENTED IN GERMAN REGULATIONS**

## ***Fulfilling the Vienna Declaration for existing reactors***

K. NÜNIGHOFF

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH  
Cologne, Germany  
Email: kay.nuenighoff@grs.de

B. BECKER

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH  
Cologne, Germany

S. EISMAR

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH  
Cologne, Germany

### **Abstract**

In 2012 the German regulator published the new safety requirements for NPPs. These requirements were developed over a period of 10 years taking into account the latest developments in nuclear safety. In Germany, nuclear safety has to meet the state-of-the-art in science and technology. Consequently, also the German regulations have to reflect the most recent international developments in nuclear safety. The IAEA Safety Standards, primarily SSR 2/1 “Safety of Nuclear Power Plants: Design”, have been consulted as a source of global consensus in nuclear safety. Furthermore, the WENRA safety objectives for new reactors representing a harmonized view of the European regulators were taken into account. Despite the fact that the construction of new NPPs is prohibited by law, the main safety objectives for new reactors were adopted for a set of requirements for existing NPPs. The paper presents how the defence-in-depth concept is implemented in the German Safety requirements. A comparison with the defence-in-depth concept described in SSR 2/1 and the accompanying IAEA TECDOC-1791 as well as with the defence-in-depth concept described in the WENRA Safety Objectives for New NPP designs is discussed. Furthermore, the paper addresses the question how independence between different levels of defence-in-depth has to be ensured. Finally, the implementation of the practical elimination of large and early releases in the context of existing German reactors is discussed. This objective has to be demonstrated by the interaction of reliable safety systems and additional on-site accident measures. For example, requirements for connection of mobile equipment to prevent core melt accidents have been added in the German regulations in the aftermath of the accident at the Fukushima Daiichi NPP. The conclusion will demonstrate that the German approach meets the objectives of the Vienna Declaration.

## **1. INTRODUCTION**

Continuously improving nuclear safety is a global challenge. In 2015, the Vienna Declaration on Nuclear Safety [1] was adopted by the Contracting Parties to the Convention on Nuclear Safety (CNS) at the Diplomatic Conference. In the Vienna Declaration the first time all Contracting Parties to the Convention on Nuclear Safety (CNS) have agreed on three principles to prevent accidents with radiological consequences and mitigate such consequences should they occur by. Principles 1 requires that for new nuclear power plants accidents with radioactive releases will neither cause long-term off site contamination nor long term protective measures and actions. Principle 2 requires the application of the above mentioned principle for existing facilities and the periodic and regular safety review. Principle 3 requires taking into account IAEA Safety Standards and other good practices while drafting or revising national regulations.

In Germany, nuclear safety has legally mandatory to follow the state of the art in science and technology. Therefore, the licences continuously improve nuclear safety at their NPPs and the German regulator regularly revises its regulations. National nuclear regulations in Germany have been constantly developed and adapted to the progressing state of the art in science and technology since the 1970s years.

## 2. REGULATORY FRAMEWORK IN GERMANY

The German legislation defines in the §7 of the Atomic Energy Act (AtG) [2] the prerequisites for granting a license to construct and operate a nuclear facility for the production, treatment, processing or fission of nuclear fuel. Amongst others, the licensee has to take the necessary precautions against damage in the light of the state of the art in science and technology in the field of nuclear safety. The German regulatory body has to consider the state of the art in science and technology in its regulatory decision making in licensing and oversight processes. Therefore, it is mandatory for the German regulator to continuously monitor the state of the art in science and technology. As nuclear safety is characterized by global developments rather than national insights the state of the art in science and technology has to be determined on an international level.

Whereas the generally binding part of the regulatory framework contains high level requirements, these are further concretized in the non-binding part, which becomes binding by either specifications in the licence or by supervisory measures. In Germany, the state of the art in science and technology is *inter alia* defined in the Safety Requirements for Nuclear Power Plants [3].

## 3. GERMAN DEFENCE IN DEPTH CONCEPT

Internationally, the defence in depth concept consists of five subsequent levels [4-8]. The Safety Requirements for existing nuclear power plants published in 2013 define a sophisticated defence in depth concept for German NPPs. It is characterized by the first four levels of defence in depth:

- Level 1: normal operation;
- Level 2: abnormal operation;
- Level 3: design basis accidents;
- Level 4: design extension conditions;
  - Level 4a: ATWS;
  - Level 4b: multiple failure of safety system;
  - Level 4c: accidents with severe fuel assembly damages.

These four levels of defence in depth fall into the responsibility of the operating organization. Level 5 is not explicitly addressed in the safety requirements because it mainly comprises the off-site emergency preparedness and response, where the licensee plays a minor role.

Intentionally, the German defence in depth concept has a strong preventive character. In Germany, prevention is understood as the collection of all designed safety features and measures of the plant internal accident management to prevent the occurrence of severe accidents in the reactor or spent fuel pool. Mitigation has the objective to minimize radiological releases in case of severe accidents.

As the existing German nuclear power plants are not designed to withstand accidents with severe fuel damage the priority is to prevent such accidents. The main idea is to stop an event escalation by high reliable safety systems on third level of defence. Avoidance of AOOs or DBA by applying conservative design principles contributes to the preventive character of the German defence in depth concept. Items important to safety have to be designed according to the following principles defined in the German Safety Requirements for NPPs [3]: *inter alia* applying well-founded safety factors, preference to inherently safe-acting mechanisms, use of qualified materials, quality assurance during manufacturing, construction and operation, execution of regular in-service inspections, reliable monitoring of operating states and operational modes, monitoring concept to detect operation and ageing induced damage. Furthermore, it is required to take operational experience into account.

For safety systems (level 3 of defence in depth) additional more stringent requirements have to be fulfilled: redundancy, diversity, functional and spatial separation, fail-safe principle, preference to passive equipment. Also auxiliary and support systems have to be designed with such reliability, that reliability of the safety systems will not be compromised. By these design principles, the frequency for events exceeding the design basis accidents will be reduced.

For accident conditions more severe than design basis accidents, i.e. design extension conditions, measures on level 4 of defence in depth have to be provided. In Germany level 4 is split into three sublevels. Transients with postulated failure of the fast reactor shutdown system (ATWS) are assigned to level 4a. Here, the same design principles as for levels 1 and 2 (see above) have to be applied. Accidents with postulated multiple failures of safety systems belong to level 4b. Both levels belong to the preventive domain, but with graded requirements to be

applied for measures and equipment on level 4b. The objective is to avoid an escalation to severe accidents by using dedicated measures and equipment. On level 4c measures are foreseen to cope with phenomena expected during severe accidents. These measures belong to the mitigatory domain. The main safety goal of level 4c of defence in depth is to ensure integrity of the containment as the last barriers as long as possible.

In the following, the integration of radiological safety objectives, independence, barrier concept and the single failure concept as well as the protection concept against internal and external hazards are discussed.

### 3.1. Radiological safety objective

In § 1 no. 2 AtG it is mandatorily required to protect life, health and real assets against the hazards of nuclear energy and the harmful effects of ionising radiation. This high level requirement is further specified in the radiation protection ordinance [9]. An effective dose limit of 20 mSv for workers must not be exceeded on levels of defence 1 and 2. For the public an effective dose limit of 1 mSv must not be exceeded. Contribution from effluents and airborne releases shall not exceed 0.3 mSv. For accidents (DBA) on level of defence 3 it has to be demonstrated that planning level of 50 mSv effective dose will not be exceeded. In all cases the ALARA principle has to be applied to minimize the potential doses. For events on level of defence 4 no limits or reference levels are prescribed in German regulations. For level of defence 4a the German Safety Requirement for Nuclear Power Plants [3] require that the on-site and off-site radiological consequences shall be kept as low as possible, taking into account all circumstances of each individual case.

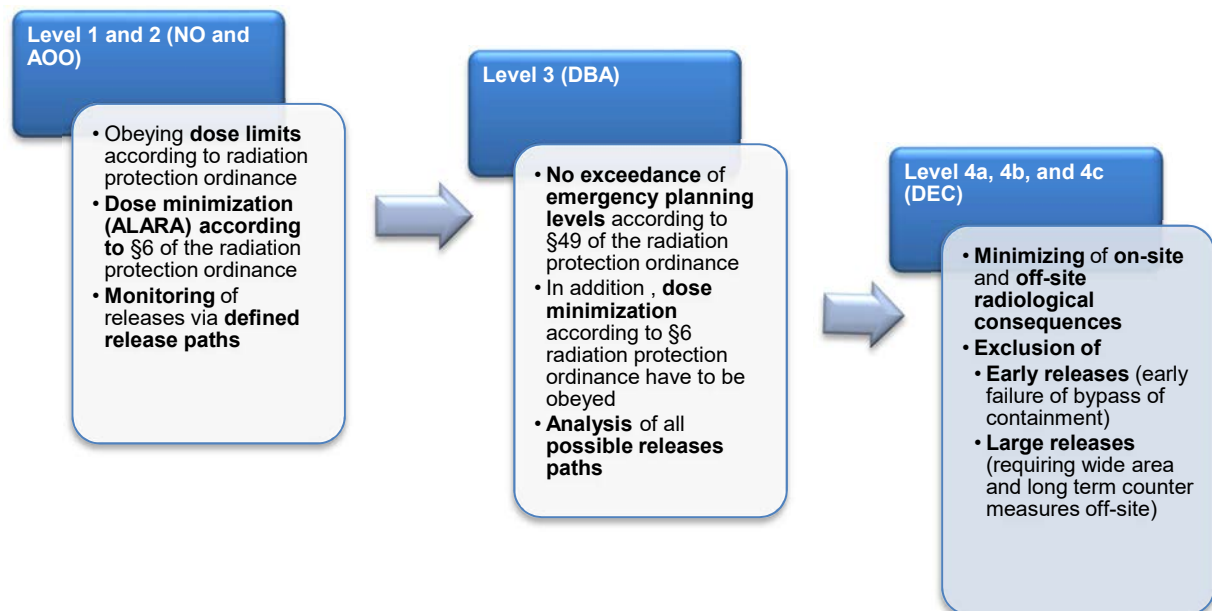


FIG. 1. Radiological safety objectives on different levels of defence in depth in Germany.

On level of defence 4b and 4c the Safety Requirements for Nuclear Power Plants [3] require either exclusion of any releases of radioactive materials caused by the early failure of the containment or any releases of radioactive materials requiring wide-area and long-lasting measures of off-site emergency preparedness or limitation of radiological consequences to such an extent that off-site emergency preparedness measures will only be required to a limited spatial and temporal extent. This radiological safety objective is in line with the expectation of principle 1 of the Vienna Declaration on Nuclear Safety [1]. It also implements the radiological objective required in IAEA Safety Standard Series No SSR 2/1 [5] to practically eliminate those plant states leading to large or early releases. The German requirement also meets the expectations expressed in the WENRA Safety objectives for new NPP designs [7] and the recently published WENRA Safety Reference Level for existing nuclear power plants [8] regarding the practical elimination of large and early releases. Fig. 1 illustrates the radiological safety objectives within the German defence in depth concept.

### 3.2. Independence

Independence of the various levels of defence in depth is an important key factor to ensure nuclear safety and to prevent the simultaneous loss of several safety features. As German NPPs have been designed and constructed in the 1970s and 1980 years, modern defence in depth concepts were not considered in the original design. One consequence is that e.g. the emergency core cooling system fulfils a safety function on level 3 of defence in depth but also operational decay heat removal in operational states (reactor shutdown) on level of defence 1. This problem of independence is addressed in German regulations twofold. First, independence between levels 1 and 2 from levels 2 and 3 is required. In addition, independence between level 4 of defence in depth and the previous levels is required. Second, in such cases, where items important to safety have to be effective on several levels of defence in depth, the design has to meet the most stringent safety requirements. In the example above, the emergency core cooling system has to meet the design principles and requirements for safety systems on level of defence 3. Crediting equipment on levels of defence 2 and 3 to control incidents on previous levels of defence in depth is only permitted if neither other technical solutions can reasonably be achieved nor negative effects on the reliability and effectiveness of the measures and equipment used for the control of events need to be assumed.

### 3.3. Barrier concept

TABLE 1. REQUIRED BARRIERS ON DIFFERENT LEVELS OF DEFENCE IN DEPTH FOR FUEL IN THE CORE AND STORED IN THE SPENT FUEL POOL

	Fuel in the core	Spent fuel pool
Level 1	Fuel cladding Pressure retaining wall	Fuel cladding
Level 2	Containment	Containment / compensating retention function
Level 3	Fuel cladding Pressure retaining wall Containment	Fuel cladding Containment / compensating retention function
Level 4a	Fuel cladding Pressure retaining wall containment	
Level 4b	At least on barrier	
Level 4c	Maintaining the integrity of the containment as long as possible	
	In case of fuel elements stored outside a containment: Maintaining the integrity of the surrounding building as long as possible	

The German Safety Requirements [3] require a concept of three barriers to prevent releases of radioactive materials to the environment. Dedicated requirements for the barriers are assigned to the different levels of defence in depth. According to German regulations, only gastight metallic barriers can be credited as a barrier, i.e. the fuel cladding, the pressure retaining wall and the containment. Other structures, like fuel pellet, coolant or biological shield are considered having a retention function, but cannot be credited as a barrier. Tab. 1 summarizes the requirements on barriers for the different levels of defence in depth.

On levels 1 and 2 of defence in depth integrity of all three barriers have to be ensured at all times for the fuel in the reactor core. For fuel stored in the spent fuel pool, the pressure retaining wall is missing and not requested. In principle for design basis accidents again all three barriers have to be in place, except the failure of the barrier is the postulated initiating event itself. For loss of coolant accidents, additional acceptance targets are in place for the number of failed fuel rods, depending on the break size. On level 4a of defence in depth, i.e. ATWS, integrity of all three barriers has to be ensured. By measures of preventive accident management the integrity of at least one barrier has to be ensured for multiple failure events. The main goal in case of severe accidents is to maintain the integrity of the containment as the last barrier as long as possible. For spent fuel pools outside of the containment, the integrity of the reactor building has to be ensured.

### 3.4. Single failure concept

The single failure concept as deterministic approach to ensure reliability of items important to safety is fully integrated into the German defence in depth concept. From a safety point of view no redundancy is required for operational systems on levels 1 and 2 of defence in depth (n+0). Exceptionally, for limitation systems to control anticipated operational occurrence a degree of redundancy of (n+1) is required. For safety systems in general a degree of redundancy of (n+2) is required considering a single failure and a maintenance case when demanding the safety systems. On levels of defence 4 no redundancy is required (n+0).

In addition, detailed requirements and boundary conditions (e.g. repair times, simultaneous maintenance of several trains of a safety system, or exception for containment isolation, etc.) are provided in an Annex to the Safety Requirements for Nuclear Power Plants [3]. Again, links to the different levels of defence are established.

### 3.5. Protection concept against internal and external hazards

In the German Safety Requirements for Nuclear Power Plants [3] a protection concept against internal and external hazards has been introduced based on the lessons learned from the accident at the Fukushima Dai-ichi NPP. It was decided, that hazards are no longer considered as postulated initiating event (in an early draft hazards have been assigned to level 4a of defence in depth). German regulations distinguish between internal hazards, natural hazards, and human induced hazards.

For internal hazards it is required, that only the affected redundancy is allowed to fail. This leads to the requirement, that spreading of an internal hazard leading to a failure of more than one redundancy has to be prevented.

For natural hazards, requirements are more stringent. The plant has to be protected in such a way, that no redundancy of safety systems will be affected by a natural hazard up to the design basis.




For human induced hazards it is required, that at least the needed capacity of trains to fulfil the demanded safety function has to be available.

## 4. COMPARISON OF GERMAN DEFENCE IN DEPTH CONCEPT WITH INTERNATIONAL RECOMMENDATIONS

The German defence in depth concept is in line with international recommendations from IAEA [5-6] and WENRA [7-8]. As can be seen in Fig. 2 the German defence in depth concept is in conformance with the recommendation of WENRA / RHWG for existing NPPs [8]. In principle, it is also in line with the defence in depth concept proposed for new NPPs recommended by WENRA / RHWG [7] or IAEA [5-6], except that for more severe events than DBA no design features are installed but control of such situations relies on accident management measures.

It has to be emphasised, that in Germany level 4 of defence in depth is not part of the original plant design, but the same radiological safety objectives as for new NPPs are required (see discussion in section 3). A particularity of the German defence in depth concept is the splitting of the design extension regime without significant fuel degradation into sublevels 4a and 4b. Sublevel 4a is reserved for transients with postulated failure of the fast shutdown system (ATWS). The main safety feature to control ATWS is the inherent design of the reactor. By negative reactivity coefficients it is ensured that an increase in reactivity, leading to a power increase of the reactor and heat up of the fuel, will stop the nuclear chain reaction. This is typically demonstrated by

dynamic coupled neutronic thermal hydraulic simulations of the postulated initiating events. Postulated accidents with multiple failures of safety systems are assigned to sublevel 4b. Such situations have to be controlled by measures of the plant internal accident management of the preventive regime. For severe accidents mitigative measures of the plant internal accident management have to be provided on level 4c of defence in depth. For both sublevels 4b and 4c requirements concerning the safety demonstration and expected reliability are established in the German Safety Requirements for Nuclear Power Plants [3]. It is emphasized, that in case of a real severe accidents the accident management programme allows to use every available system, independent of its assignment to any level of defence in depth either to prevent a severe accident or to mitigate the consequences of a severe accident.

Plant states						
Level	existing NPP			new NPP		
1	Normal operation		Normal operation	Normal operation		Normal operation
2	Abnormal operation		AOO	AOO		AOO
3	Accidents (DBA)		DBA	3a	Postulated singel initiating events	DBA
4	4a	Very rare events	DEC without core melt	3b	Postulated multiple failure events	DEC without significant fuel degradation
	4b	Events involving multiple failure of safety equipment				
	4c	Accidents involving severe fuel assembly damages	DEC with core melt	4	Postulated core melt accidents	DEC with core melt
5	Off-site emergency response					

FIG. 2. Comparison German defence in depth concept with IAEA and WENRA approaches.

## 5. GERMAN APPROACH TO PRACTICAL ELIMINATION OF LARGE OR EARLY RELEASES IN EXISTING NPPS

German NPPs in operation have been designed according to safety standards of the 1970s and 1980s. At that time no design provisions to cope with severe accidents were required. Consequently, the existing plants are designed to cope with traditional design basis accidents only. The practical elimination of events leading to early or large releases at German NPPs is demonstrated by the interaction of plant operation, high reliability of the safety system and a comprehensive accident management. It can be illustrated by five tiers.

The first tier forms the design of systems, structures and components of high reliability and quality. One example is the application of the concept of basic safety developed in the late 1970s years to prevent catastrophic failure of those components. It is characterised by the following principles: safety high-quality materials, especially with respect to fracture toughness, conservative stress limits, avoidance of peak stresses by optimisation of the design, ensuring application of optimised manufacturing and test technologies, knowledge and evaluation of existing flaws and accounting for the operating medium. Later on this concept was developed further to the integrity concept. Until now, the integrity concept has been proven in practice and presents an important contribution in terms of damage precaution. The technical basis for it is nuclear safety standard KTA 3206 “Verification Analysis for Rupture Preclusion for Pressure Retaining Components in Nuclear Power Plants” [10].

By thorough application of these deterministic approaches, the frequency of e.g. loss of coolant accidents could be reduced.

The third tier is represented by the measures of the preventive plant internal accident management. The licence has to retain pre-planned measures to re-establish the fundamental safety functions. The effectiveness of these measures has to be demonstrated by safety analyses. For such safety analyses realistic models and boundary conditions can be applied.

Mitigative plant internal accident management can be considered as the fourth tier to achieve practical elimination of large and early releases. Again, the effectiveness of these measures has to be demonstrated by safety analyses applying realistic models and boundary conditions;

The above mentioned four tiers are based on deterministic approaches. Complementary probabilistic safety analysis (PSA) can be considered as the fifth tier. By PSA level 1 and PSA level 2 the achievement of practical elimination can be substantiated. It can be demonstrated, that the implemented design features, periodic testing and in-service inspections, together with preventive and mitigative measures of the plant internal accident management will lead to very low values of large early release frequencies (LERF). It has to be stated, that Germany has no quantitative target values, but it is considered to be sufficient that those sequences leading to large or early releases will have a low frequency compared to other accident sequences.

## 6. VIENNA DECLARATION

The Vienna Declaration on Nuclear Safety defines three principles [1]. An in-depth discussion of this topic can be found in the seventh National Report under the Convention on Nuclear Safety [11]. This section summarizes how Germany complies with all of the three principles.

### 6.1. Principle 1

§ 7 para. 1 AtG prohibits issuing construction as well as operating licences for new NPPs for electricity production. Thus, no rules for new nuclear installations in terms of Principle 1 of the “Vienna Declaration on Nuclear Safety” are necessary to be implemented in Germany’s nuclear regulations.

Principle 1 fosters the implementation of defence in depth by preventing accidents and, should an accident occur, mitigate the radiological releases in such a way, that long term protective actions are not necessary. Despite Germany’s decision to phase out from nuclear energy, both aspects have been transferred to the German regulatory framework applicable for existing nuclear power plants. The radiological objective to practically eliminate large and early releases is required by the German Safety Requirements for Nuclear Power Plants [3]. To achieve this demanding objective, a sophisticated defence in depth concept has to be and is applied by the existing German NPPs.

### 6.2. Principle 2

Since 2002, § 19a para. 1 AtG [2] requires ten-yearly safety reviews of nuclear installations in power operation. For nuclear installations in transition from power operation to post-operation, a safety status analyses to be prepared on the basis of the “Check list for the performance of an assessment of the current safety status of the installation for the post-operational phase” [12] was made mandatory. The periodic safety review represents a supplement to the continual review within the framework of nuclear supervision in Germany. The results are presented by the licence holders to the respective competent nuclear licensing and supervisory authorities of the federal state. The results are assessed by independent authorised expert organisations on behalf of the licensing and supervisory authority. A final assessment is made by the competent nuclear authority. An implementation plan (including a time schedule) to improve nuclear safety has to be proposed by the licensee and need to be agreed by the responsible licensing and supervisory authority.

By the mandatory periodic safety reviews Germany meets principle 2 of the Vienna Declaration on Nuclear Safety. While reviewing the NPP and assessing nuclear safety against the most recent state of the art in science and technology possible safety improvements will be identified and implemented. It can be concluded, that periodic safety review is an effective instrument to improve nuclear safety.

Independently of the periodic safety review, many backfittings have been performed at German pressurized water reactors (PWR) and boiling water reactors (BWR). Especially in the late 1980s years many accident management measures have been implemented.

### 6.3. Principle 3

The national nuclear regulations in Germany have constantly been developed and adapted to the progressing state of the art in science and technology since the 1970s. When developing new regulations or revising existing ones, the determination of the current state of the art in science and technology is mandatory by law. Amongst other sources, the IAEA safety standards are an important source of information and are regularly taken into account. For recently published IAEA Safety Standards, a gap analysis is performed to identify possibilities to further improve German regulations if deemed necessary.

## ACKNOWLEDGEMENTS

The work presented in this article is supported by the Project 3616R01560 “Ermittlung des Internationalen Standes von Wissenschaft und Technik auf dem Gebiet der kerntechnischen Sicherheit und dessen nationale Umsetzung” funded by the German Ministry of Environment, Nature Conservation, Building and Reactor Safety.

## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna Declaration on Nuclear Safety, INFCIRC/872, IAEA, Vienna (2015).
- [2] Atomic Energy Act (AtG), published in Bundesgesetzblatt (Federal Law Gazette, BGBl.) I 1985, No. 41, with last amendment in Bundesgesetzblatt I 2016, No. 37, and a correction in Bundesgesetzblatt I 2016, No. 61.
- [3] “Safety Requirements for Nuclear Power Plants”, Sicherheitsanforderungen an Kernkraftwerke in der Fassung der Bekanntmachung vom 3. März 2015, BAnz AT 30.03.2015 B2.
- [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, Safety Standard Series No. SSR 2/1 “Safety of Nuclear Power Plants: Design”, Rev. 1, IAEA, Vienna (2016).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, “Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants”, IAEA-TECDOC-1791, IAEA, Vienna (2016).
- [7] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, “Safety of new NPP designs”, Study by Reactor Harmonization Working Group (RHWG), WENRA (2013).
- [8] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, “WENRA Safety Reference Levels for Existing Reactors”, WENRA (2014).
- [9] Radiation Protection Ordinance, published in Bundesgesetzblatt (Federal Law Gazette, BGBl.) I 2002, Nr. 27, S. 1459.
- [10] KTA, “Verification Analysis for Rupture Preclusion for Pressure Retaining Components in Nuclear Power Plants”, KTA 3206, November 2014.
- [11] FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURE CONSERVATION, BUILDING AND NUCLEAR SAFETY, “CNS, Report by the Government of the Federal Republic of Germany for the Seventh Review Meeting in March/April 2017”, 22 June 2014.
- [12] FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURE CONSERVATION, BUILDING AND NUCLEAR SAFETY “Merkpostenliste für die Durchführung einer Bewertung des aktuellen Sicherheitsstatus der Anlage für die Nachbetriebsphase“, 2 October 2014.



# **REVIEW OF THE UPGRADED SEVERE ACCIDENT MITIGATION STRATEGIES FOR THE GENERATION II PWRs IN FRANCE FORESEEN IN THE FRAMEWORK OF PLANT LIFE EXTENSION**

R. COZERET  
IRSN  
Fontenay-aux-Roses, France  
Email: romain.cozeret@irsn.fr

C. DEBAUDRINGHIEN, G. CENERINO, E. RAIMOND  
IRSN  
Fontenay-aux-Roses, France

## **Abstract**

In France, EDF is developing a Plant Life Extension (PLE) program for the Gen II PWRs, which both takes into account the lessons of the Fukushima Dai-ichi accident and aims at reducing the gaps in terms of safety with the Gen III EPR, as requested by the French Safety Authority ASN. This program is progressively reviewed by IRSN for the ASN. The paper presents some intermediate statements of this review for the upgraded strategies proposed by EDF in order to reduce the consequences of a severe accident on a Gen II PWR. It gives some comparisons with the Flamanville 3 EPR.

## **1. INTRODUCTION**

The French electrical utility EDF is currently operating a fleet of 58 Gen II Pressurized Water Reactors (PWRs) (900, 1300 and 1450 MWe series) built between 1977 and 1999. Periodic Safety Reviews (PSRs) are conducted every 10 years. These reactors were not designed to face a core melt accident and several plants reinforcements have been discussed in France and progressively implemented by EDF to allow for the management of severe accidents.

In 2009, EDF presented to the French Safety Authority (ASN) a Plant Life Extension (PLE) program, in order to give a possibility to extend the Gen II PWRs operation duration beyond 40 years. It included an ageing program but also some reinforcements to reduce the gap with the safety objectives of the new nuclear power plants like the Gen III EPR. This program has been reviewed by IRSN for ASN in parallel with the Complementary Safety Assessments (CSA) after the Fukushima Dai-ichi accident.

Today, the PLE and the CSA programs are combined in a vast industrial project by EDF with also some important efforts from IRSN and ASN to review the different steps of the project until final implementation.

The paper summarizes some of IRSN statements after the review of the EDF upgraded severe accident mitigation strategies for the generation II PWRs (firstly 900 MWe series) foreseen in France in the frame of PLE and CSA. This review has been presented in July 2016 to the French Advisory Committee for Nuclear Reactor Safety and ASN.

## **2. FRENCH GEN II PWRs BACKFITTING FOR SEVERE ACCIDENT**

Before presenting the future PWRs safety reinforcements for severe accident, it is important to remind some NPPs upgrades that are or are being implemented on the French Gen II reactors [1]:

- Development and update of severe accident management guidelines;
- Installation of an Emergency Filtered Containment Venting System (EFCVS), with some specific procedures which can differ from one reactor to the other;
- Installation of Passive Autocatalytic Recombiners (PARs);
- Reinforcement of the closure system of material access penetration for the 900 MWe PWRs reactor building (above the design pressure);
- Reactor cavity reinforcement (basemat width and corium spreading area) for Fessenheim NPPs;
- Instrumentation to detect hydrogen in the reactor containment;
- Instrumentation to detect a vessel failure;
- Modification of the pressurizer safety valves (reliability in case of station black out);

- Reinforcement of electrical supply of the containment isolation system and optimization of procedures for the manual actions;
- Reinforcement of the ventilation system of the secondary reactor building for the 1300 and 1450 MWe PWRs;
- Re-injection of contaminated water from auxiliary buildings (in case of leakage on sump recirculation circuits) to the reactor building (for 1300 MWe PWRs).

All these backfittings have been decided and designed based on the knowledge obtained from research on severe accident and learnings obtained from deterministic safety studies or Level 2 Probabilistic Safety Assessment (L2 PSA) studies.

In parallel, EDF is conducting a verification that the equipment and structures which are needed to mitigate a core melt accident can withstand to the severe accident conditions. If any, the limits to the equipment robustness have to be known.

Even if all these reinforcements bring very substantial risk reduction, especially for the short term of any severe accident, it has to be recognized that there are some important gaps with the solutions developed for a Gen III reactor like EPR.

For example, in the worst severe accident situations (typically a long term total loss of core cooling), it is difficult to demonstrate that the corium can be stabilized after vessel failure. Another important limit is the protection of severe accident equipment against external hazards (earthquake, especially) which was not considered before the Fukushima Dai-chi accident. That means that the efficiency of the long term accident management strategies for the Gen II PWRs is still limited in comparison with the efficiency of the EPR strategies.

For IRSN, these limitations, and also the progress in the knowledge on severe accident progression, justify to continue efforts in Gen II PWRs reinforcement for severe accident.

### 3. GEN II PWRs SAFETY OBJECTIVES ASSOCIATED TO THE REDUCTION OF POTENTIAL RADIOACTIVE RELEASES IN THE FRAMEWORK OF PLE

In the framework of the Gen II PWR program, the French Nuclear Safety Authority stated to EDF that the safety objectives of the Gen III reactors (for instance the Flamanville 3 EPR) should be used as a reference for all studies undertaken in the frame of PLE. For EPR, the general objective [1] related to the reduction of potential radioactive releases is “*to achieve a significant reduction of potential radioactive releases due to all conceivable accidents, including core melt accidents*”. It means:

- “For accident situations without core melt, there shall be no necessity of protective measures for people living in the vicinity of the damaged plant (no evacuation, no sheltering);
- Accident situations with core melt which would lead to large early releases 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;
- Low pressure core melt sequences have to be dealt with so that the associated maximum conceivable releases would necessitate only very limited protective measures in area and in 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, no long term restrictions in consumption of food”.

The first objective is mainly related to Steam Generator Tube Rupture (SGTR) and Loss of Coolant Accident (LOCA) design basis accidents. The EDF proposals for the 900 MWe PWRs PLE program have not been reviewed yet by IRSN and are not developed in this paper.

The second objective has been largely addressed by the modifications which have been summarized above.

For the third objective, two remaining issues have to be considered:

- The long term stabilization of the corium in case of vessel failure cannot be demonstrated for all conditions;
- The EFCVS decontamination factor for gaseous iodine is not sufficient to limit the need for emergency evacuation to the immediate vicinity of the plants.

EDF, in accordance with its initial PLE program, the post-Fukushima lessons and the ASN requests has included the three important following Gen II PWRs upgrades in its PLE program:

- A strategy to allow corium stabilization without concrete basemat melt-through by the molten core after RPV failure;

- A strategy to remove heat from the containment without containment venting;
- A strategy to reduce the iodine release in case of containment venting during a core melt accident.

There are also few remaining issues associated to uncertainties in the studies, which are relevant for both the second and the third objectives: effects of an ex-vessel steam explosion, effects of an uncontrolled injection of non-borated water during accident progression (inherent heterogeneous dilution), optimization of water management to limit residual risk for hydrogen and increase the in-vessel corium stabilization possibility (in-vessel water injection during in-vessel core degradation, spray system activation, ...).

#### 4. MODIFICATIONS TO AVOID REACTOR CONCRETE BASEMAT MELT-THROUGH BY THE MOLTEN CORE AFTER RPV FAILURE

To limit the risk of reactor basemat melt-through by molten core after RPV failure, EDF has retained the following strategies:

- The vessel cavity (or reactor pit) is modified to avoid any water entry before vessel failure (in the existing design, the spray system activation fills the cavity with water);
- The reactor sumps are filled with water before the vessel failure;
- In case of vessel failure after core melt, the corium falls and spreads in the dry vessel cavity and optionally in an adjacent area. After complete spreading, some triggers are passively activated, allowing water from the sumps to submerge the spread corium;
- This water allows the corium cooling and its stabilization.

After the review of the principle of these modifications, IRSN has highlighted that:

- This strategy reduce significantly the possibility of containment failure by steam explosion in a flooded vessel cavity and is a good compromise between efficiency and feasibility for the ex-vessel corium stabilization;
- The size of the corium spreading area, depending on the reactor, has to be further discussed;
- Some design features have still to be defined, such as the passive trigger system for water submerging above the corium into the reactor cavity;
- There is a need for instrumentation (for instance to know the sumps water level) to provide information to the emergency teams, in order to alert any situation where the spread corium would not be submerged by water (emergency teams shall anticipate any need for additional water into the sumps).

The final studies of these modifications will be analysed during the next steps of the safety review process.

#### 5. MODIFICATIONS TO REMOVE THE DECAY HEAT FROM THE CONTAINMENT WITHOUT OPENING THE EMERGENCY CONTAINMENT FILTERED VENTING SYSTEM

In order to allow the possibility to remove the decay heat from the containment without opening the EFCVS, EDF intends to implement a disposal (Fig. 1) composed of:

- A fixed circuit (located in the fuel building for the 900 MWe series).
  - A pump qualified to extreme external hazards conditions and SA situations;
  - An injection line connected to the cold leg of the primary coolant circuit and another one feeding the sumps of the reactor containment building;
  - A suction line connected to the safety injection tank (direct injection) and another one pumping in the sumps of the reactor containment building (recirculation);
  - A heat exchanger;
  - Actuators enabling the disposal activation from the control room.
- A “cooling mobile circuit” (ultimate heat sink) composed of a mobile pump and hoses directly drawing up in the heat sink and lined on the heat exchanger by the EDF rescue team - FARN (Nuclear Rapid Response Force).

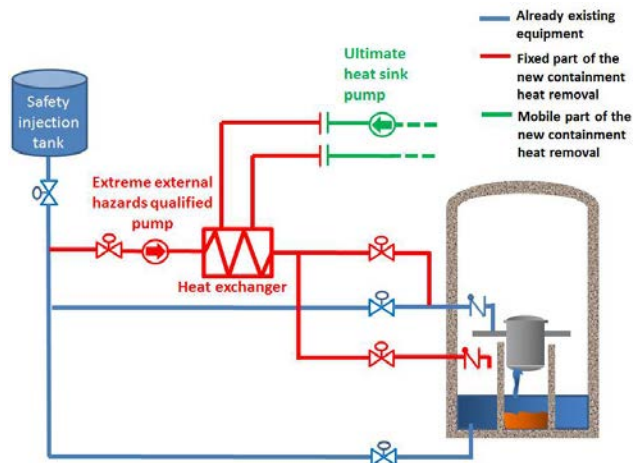


FIG. 1. New containment heat removal disposal (preliminary).

After the review of the principle of this modification, IRSN has concluded that:

- The new disposal intended by EDF is satisfactory in principle and should enable to remove the decay heat from the containment, if the reactor cooling by the steam generators had previously been realized during a sufficient time;
- An appropriate instrumentation is important to avoid any excessive pressure or temperature for the new disposal circuit and for the containment building;
- The possibility of circuit leakage during operation in severe accident conditions has to be considered with specific provisions like instrumentation to detect leakage, contaminated liquid management, reliable isolation valves;
- FARN activation criteria are important to install the mobile ultimate heat sink in due time with margins.

The final studies of this modification and its qualification to severe accident conditions will be analysed during the next steps of the safety review process.

## 6. MODIFICATION TO REDUCE THE IODINE RELEASE IN CASE OF FILTERED CONTAINMENT VENTING DURING A CORE MELT ACCIDENT

On the 900 MWe PWR series, in case of core melt accident, silver released from the control rods and deposited into the sumps water would enable iodine stabilization in the sumps. The 1300 and 1450 MWe PWRs control rods include a limited quantity of silver compared to 900 MWe so this stabilization process would be limited.

In order to reduce the gaseous iodine release in case of filtered containment venting during a core melt accident on the 1300 and 1450 MWe PWRs, EDF is installing some sodium tetraborate (borax) baskets on the sumps floor to passively alkalize the sumps water and consequently trap iodine.

After the review of this modification, IRSN has concluded that:

- Implementation of borax baskets will allow trapping a large part of the iodine in the reactor building sumps for accident where sodium hydroxide cannot be injected by the containment spray system;
- The release coming from the iodine in the upper part of the containment would not be fully affected by the iodine stabilisation in the reactor building sumps;
- There is still an interest to examine, for all Gen II PWRs, the possibility to upgrade the existing EFCVS to reduce the gaseous iodine release.

This topic and also the EFCVS seismic reinforcement for all Gen II PWRs will be discussed during the next steps of the safety review process.

## 7. CONCLUSION

For IRSN, the principles of the modifications planned by EDF in the framework of PLE (and the Post-Fukushima action plan) will really give more credit in reaching a stable reactor state after a core melt without any major failure of the reactor containment. During the coming period, the EDF detailed studies supporting the demonstration of the efficiency of main Gen II PWRs upgrades will be carefully examined, using available knowledge from research programs, especially for the corium coolability during molten core concrete interaction. This will allow the present French reactors to reach as far as possible the EPR safety objectives for severe accident, even if some specific EPR features cannot be directly implemented for the existing reactors (core-catcher with corium bottom and top cooling, buildings arrangement to prevent possibility of direct leaks to outside, ...).

After reaching a demonstration of the efficiency of these new disposals, will come the industrial challenges associated to the practical implementation on each reactor.

## REFERENCES

- [1] RAIMOND, E., et al., “Progress in the implementation of severe accident measures on the operated French PWRs – some IRSN views and activities”, OECD/NEA Workshop on the Implementation of Severe Accident Management Measures (ISAMM 2009), Böttstein, Switzerland.
- [2] Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, adopted during the GPR/German experts’ plenary meetings held on October 19<sup>th</sup> and 26<sup>th</sup> 2000.
- [3] CÉNÉRINO, G., et al., “Radiological objectives and severe accident mitigation strategy for the generation II PWRs in France in the framework of PLE”, Third International Conference on Nuclear Power Plant Life Management (PLiM) (Proc. Int. Conf. Salt Lake City, Utah, USA, 2012).

## PERIODIC SAFETY REVIEW AND ASSESSMENT

**Chairperson**

**C. TÓTH**  
Hungary



# RECENT APPROACHES RELATED TO SAFETY ENHANCEMENT OF OPERATING NPPS IN KOREA

T. JIN

KEPCO E&C

Gimcheon Gyeongsangbuk-Do, Republic of Korea

Email: renewfuture@gmail.com

## Abstract

There are 25 operating nuclear power plants (NPP) in Korea and five units are under construction. The safety of NPP is the most important goal in Korea like many other countries. The paper deals with the various safety enhancement activities in Korean NPPs. First of all, to conduct a Periodic Safety Review (PSR) based on IAEA safety series is one of the most effective ways to enhance the plant safety. The current status related to PSR is reviewed and some safety enhancement remedy actions are described. Also stress test is the effective way to improve the safety of operating NPPs against extreme natural disasters. Stress test targets, procedures and upgrading activities are presented. On September 12, 2016, there was an earthquake in Gyeongju, the southeastern part of the Korean peninsula, near Wolsong site. Fortunately, there are no serious casualties or damage. After this earthquake, Korean government started seismic-resistant program. The paper describes these kinds of safety re-enhancement actions in Korea.

## 1. INTRODUCTION

Since the first nuclear power plants (NPP) started commercial operation in 1978, Korea has built NPPs and currently operates 25 NPPs with 5 additional NPPs under construction [1]. Among them 20 NPPs have been operating more than 10 years while Kori Unit 1 will finish almost its first life extension on 2017. The first CANDU NPP, Wolsong Unit 1, started its continued operation from 2015 after its 30 years of design life.

As the number of aging plants increases, public concern over the safety of operating NPPs has risen. Systematic and comprehensive operational safety assessment and plant lifetime management are necessary to maintain a high level of safety, taking into account improvements in safety standards and practices, the cumulative effects of plant aging, operating experience, and the evolution of science and technology.

Periodic Safety Review (PSR) system was introduced and well established with sound legal basis for the comprehensive and systematic safety evaluation of operating plants. Stress test which was introduced after Fukushima accident in Korea is also one of effective ways to ensure the safety of NPP. There was an earthquake in Gyeongju area near Wolsong last year. It recorded 5.8 in Richter scale magnitude which was the largest in the history of Korean earthquakes since 1978 when the government started monitoring seismic activities. Various countermeasures are considered against earthquake.

This paper describes the current status, implementation structure and safety enhancement activities for operating NPPs, especially in the area of PSR including aging management and stress test which was introduced after Fukushima accident. Description of the safety enhancement activities after Gyeongju earthquake, led by the government, is also provided in this paper.

## 2. CURRENT TRADITIONAL REGULATIONS

### 2.1. Legal Basis for Regulation

The legal basis for regulation of Korean NPPs [2] is composed of the following attributes:

- Atomic Energy Act,
- Enforcement Decree of Atomic Energy Act (Presidential Decree),
- Enforcement Regulation of Atomic Energy Act (Ministerial Ordinance),
- Regulation on Technical Standards of Nuclear Installations (Ministerial Ordinance),
- Regulation on Technical Standards of Radiation Protection (Ministerial Ordinance),
- Notice of the Minister of Science and Technology.



## 2.2. Procedural Requirements

Construction permit is issued based on radiological environmental report, preliminary safety analysis report, quality assurance program for design and construction and early site approval for limited construction work on a proposed site before the construction permit is issued. Operating license is issued based on the operational technical specifications (TS), FSAR, quality assurance program for operation, radiological environmental report and radiological emergency plan. It should be noted that prescriptive limit on license term is not given in the license, however, the FSAR clearly identifies the design life. After the commercial operation, all the important changes related to the safety should be reported and reviewed and then the changes of FSAR have to be made.

## 2.3. Design Requirements

- Quality standards: Design, testing, and inspection of Structures, Systems and Components (SSCs) conducted to quality standards commensurate with the importance of the safety functions.
- Environmental and dynamic effects design bases: SSCs are designed to accommodate the effects of, and to be compatible with the environmental conditions including the effects of aging.
- Equipment qualification: Equipment is installed after meeting qualification of its functional capabilities by experience, analysis, test or their combination.
- Testability, monitorability, inspectability, maintainability: SSCs designed to be tested, monitored, inspected, and maintained to ensure that their structural integrity, leak tightness, functional capability, and operability are maintained during the life of the nuclear power plant.

## 2.4. Inspection Requirements

- Pre-operational inspection: Conducted regarding the installation and performance of the facilities by means of a document inspection and a field inspection.
- Periodic inspection: Conducted regarding the performance of the several facilities including reactor with a 20-month interval during refueling outage.
- Quality assurance inspection: Conducted to check quality assurance activities according to the quality assurance program.

## 2.5. Requirements on Safety Measures for Operation

- Conformance to technical specifications (TS): To monitor the limiting conditions for operation in TS, and to take proper actions.
- Testing, monitoring, inspection and maintenance of SSCs
  - ISI: Aging related degradation in material and performance of safety related SSCs shall be monitored, evaluated and managed based on the appropriate remedy actions.
  - IST: For major pumps and valves necessary for safe shutdown and reduction of accident consequences, the performance and the aging related degradation shall be monitored evaluated and managed.
  - RPV surveillance test: The degradation in material properties of reactor pressure vessel due to neutron irradiation shall be monitored, evaluated and managed.

## 2.6. Corrective Actions and Enforcement

Nuclear facilities shall be used when the integrity and performance are confirmed to be satisfactory through pre-operational inspections for each construction process. The reactor is allowed to be at a critical state if the performance of nuclear facilities is confirmed to be satisfactory through periodic inspections. Regulatory body could order to take corrective or complementary measures, such as suspension of use, repair, or modification of guidelines for operation, against inadequate performance of facilities and safety measures for the operation. Also, they could order to submit report or documents on the corrective activities, and order to take corrective or complementary measures as a result of the inspections.

### 3. PERIODIC SAFETY REVIEW

#### 3.1. Current Progress

Nuclear Safety Commission decided basic framework for the implementation of the PSR in December 1999. Ministry of Science and Technology (MOST) issued 'Implementing Guidelines for PSR' in May 2000 after deliberation of Nuclear Safety Commission. Korea Hydro and Nuclear Power Company (KHNP) submitted the PSR Plan on 30 May 2000, which includes the plan for Kori Unit 1 to be completed by November 2002 and Wolsong Unit 1 by June 2003. Atomic Energy Act was revised to adopt PSR system in January 2001, including basic direction and framework for the implementation of PSR. Detailed provisions including review scope, method, procedure, and technical standards are included in the Enforcement Decree (Presidential Decree) and the Enforcement Regulation (Ministerial Ordinance) of the Atomic Energy Act. Since then PSR have been performed continuously in Korea. The 1<sup>st</sup> round PSR for 20 NPPs that have been operating for more than 10 years has been completed. The 2<sup>nd</sup> round PSR for the following three NPPs are currently being carried out:

- Kori-2
- Hanbit-5, 6.

#### 3.2. PSR Implementation Structure

PSR is specified to be carried out every 10 years after the first criticality before the commercial operation. The operator of NPPs (KHNP) has the responsibility of performing the PSR. Former Ministry of Science and Technology (MOST) specified PSR requirements and currently Nuclear Safety and Security Commission (NSSC) reviews the PSR results. Review scope is based on 14 safety factors suggested by IAEA in Safety Series [3], and detailed scope may vary depending on plant age. PSR for twin plants having a single FSAR is assembled together into a single report but separately consider the aging of SSCs and the physical status of each plant. Once the PSR report is submitted, NSSC/KINS (Korea Institute of Nuclear Safety) reviews PSR results and prepares safety evaluation report (SER) with identification of safety issues.

Aging review is focused to ensure that plant aging is being effectively managed so that required safety margins are maintained and adequate aging management program is in place for future safe operation of the plant. The aging management for the passive system is one of the most important factors in PSR and implemented as shown in Fig. 1.

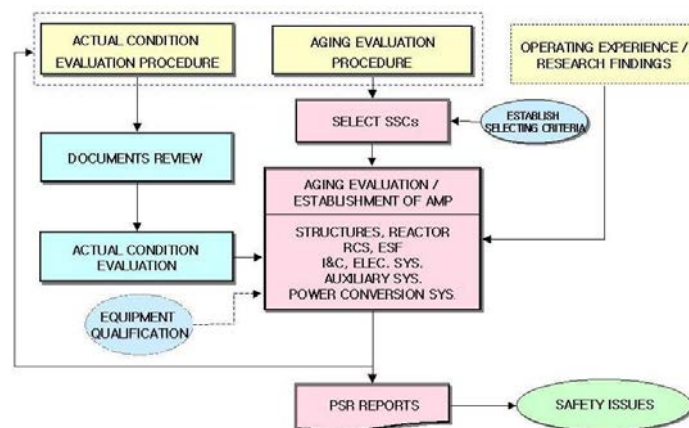


FIG. 1. Evaluation method of passive SSCs in PSR.

#### 3.3. Safety Enhancement Activities in PSR

All the possible remedy actions based on each PSR per plant are clarified and performed to improve the safety of the NPPs. For example, transient evaluation results showing the fatigue integrity of the pressure boundary components is important for the next 10 years of safe operation. Transient counting monitoring system is installed for each NPP. Not only the results of the past 10 years in-service inspection but also the effectiveness of applicable code and standard are confirmed and check again to re-ensure the integrity of the results and evaluations.

The utility (KHNP) has to report the implementation status of PSR to KINS every three months and regulatory authority controlled the follow-up measures.

#### 4. STRESS TEST

##### 4.1. Current Progress

After Fukushima accident, there was a strong need for comprehensive and transparent risk and safety assessment of NPPs. The Korean government also decided to perform stress test of the older NPPs. Stress test for Kori-1 and Wolsong-1 were performed based on the international experience to reassess the targeted safety margin. Stress test aims to strictly re-confirm the safety of NPPs by evaluating its capability to respond to large-scale natural disasters beyond the design basis. Stress test report for Wolsong-1 was submitted to KINS on June 2013. KINS and civilian inspection team reviewed the results and finally the continued operation of Wolsong-1 was permitted on February 2015. Stress Test Report for Kori-1 was also submitted on December 2013. The Korean government decided to perform stress test for the remaining 22 NPPs by late 2018.

##### 4.2. Stress Test Implementation Structure

Evaluation areas for the stress test are mainly the following 5 areas.

- Safety of SSCs against Earthquakes,
- Safety of SSCs against Tsunami, Storm Surge, and Other Natural Disasters,
- Plant Response to Loss of Electrical Power and or Loss of the Ultimate Heat Sink,
- Severe Accident Management Capability,
- Emergency Preparedness and Response.

##### 4.3. Safety Enhancement Activities in Stress Test

Probabilistic seismic hazard analysis was performed and the exceeding probability was much less than the criteria based on 0.2g. Safety of SSCs against tsunami, storm surge, and other natural disasters was also evaluated and the appropriate measures are prepared. All the safety equipment important to maintain the safety functions of the NPPs was evaluated to test the plant response to loss of electrical power and or loss of the ultimate heat sink. Natural cooling concept was prepared shown in Fig. 2. [4] Severe accident management guide (SAMG) was updated and passive autocatalytic recombiners (PAR) were installed additionally to mitigate the possibility of hydrogen explosion. Emergency preparedness and response procedure was also reinforced.

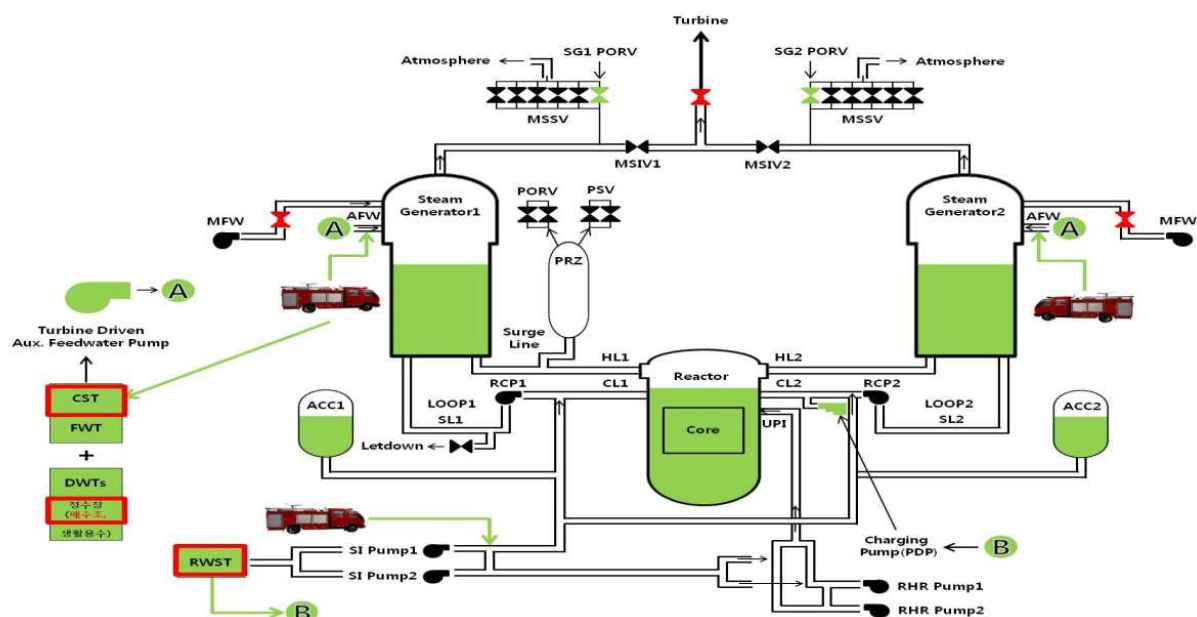


FIG. 2. Natural Circulating Cooling System.

## 5. EARTHQUAKE ISSUE

### 5.1. Current Progress

There was an earthquake on September 12, 2016 at Gyeongju near Wolsong site. Measured at 5.8 on the moment magnitude scale, it was the strongest ever recorded in Korea since measurements begun in 1978. Even though there was no significant damage on the human and houses, it was the starting point to strengthen the anti-seismic remedy actions. Various seismic evaluations including the fault survey are performed currently.

### 5.2. Seismic Design Structure

The OPR 1000 which is the Korean standard nuclear power plant with a two-loop 1000MWe PWR reactor was originally designed to withstand 0.2g Peak Ground Acceleration(PGA) of the Certified Seismic Design Response Spectra (CSDRS) from RG 1.60. After the Fukushima accident, the OPR1000s have been upgraded to withstand 0.3g PGA. The APR1400, the advanced type of the OPR1000, is being designed to withstand 0.3g PGA and to perform their intended safety function at 0.5g PGA level. Emergency response buildings designed to withstand 0.5g PGA were planned to be constructed at every site for nuclear power plants in Korea after Fukushima accident and accelerated to be constructed by 2020 after Gyeongju earthquake.

### 5.3. Safety Enhancement Activities against Earthquake

Ministry of Trade, Industry and Energy set up the following 5 tasks and seismic measures which consist of 22 sub-tasks.

- Evaluation and countermeasures of seismic hazard near NPP areas,
- Acceleration of seismic performance enhancement,
- Strengthening emergency response capability,
- Continuous evaluation and enhancement of earthquake-resistance,
- Improvement of NPPs long-term safety.

Nuclear Safety and Security Commission also prepare safety enhancement actions against seismic damages.

- Improvement of seismic response systems,
- Seismic reinforcement and detailed evaluation of seismic capability for operating NPPs,
- Enhancement of the safety of Korea radioactive waste agency (KORAD) in Gyeongju,
- Detailed geological survey and re-evaluation of design criteria around Gyeongju area,
- Preparedness of emergency response facilities against earthquakes,
- Enhancement of emergency response capability against earthquakes.

## 6. CONCLUSIONS

Safety enhancement activities are continuously reinforced for the operating NPPs in Korea. It is mainly based on PSR structure, in addition to the routine operation activities like ISI, IST and so on. PSR system was introduced and well established with sound legal basis for the comprehensive and systematic safety evaluation of the operating plants. Aging assessment and remedy actions in PSR contribute directly to the safety enhancement of NPPs. Recently stress test and earthquake countermeasures also play an important role to increase the safety of the Korean NPPs.

## REFERENCES

- [1] MOTIE, Handbook of Strategy for Nuclear Power Plants (2015).
- [2] KIM, H.-J., Nuclear Safety and Regulation, Hanshuse, Seoul (2012).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review for Nuclear Power Plants, IAEA-SSG-25, IAEA, Vienna (2013).
- [4] KHNP, Report on the stress test for Kori-1, internal report, KEPSCO E&C, Seoul, 2013.

## EXTERNAL EVENT LEVEL 1 PSA FOR THE WWER440 TYPE REACTORS IN SLOVAKIA

Z. KOVACS

RELKO Ltd, Engineering and Consulting Services

Bratislava, Slovakia

Email: kovacs@relko.sk

### Abstract

The objective of the external event PSA is to quantify the core damage frequency for all operating modes and to understand the overall risk from external events (seismic events and non-seismic natural events and man-made events), identify the dominant contributors to the risk, determine the external event loads which dominate the plant risk, compare external event risk to risk originating from internal events and propose safety measures to improve the plant safety. The basic inputs used for modeling of the plant are the results of the external event hazard analysis of the site (hazard curves), the fragility analysis of the plant structures, systems and components (fragility curves) and the existing level 1 full power and shutdown PSA model for internal initiating events. The impact of external events on safety of WWER440 reactors is being evaluated in the light of Fukushima accident. Only extreme external events can have impact on the plant safety. The nuclear power plants are protected against all external events that are likely to experience within the projected life time. The challenge is to estimate the frequency of such conditions which has potential to damage the plant.

### 1. INTRODUCTION

The external event PSA has the objective to demonstrate how the plant is resistant to seismic event, extreme weather conditions and man-made events and to an irreversible process of degradation (cliff-edge effect) after the occurrence of the events. The ultimate aim is to show that the impact of external events is acceptable or will be either removed or minimized.

External events can occur as single events or as combinations of two or more external events. The potentially combined events are two or more external events having a conditional probability of simultaneous occurrence, e.g., strong winds occurring at the same time with extreme rain or snow. The single external events are presented in part 2 of the paper. The single events and their potential to create combinations are described in more detail in the third part of the paper. In addition, the relevant combinations of the events are identified and the occurrence frequency calculation is presented. The results and conclusions are available in the fourth part of the paper. The paper is prepared on the basis of [1-5] for the J. Bohunice site.

### 2. THE SINGLE EVENTS

After careful evaluations of all threats and in coincidence with internationally accepted approaches, the following events are considered as external events for the Slovak NPPs:

- extreme wind,
- tornado,
- extremely high outside temperatures,
- extremely low outside temperatures,
- extreme rain,
- extreme snow,
- icing,
- lightning,
- earthquakes, and
- geomagnetic currents.

In addition, the following man-made events are considered:

- aircraft crash,
- influence of neighboring industry, and
- other external influences.

### 3. EVALUATION OF COMBINATION OF EXTERNAL EVENTS

#### 3.1. The methodology

After identification of the relevant natural single events, the combinations of events are identified. In the first step exclusion of combinations with two events is performed. High number of combinations can be screened out using the following criteria:

- Independent events: the selected events that have no dependency with other events are excluded from further evaluation within the combination analysis.
- Seasonal variation: the events occurring in different seasons cannot form a relevant combination.
- Exclusive preconditions: some events require specific preconditions related to weather conditions. The events that have opposite preconditions cannot form a relevant combination.
- Similar or same effects: the effects of two events are the same or very similar (the same initiating events are initiated from the list of internal event PSA). Given the first event occurred, no further consequences are caused by the second event. These event combinations are not considered. However, the event combination is relevant if the combined effect is significantly greater than the effect of a single event.

A combination of events is assumed relevant only if the simultaneous occurrence of the events is dependent. Given that two rare events occur independently, the combined occurrence is so improbable that the combination can be considered insignificant.

There are two types of dependencies:

- Fundamental dependency: the occurrence of events is related to the same basic phenomenon or the events are created by the same mechanism.
- Cascade-type dependency: The first event strengthens the second event, it means that its probability is increased or its effect is worsened.

The qualitative and quantitative assessment is performed for the identified relevant combinations of two events. If after a qualitative assessment a combination is still considered relevant, the frequency of the event combination is calculated by using the frequencies of occurrence of the single events. These frequencies are estimated using the extreme value theory [3, 4, 5] and input data of the events for at least 30 years. The event with a lower frequency is assumed to be occurred and the conditional probability for the other event to occur is estimated.

An event combination may be considered relevant if it exceeds the general cut-off value frequency ( $1.0E-7/y$ ) normally applied in the PSA. The cut-off value is lower ( $1.0E-9/y$ ) given that the conditional core damage probability or conditional large early release probability after the occurrence of event combination is one.

The combinations with more than two events are also identified. The approach is that the two-events combinations are evaluated whether there is additional event which has a dependency with both events. The approach is the same for combinations with more than three events.

#### 3.2. Application of the methodology

##### 3.2.1. Independent event

The earthquakes and geomagnetic currents are assumed to be independent of any other events. Earthquakes are related to sudden release of energy in the Earth's crust and are thus independent from any natural or man-made events occurring on the Earth surface or atmosphere. Geomagnetic currents are caused by highly energetic particles ejected from the sun (solar wind), which also create the aurora borealis. The space weather is independent from any events that originate on Earth surface or atmosphere.

##### 3.2.2. Seasonal variations

The seasonal variation of each event is analyzed based on measurement data from weather stations at the plants, weather simulations, documented observations and expert judgement. The relative monthly probabilities of external events are shown in Table 1. Seasonal variation of air temperature according to the Slovak weather station is available. The warmest months are July and August. The coldest month is January. In general, warm

temperatures can be expected between June and September and cold temperatures between November and February. Extreme high and extreme low air temperatures cannot form event combination due to season variation.

The monthly occurrence of extreme wind presents the monthly distribution of annual 10 minute wind speed maxima for the last 30 years. Extreme wind is probable during the whole year. January is the only exception. So, the extreme wind has high potential to enter with other events into combination.

TABLE 1. THE RELATIVE MONTHLY PROBABILITIES OF EXTERNAL EVENTS

No.	External event	January	February	March	April	May	June	July	August	September	October	November	December
1	Extreme wind												
2	Tornado												
3	Extremely high air temperature												
4	Extremely low air temperature												
5	Extreme rain												
6	Extreme snow												
7	Icing												
8	Lightning												

Colour marking of probabilities: High Moderate Low Very low

### 3.2.3. Event preconditions

Natural events related to atmosphere typically require certain simple preconditions. The preconditions analyzed in this paper are: air temperature (at ground level) above or below zero, wet/rainy or dry conditions. Table 2 presents the preconditions required by different events.

Tornado requires an adequate air temperature and is nearly always accompanied by rainfall. High air temperature requires dry conditions because rainfall cools down the air and direct sunlight cannot heat the earth's surface due to clouds.

TABLE 2. PRECONDITIONS OF EXTERNAL EVENTS

N.	External events	Air > 0 °C	Air < 0 °C	Wet/Rainy	Dry
1	Extreme wind				
2	Tornado	x		x	
3	High temperature	x			x
4	Low temperature		x		
5	Extreme rain	x		x	
6	Extreme snow		x	x	
7	Icing		x	x	
8	Lightning	x		x	

### 3.2.4. Plant effects

Different parts of the buildings and structures can be affected by external events, such as building roofs, walls, switchyard, etc. Ventilation can be affected by different mechanisms. Humid and hot conditions weaken the heat transfer capacity, the air intakes could be blocked by icing, snow or material detached by extreme wind or tornado, low air temperature could lower the room temperatures, pressure differences caused by strong wind might disturb the air movement and dense smoke could enter the intakes if a fire occurs nearby. The loss of heat sink could result if extreme wind or tornado blows material into the cooling water intake. The intake screens could also be blocked by ice. Loss of offsite power could be caused by different phenomena that cause structural or functional damage to grid components. Extreme wind, snow and ice loads could cause damage to grid structures, and grid components could also fail due to lightning strikes. The source of flooding can be rainfall.

Initiating events initiated by different external events are identified from the internal event PSA. The extreme wind tornado and extreme snow can initiate the same initiating events:

- Loss of essential service water,
- Opening of all steam dump stations to the atmosphere or SG safety valves,
- Closing of all quick closing valves on the steam lines,
- Loss of offsite power,
- Loss of circulating cooling water, and
- Loss of feedwater supply.

Extreme high temperature leads to reactor trip. Extreme low temperature initiates loss of essential service water and reactor trip. Extreme rain initiates loss of essential service water, loss of circulating cooling water and reactor trip. Icing and lightning initiate loss of offsite power and reactor trip.

### 3.2.5. Identification of event combinations

The irrelevant combinations are identified according to the screening criteria presented in part 3.1. The excluded event combinations according to screening criteria 2, 3 and 4 are presented with a red color in Table 3. After the exclusion of irrelevant combinations, the remaining combinations of two events are considered one by one to identify the types of dependencies (a or b). The dependent events have been marked with green color in Table 3. In addition to the combinations with two events, a relevant combination with three events was identified: extreme wind and extreme snow and icing.

TABLE 3. EXCLUDED AND INCLUDED COMBINATIONS OF EXTERNAL EVENTS

	Extreme wind	Tornado	High temper.	Low temper.	Extreme rain	Extreme snow	Icing	Lightning
Extreme wind								
Tornado	4							
High temper.	3	3						
Low temper.	b	3	2					
Extreme rain	a	a	3	3				
Extreme snow	a, b	3	3	3	3			
Icing	b	3	3	b	3	b		
Lightning	a	a	3	3	a	3	3	

### 3.2.6. Quantification of occurrence frequencies

The frequency of combination with two events is calculated by multiplication of the lower single event frequency and the conditional probability of the other event. The frequency of combination with three events is calculated by multiplication of the lowest single event frequency and the conditional probabilities for the other events. Frequency calculation was performed using the extreme value theory [3] for the single events based on measurement data from the weather stations at the plant. Detailed evaluation of a combination (extreme low temperature and extreme wind) is presented for illustration of using the conditional probabilities. The single event frequency is lower for the extreme low temperature ( $1.62\text{E-}4/\text{y}$ ) than for the extreme wind ( $1.00\text{E-}3/\text{y}$ ). The occurrence of the extreme wind is possible from the beginning of February until the end of December. It means that during 91.67% of the year  $[(11/12) \times 100]$  simultaneous occurrence of extreme low temperature and extreme wind is possible. So, the conditional probability for occurrence of extreme wind is 0.9167. Now the frequency for simultaneous extreme low temperature and extreme wind occurrence is calculated:  $1.62\text{E-}4/\text{y} \times 0.9167 = 1.49\text{E-}4/\text{y}$ . The results for all combinations are presented in Table 4.



### 3.2.7. Evaluation of man-made external events

Frequency of occurrence is less than  $1.0\text{E-}7/\text{year}$ . Thus, the aircraft crash is excluded from further analysis. Similarly, influence of neighboring industry and other external influences were estimated and excluded from further analysis. The natural non-seismic external events and man-induced events are treated as independent events. Their combinations have negligible frequency of occurrence.

TABLE 4. INCLUDED COMBINATIONS OF EXTERNAL EVENTS

Event 1	Event 2	Event 3	Frequency (1/year)
Lightning > 200 MA	Extreme wind > 42 m/s	-	1.25E-4
Extreme low temperature < -45°C in 10 h	Extreme wind > 42 m/s	-	1.49E-4
Extreme rain > 175 mm in 24 h	Extreme wind > 42 m/s	-	3.97E-7
Extreme snow > 2000 Pa	Extreme wind > 42 m/s	-	2.24E-6
Icing > 700 g/m	Extreme wind > 42 m/s	-	6.99E-4
Extreme rain > 175 mm in 24 h	Lightning > 200 MA	-	1.08E-7
Extreme snow > 2000 Pa	Icing > 700 g/m	-	8.02E-7
Extreme low air temperature < -45°C in 10 h	Icing > 700 g/m	-	5.39E-5
Extreme rain > 175 mm in 24 h	Tornado		1.96E-4
Lightning > 200 MA	Tornado		1.17E-4
Extreme snow > 2000 Pa	Extreme wind > 42 m/s	Icing > 700 g/m	7.38E-7

## 4. RESULTS AND CONCLUSIONS

The seismic contribution to the overall risk (core damage frequency - CDF) during full power operation is extremely high. The reason is that the site seismic hazard is overestimated, therefore, new hazard curves must be constructed to estimate the realistic hazard level based on [7]. In addition, the seismic capacity of structures and components of the plant is determined by the GIP WWER methodology [8] which provides conservative values, detailed analysis must be performed for the dominant structures and components based on [6].

The non-seismic external event contribution to the overall CDF is high due to extreme wind. Safety upgrading was proposed to increase the wind capacity (resistance) for selected structures and components to reduce the risk. Significant attention was paid to event combinations. Qualitative and quantitative methods were developed and applied to identify the potentially relevant combinations. The initial list of relevant single events included 8 events. 28 different combinations with two events have been formed. From these combinations 18 were excluded by using screening criteria. After the qualitative analysis the number of relevant dependent event combinations with two events is 10 and with three events is one. However, their impact on the risk is negligible.

The multi-unit interactions are not part of the analysis. It is task for the future.

## REFERENCES

- [1] KNOCHENHOUER, M. and LOUKO, P., Guidance for external event analysis, SKI report, 02:27, February 2003, Sweden, The Swedish Nuclear Inspectorate.
- [2] HELANDER, J., Identification and analysis of external event combinations for Hanhikivi 1 NPP, PSAM13, Seoul, Korea, 2016.
- [3] HAAN, L. and FERREIRA, A., Extreme value theory, an introduction, Springer, 2006.
- [4] Probabilistic Safety Assessment of Unit 3 of J. Bohunice V2 NPP for External Events - Level 1 Fullpower PSA study for non-seismic external events, main report, RELKO report 5R0414, Issue 2, December 2016, Bratislava.
- [5] Probabilistic safety assessment for unit 3 of J. Bohunice V2 NPP for external events – Shutdown Level 1 PSA study for non-seismic external events, main report, RELKO report 5R0414, Issue 2, December 2016, Bratislava.
- [6] EPRI “Methodology for Developing Seismic Fragilities,” EPRI TR-103959, EPRI, Palo Alto, California, June 1994.

- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Hazards in Site Evaluation for Nuclear Installation, IAEA-SSG-9, IAEA, Vienna (2010).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Earthquake Experience and Seismic Qualification by Indirect Methods in Nuclear Installations, IAEA-TECDOC-1333, IAEA, Vienna (2003).

**BIBLIOGRAPHY**

KOVACS, Z., Probabilistic Safety Assessment of WWER440 Reactors, Springer, Heidelberg, New York, London (2014).

## ADDRESSING FIRE SAFETY “THE RIGHT WAY”

R. KALANTARI

President, Engineering Planning and Management, Inc.  
Framingham, Massachusetts, U.S.A.  
Email: rbk@epm-inc.com

T. JUTRAS

Vice-President, Engineering Planning and Management, Inc.  
Framingham, Massachusetts, U.S.A.  
Email: thj@epm-inc.com

P. OUELLETTE

Vice-President, Engineering Planning and Management, Inc.  
Framingham, Massachusetts, U.S.A.  
Email: pro@epm-inc.com

### Abstract

The paper discusses the evolution of fire safety regulations in the United States since the 1975 Browns Ferry fire. It discusses the challenges the nuclear power industry had with the original, unrealistic deterministic rule and the reasons why, 20 years later, risk-informed methods were introduced. The paper will discuss in-depth why addressing fire safety has been one of the most challenging and costly regulation for US NPPs. The paper analyzes the problems with the original proposed regulation and the efforts the US nuclear power industry took to address this complex regulation. The paper will also provide key lessons learned, and provide methods and solutions for addressing fire safety, “the right way” which will be essential for other countries facing strict fire safety regulations.

### 1. BACKGROUND

The significance of the issue of fire safety at nuclear power plants was made evident by the impact of the fire at Browns Ferry in the US in 1975. In this fire which was started by an employee using a lit candle to check for air leaks, the fire damage extended from the cable spreading room into an adjacent area in the unit 1 reactor building and impacted approximately 1600 cables which affected two separate units at the site. Electrical cables shorted together and grounded to their supporting cable trays and conduits, resulting in the loss of control power associated with required equipment. All of the emergency core cooling systems for the Unit 1 reactor were rendered inoperable and portions of Unit 2's systems were likewise affected [1]. The fire and its aftermath revealed some significant inadequacies in design and procedures related to fires. The fire protection programs in the U.S. today, as well as many other countries across the globe, are a direct result of this fire and its lessons learned.

Today, fire is considered a major or even dominant contributor to the total risk of core damage for most plants. Based on the similarities of many of the nuclear plant designs globally, and the fact that fires can occur anywhere, this nuclear safety issue is considered universal in nature. The solutions outlined below are, therefore, also considered to be effective universally and this has been witnessed through our experience internationally in Canada, Europe and Asia.

### 2. US REGULATIONS

Prior to the Browns Ferry Fire, Title 10 of the Code of Federal Regulations Part 50 (10 CFR 50) Appendix A, General Design Criteria (GDC) 3 [2] formed the basis for regulatory acceptance of fire protection programs in the US. The requirements of GDC 3 are broad and provide no specific details with regard to ability to safely shutdown.

In the early days following the Browns Ferry fire, regulations were developed in the US to make fire protection measures more robust. These early regulations, however, did not address the concept of fire safe shutdown adequately and in many cases were implemented in a manner that provided little safety benefit while costing utilities tens of millions of dollars.

While several fire safety concepts were developed soon after the Browns Ferry fire, it took more than twenty (20) years before the concepts were sufficiently understood and documented such that some consistency in the nuclear industry was achieved. Even today, however, complete consistency has not been reached and the approach to some concepts (e.g. multiple spurious operations) remains dynamic and unsettled.

### 3. BTP APCSB 9.5-1 "GUIDELINES FOR FIRE PROTECTION FOR NUCLEAR POWER PLANTS" MAY 1, 1976 [3]

Branch Technical Position (BTP) APCSB 9.5-1 was a quick response to the Browns Ferry fire and provided guidelines acceptable for implementing fire protection criterion for nuclear reactor power plants. The primary purpose of the Fire Protection Program for nuclear power plants is to maintain the ability to perform safe reactor plant shutdown functions and to minimize radioactive releases to the environment in the event of a fire. This BTP relied on Regulatory Guide 1.75 [4] for criteria for cable separation distance. Appendix A to BTP provides specific guidance on the preferred and, where applicable, acceptable alternatives for fire protection programs at nuclear facilities whose construction permits were docketed prior to July 1, 1976, and applies to plants that were under review, under construction or operating prior to July 1, 1976.

The BTP and Appendix A to the BTP provided detail design methods and requirements for various plant areas with regard to the need for systems such as fire suppression and detection systems and features, and required performing a detailed fire hazards analysis. It also provided very general requirements for separation of plant safety related systems, with no specific details, other than stating: *"Separate redundant safety related systems from each other so that both trains are not subject to damage from a single fire."*

While meeting the requirements for fire protection system and feature upgrades was relatively straight forward, meeting the safe shutdown requirements was not practical and plants were unable to show compliance to the requirements. What BTP 9.5-1 and Appendix A to the BTP did not completely address was Post-Fire Safe Shutdown capability.

### 4. 10 CFR 50.48, "FIRE PROTECTION" [5] AND 10 CFR 50 APPENDIX R, "FIRE PROTECTION PROGRAM FOR NUCLEAR POWER FACILITIES OPERATING PRIOR TO JANUARY 1, 1979" [6]

By the late 1970s, the majority of operating plants in the US had completed their analyses and had implemented most of the fire protection program requirements of Appendix A to the BTP. In most cases, the analysis and the proposed modifications by the utilities were reviewed by the US NRC and were found to be acceptable. However, the issue that remained unresolved was addressing safe shutdown, and the requirement for developing an alternative shutdown capability in the event of fire requiring control room evacuation.

In May of 1980, the US NRC decided to resolve this issue through the rulemaking process and by February of 1981 issued a new rule, 10 CFR 50.48, "Fire Protection" and Appendix R to 10 CFR 50, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979". However, newer plants were subject to essentially the same technical requirements which were specified in their operating license. In July 1981, the US NRC issued Section 9.5.1 of the Standard Review Plan which describes fire safety provisions applicable to all plants licensed after January 1, 1979. In general, this document closely reflects the technical requirements of Appendix R.

The proposed rule was deterministic and mandated a strict compliance for all plant areas. It simply stated: *"Ensure one train remains free of fire damage."*

This new deterministic rule made significant strides toward addressing the problem of ensuring a safe shutdown in the event of fire. In many cases, however, this deterministic rule was misinterpreted, misapplied or was impossible in some cases to comply with. The US NRC recognized the shortcomings of literal compliance to this regulation and allowed plants to apply for exemptions to demonstrate safe shutdown in lieu of literal compliance.

## 5. WHAT IS FIRE SAFE SHUTDOWN ANALYSIS?

A Fire Safe Shutdown Analysis (FSSA) is a comprehensive analysis that demonstrates those SSCs important-to-safety can accomplish their respective post-fire safe-shutdown functions. Such an analysis demonstrates that the success path SSCs, including electrical circuits, remain free of fire damage in the event of postulated fires. As required by applicable regulations, fire barriers, physical separation with no intervening combustibles, and/or automatic detection and suppression are acceptable means to provide this protection. Where a safe shutdown success path cannot be adequately protected, an alternative or dedicated shutdown success path must be identified and protected to the extent necessary to ensure post-fire safe shutdown.

The major steps involved with the Fire Safe Shutdown Analysis (FSSA) include:

- Determination of Fire Safe Shutdown (SSD) Performance Goals;
- Selection of SSD Systems and Components;
- Circuit analysis for each SSD component to identify the required SSD Cables;
- Identification of physical location of SSD Cables and Components;
- Evaluate Potential Impact of Fire Hazards to SSD systems;
- Identify equipment and cable interactions;
- Document resolutions.

As can be seen from the list above the tasks involved to address fire safe safety and fire safe shutdown requires not only involvement of knowledgeable fire protection engineers, it also requires a significant amount of support from mechanical systems and electrical engineers trained in the area of fire induced equipment and circuit failures. These engineers play a large role in the performance of a successful FSSA.

## 6. EFFORTS AND CHALLENGES ADDRESSING THE PROPOSED REGULATION

In general addressing the requirements of BTP and Appendix A were relatively straight forward, although costly. US plants typically spent between \$5 million to \$50 million for the analysis and physical plant modifications. However, the efforts for addressing the safe shutdown capability during a fire was far from being done, and done per the requirements of the proposed Appendix R rule.

Literal compliance to the requirement that one train of equipment free of fire damage, is impossible when considering a full area burnout that results in complete damage to all FSSA equipment and cables in plant areas like the cable spreading room or the main control room. Also in some plant areas, it does not improve plant safety, especially in large open areas with low or no combustibles and/or hazards. Nevertheless, a number of US plants tried to meet this requirement by proposing extensive modifications to safe shutdown systems, circuits, and in many cases provided three hour raceway barrier protection where no fire hazards existed, but they still did it to meet the requirements of the rule. The modifications were very costly. By the late 1980s, every utility had completed “an analysis” and millions of dollars were spent for the analysis. In addition, millions of dollars were spent modifying the plant. The US NRC also granted several hundred exemptions as part of this process. However, not everyone (i.e., the utilities and vendors) had the same interpretation and understanding of the regulation.

Upon further review in the late 1990s, the US NRC inspectors found new problems with fire induced circuit analysis and also identified concerns about Themolag<sup>TM</sup> fire barriers that were used as raceway protection. The fire barrier material did not meet the qualification criteria. The industry tried to resolve this issue by reanalyzing their plant and in some cases proposed manual actions in lieu of compliance to the deterministic rule. The industry also tried to defend their position by offering fire testing of cables. This was deemed unfavorable to the industry as the fire test resulted in failures that were not originally anticipated. This resulted in a new requirement for consideration, multiple concurrent spurious operations, due to multiple concurrent circuit failures occurring during the fire.

## 7. NEW OPTIONAL REGULATION, PERFORMANCE BASED APPROACH

Fire science has evolved during the many years since the early regulations and with it so have the fire safety regulations. An effort to develop a Performance-Based standard by the National Fire Protection Association (NFPA) started in the mid-1990s. The standard, NFPA 805 [7] was developed by the Technical Committee on

Fire Protection for Nuclear Facilities. The technical committee included several fire protection and fire safe shutdown engineers from the US nuclear utility industry, the insurance industry and the US regulator, the NRC. The standard was approved and issued by NFPA in 2001, and later on endorsed by the US NRC (with some exceptions) as a new RIPB compliance rule on July 16, 2004.

This new optional regulation allows the use of performance based analysis and fire modeling tools as well as probabilistic risk assessment to determine compliance. Driven in part by the results of the industry cable fire tests mentioned above, and corresponding new interpretation of the fire protection rule to consider multiple concurrent spurious operations, this option provided utilities with an alternative to the deterministic approach of demonstrating compliance with the US fire protection regulations. To date, NFPA 805 has been adopted by approximately half of the operating US plants.

## 8. WHAT WORKED AND WHAT DID NOT WORK SO WELL WITH RIPB APPROACH

This new RIPB compliance rule change required the creation of hundreds of pages of new regulation and supporting guidance documents beyond NFPA 805 in the form of NUREGs, Regulatory Guides, NEI Implementation guides, Frequently Asked Questions (FAQs), etc. Unfortunately, this complex compliance option proved costly and did not get implemented smoothly for several reasons. Although there was a pilot process to implement the new approach at two sites, regulatory incentives resulted in most plants adopting the new rule to commit to schedules which caused them to perform the transition at essentially the same time as the pilots. This defeated the purpose of having the pilot plants vet the process, which in turn caused significant iteration, rework and delays. Two other major contributors to the cost were the extensive revalidation of the existing fire protection licensing basis mandated by the new rule in order to transition from a deterministic to risk informed regulation, and the requirement by the regulator to perform a risk assessment, which required plants to perform full fire Probabilistic Safety Analysis (PSA). Fire PSA identified high risk plant areas which required extensive modifications and huge cost.

However, in the end, utilities that performed a RIPB analysis recognized significant safety benefits by identifying and addressing hidden risks in areas considered “compliant” with the existing deterministic rules. The varying results of these RIPB analyses performed in the US revealed that it was critical for the analysis team to have a sound understanding of the fire hazards and corresponding scenarios and how to model them, as well as being very cognizant of the subsequent impact to electrical circuits, components and associated plant safety systems. Those that performed the analysis properly saved millions of dollars over those who didn’t by achieving this increased level of safety without the need for significant unnecessary plant modifications.

## 9. A REASONABLE APPROACH TO ADDRESS FIRE SAFETY AT NPPS

As discussed in this paper, deterministic compliance is not practical, nor does it improve plant safety in all plant areas. Assuming all cables will fail due to a deterministic fire in an area that contains no hazards and protecting such cables in order to achieve compliance with a rule does not provide any appreciable improvement to plant safety. A performance based method, with realistic engineering evaluation based on qualitative and/or quantitative assessment of the plant design will provide the best results. Based on this, instead of separating plant redundant systems by three hour barriers or 6 meters of separation in all plant areas, the redundant systems should be separated adequately, commensurate with the hazards in the area. This process is fully documented in the NFPA 805 standard. It should be noted that a very similar performance based technique was utilized to address fire safety in all Canadian plants, even before NFPA 805 became a standard in 2001. Canadian regulation for addressing fire safety was initiated by CSA N293-95, and later on revised in 2007 and 2012 [8]. This standard allowed the use of a performance-based approach to fire safe shutdown for all Canadian nuclear plants.

A performance based analysis is not less onerous than a deterministic one. It requires a very similar effort to that of the deterministic analysis discussed earlier, and in some cases, may require more effort to collect and analyze the data, especially the fire modeling efforts. However, in the end, it does provide better results by focusing on plant areas that are vulnerable to fire damage to safe shutdown systems from real fire hazards and realistic fires. Performance based approaches provide focused resolutions and less plant modifications that provide little or no safety benefit. A high level overview of the analysis and the screening process for each plant area is presented below.

Screen 1, no credited safe shutdown equipment and/or cables in the fire zone. For screen 1, evaluate fire zone boundaries and fire hazards. If the zone has no fire hazards, no further analysis is necessary. If fire hazards exist, postulate a realistic fire based on the hazards, and potential impact of fires on adjacent screen 2 or 3 fire zones.

Screen 2, all performance goals can still be met, even with loss of all credited equipment and/or cables in the fire zone. For screen 2, evaluate fire zone boundaries and fire hazards. If fire hazards exist, postulate a realistic fire based on the hazards, and potential impact of fires on adjacent screen 2 or 3 fire zones. Assure that no single fire could impact redundant safe shutdown systems if fire can propagate into adjacent zones. Identify where performance goals may be impacted due to fire spread. In addition, combine screen 2 fire zones where possible.

Screen 3, one or more performance goal cannot be met due to loss of all credited equipment and/or cables in the fire zone. For screen 3, evaluate fire zone boundaries and fire hazards. If fire hazards exist, postulate a realistic fire based on hazards and potential impact of fires within the subject zone and on adjacent screen 2 or 3 fire zones. Assure that no single fire could impact redundant safe shutdown systems. Identify where performance goals may be impacted due to fire spread.

The following are typical methods for resolving fire impact on safe shutdown systems:

- Removing the fire hazards from the area if feasible;
- Reducing the impact of the hazards (i.e., installing dike around a pump, installing heat shields);
- Protecting the cable trays by installing heat shields;
- Installing or upgrading the detection and or suppression system;
- Provide additional barrier protection;
- Operator manual action if feasible and practical;
- Cable protection, i.e., wrapping raceways should be considered as a last resort.

It is important to note that a deterministic or Performance Based Fire Safe Shutdown Analysis provides an assessment of plant's capability to safely shut down the plant during a postulated fire. However, it does not provide an indication of plant risk; performance of fire PSA provides insights to plant risk, i.e., Core Damage Frequency (CDF), due to fire.

For example, a deterministic and/or Performance Based Fire Safe Shutdown Analysis may show that a plant can achieve safe shutdown during a fire that adversely impacts one train of emergency power system in the plant. While in general this scenario meets the requirements for safe shutdown during that fire, losing one train of emergency power without having the offsite power available will increase plant's risk and CDF by one or sometimes by two orders of magnitude. Simply said, Fire PSA identifies additional vulnerabilities due to fires, and provides insights necessary to minimize the risk of fire to a nuclear power plant.

## 10. RESOURCES AND MANPOWER

In order to effectively perform a Fire Safe Shutdown Analysis (FSSA) using deterministic or performance based approaches, the proper inputs must be provided. This includes general plant arrangement drawings, P&IDs, electrical one-lines and schematics, etc. as well as existing plant databases (e.g., cable and raceway system, plant equipment database, etc.). This information will be used by qualified Mechanical and Electrical engineers to build an accurate FSSD analysis model to allow for evaluation of potential equipment and cable interactions.

Due to the enormous amount of data involved in an FSSA it is recommended to have an analysis software tool that allows the project team to automate the safe shutdown analysis. The software tool would utilize an analysis model, created by the project team, composed of plant systems, equipment and cables, and their physical locations. There are many advantages to using software tools as opposed to performing the analysis manually including efficiency, accuracy, and ease of maintenance of the analysis. This approach enables engineers to analyze each fire zone / fire area with the click of a button and display the analysis model graphically; enabling the analyst to view all components in either an entire layered model or selected portions of the analysis model further assisting them to quickly evaluate the results and postulated resolutions.

Performing an FSSA is a tedious and complex process. Even with qualified engineers using the proper tools and accurate inputs, a complete analysis is extremely time-consuming. At a minimum, this effort, from beginning to end, usually requires a dedicated team of 4 - 6 FTEs and takes in the range of 15,000 - 25,000 man hours.

## 11. CONCLUSION

Performance based fire safe shutdown analysis that focuses on real fire hazards and realistic fire scenarios will provide an accurate and realistic analysis and is cost effective. Protection in the form of physical separation of critical components and cables as well as the effective use of active and passive fire protection systems and features based on these results assures that no single fire could compromise plant safe shutdown goals.

## REFERENCES

- [1] U.S. NUCLEAR REGULATORY COMMISSION, “Background on Fire Protection for Nuclear Power Plants”, (2013) (<https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fire-protection-fs.html>).
- [2] Title 10, Code of Federal Regulations, Appendix A to Part 50, Criterion 3, “Fire Protection”.
- [3] U.S. NUCLEAR REGULATORY COMMISSION Branch Technical Position APCSB 9.5-1, “Guidelines For Fire Protection For Nuclear Power Plants”.
- [4] U.S. Nuclear Regulatory Commission Regulatory Guide 1.75, “Physical Independence of Electrical Systems”
- [5] Title 10, Code of Federal Regulations, Section 50.48, “Fire Protection”.
- [6] Title 10, Code of Federal Regulations, Appendix R to Part 50, “Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979”.
- [7] NATIONAL FIRE PROTECTION ASSOCIATION, NFPA 805, “Performance Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants”, (2001).
- [8] CANADIAN STANDARDS ASSOCIATION, CSA-N293-95/07/12, “Fire Protection for CANDU Nuclear Power Plants”.



## UPDATING OF A SCREENING METHOD FOR ASSESSMENT OF COMPREHENSIVENESS OF DEFENCE IN DEPTH AND AREAS FOR ITS APPLICATIONS

J. MISAK  
UJV Rez, a.s., Nuclear Research Institute  
Husinec-Rez, Czech Republic  
Email: Jozef.Misak@ujv.cz

### Abstract

The paper describes the updated IAEA screening method for assessment of comprehensiveness of defence in depth for both existing as well as new nuclear power plants. In its first part the paper briefly summarizes the original IAEA method developed more than 10 years ago, described in the IAEA Safety Report No. 46 – Assessment of defence in depth for nuclear power plants. Further on, the need for updating the methods is justified making reference to relevant new IAEA Safety Standards and other guidance documents used for updating the method with consideration of new safety requirements and main directions in safety enhancement. Key modifications in the original IAEA method of objective trees are summarized. An example of the updated objective tree is provided and compared with the original tree. In the last part of the paper the potential areas for the use of the method are indicated.

### 1. INTRODUCTION

As reconfirmed by different forums, defence in depth based on multiple barriers and variety of means (provisions) to protect the barriers is and should remain an essential strategy to ensure nuclear safety for both existing and new nuclear power plants (NPPs).

Since many years, defence in depth represents a focal point for IAEA safety related activities. The need for a practical tool aimed at facilitating assessment of comprehensiveness of defence in depth has been recognized by the IAEA at the end of 90-ties with the objective to contribute to more specific understanding of this very general term: all NPPs have physical barriers and means to protect the barriers, while their level of defence in depth can be very different.

Among many IAEA documents related to defence in depth there are two documents with special importance for the present report. One of them is INSAG-12 (update of INSAG-3) - Basic Safety Principles for NPPs, published in 1999 [1], introducing the concept of basic safety principles as necessary conditions for ensuring plant safety, and Safety Report No. 46 - Assessment of defence in depth for NPPs, published in 2005 [2], which describes a screening method for assessing comprehensiveness of the defence in depth capabilities of a NPP (mainly of an existing plant), including all necessary measures taken to ensure safety. Since development of Safety Report No. 46 significant enhancement in international safety requirements including also enhancement of defence in depth took place, in particular after the Fukushima accident. For further use of the Safety Report No. 46 it is therefore necessary to update the report taking into account all new safety developments and also to improve user friendliness of the method based on experience from its previous applications.

In 2016, the Czech electric utility CEZ a.s. decided to update the method of objective trees with due consideration of all new safety requirements with the aim to use the method in next periodic safety reviews of NPPs in the Czech Republic. The updated methodology should provide a tool for periodic safety assessment of operating NPPs in the scope defined in the IAEA Specific Safety Guide SSG-25 – Periodic Safety Review for Nuclear Power Plants [3].

The paper describes the updated screening method developed in response to the CEZ decision. In its first part the paper briefly summarizes the original IAEA method as described in Safety Report No. 46. Further on, the need for updating the method is justified making reference to the relevant new IAEA Safety Standards and other international guidance documents. Key modifications in the original IAEA method of objective trees are summarized. An example of the updated objective tree is provided. It is obvious that the use of the method can be much broader than just to be a tool for performing the periodic safety review. In the last part of the paper such potential areas for the use of the method are presented.

The updated method is intended to be predominantly used by the operating organization, and therefore the provisions for ensuring safety are focused on those which can be managed by the operating organization.

It is assumed that the IAEA can provide a forum for further improvement of the method and its broader distribution and utilization by the Member States.

## 2. BRIEF DESCRIPTION OF THE METHOD OF OBJECTIVE TREES

IAEA Safety Report No. 46 describes the reference approach for checking the completeness and quality of implementation of the concept of defence in depth in a systematic way. The bases for the approach were as follows:

- Safety should be ensured by implementing safety provisions at all 5 levels of defence in depth at any time;
- Each of the levels should be individually robust;
- Each level has its relevant safety objectives ensured by corresponding integrity of the physical barriers;
- For maintaining integrity of the barriers, the fundamental safety functions (FSFs) and more detailed (derived) safety functions (SFs) should be performed;
- SFs can be challenged by a number of mechanisms affecting their performance;
- To prevent mechanisms affecting the SFs, safety provisions of different kinds should be implemented;
- Provisions implemented at different levels of defence should be reasonably independent.

The concept of defence in depth has been often oversimplified and misinterpreted just as a set of physical barriers, whose integrity is ensured by safety provisions as the plant systems (hardware provisions) implemented at various levels of defence. However, comprehensive measures to ensure effectiveness of the barriers against releases of radioactive substances should include much broader variety of safety provisions: organizational, behavioural and design measures, namely inherent safety characteristics; safety margins; active and passive systems; operating procedures and operator actions; human factors and other organizational measures; safety culture aspects. It is important to underline that although plant technological systems are very important, they are not the only components of defence in depth.

The screening approach described in the IAEA Safety Report No. 46 uses so called objective trees (Fig. 1) for screening the availability safety provisions at five levels of defence. The top down approach has been used for the development of objective trees, i.e. from stating the objectives and relevant SFs for each level of defence, through the challenges to performance of these SFs composed of various mechanisms affecting the performance, up to the provisions which may be implemented to prevent challenges to SFs to take place. The provisions are aimed at preventing the mechanisms and challenges to SFs to take place so that to ensure integrity of physical barriers and achieving safety objectives at each level of defence.

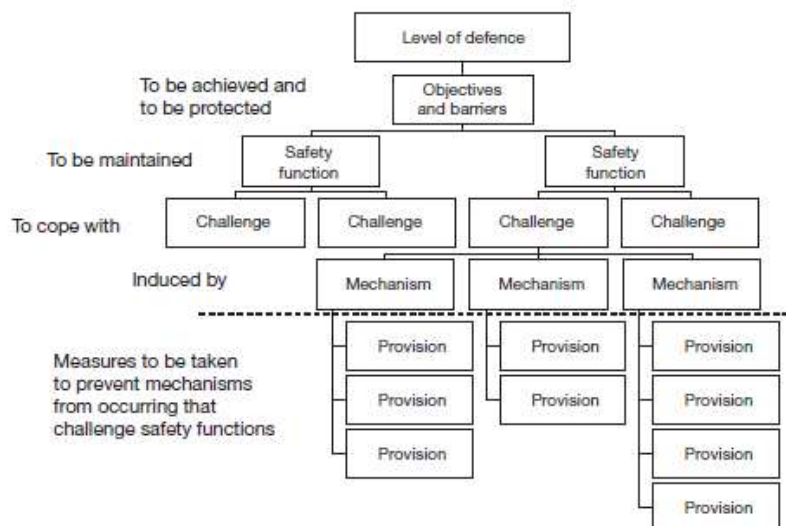


FIG. 1. Illustrative structure of the objective tree at each level of defence.

Graphical depiction of links between safety objectives and safety provisions in the form of an objective tree helps to identify weaknesses in defence in depth and supports the questioning attitude essential for nuclear safety. Screening by means of objective trees should be understood not only as a comprehensive tool for assessment, but also as a way of thinking on nuclear safety in very broad circumstances.

Nevertheless, it should be mentioned that the approach described in Safety Report No. 46 does not include any quantification of the extent of defence in depth nor prioritization of the provisions of defence. The approach is intended only for screening, i.e. for identification of both the strengths and weaknesses and for identification which additional provisions could be considered. There are no criteria on what is considered a sufficient level of implementation of individual provisions. The level of detail and completeness of evaluation are at the discretion of every user of the approach.

Use of the method for checking comprehensiveness of defence in depth is done in a reverse way compared to development of the method, it means by bottom up of screening of individual provisions, including the following steps:

- Comparison of provisions specified in the objective trees with capabilities of the plant;
- Judgment of the level of implementation of each provision in siting, design, construction, commissioning and operation;
- Consideration of optional provisions and judgment whether an absence of a provision leads to the weakness in defence in depth;
- Judgment whether a mechanism can be considered as prevented to occur;
- Judgment whether a challenge can be considered as prevented to affect fulfillment of a safety function.

In summary, the objective trees in the IAEA Safety Report No. 46 included 95 different challenges (some of them applicable for several levels), 254 different mechanisms and 941 different provisions. It will be shown further in the paper that updating the Safety Report No. 46 will lead to significantly increased number of items in the objective trees.

### 3. THE NEED FOR UPDATING THE METHOD FOR ASSESSMENT OF COMPREHENSIVENESS OF DEFENCE IN DEPTH

The Fukushima accident demonstrated importance of comprehensive implementation of defence in depth and reactivated interest in various methods for its assessment. There was the IAEA International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety held in Vienna, 21-24 October 2013 [4]. Among conclusions of the conference there was a confirmation of importance and value of defence in depth for both existing and new plants. Further development of the tools based on the methodology described in the Safety Report No. 46 was recommended as a means for ensuring that defence in depth safety provisions are comprehensive enough. In the conclusions of the conference a number of recommendations were presented with the objective of further strengthening the defence in depth. Among the recommendations there was also the need to take into account the most recent IAEA Safety Standards and maintenance of compliance with these Standards by periodic safety reviews over the entire life of the plants. The need for further development of guidance documents and tools for assessment of required new features of defence in depth was also included in the recommendations.

Following the conference, there were several meetings organized by the IAEA partially addressing the defence in depth, but no specific actions on updating of Safety Report 46 were taken up to now.

In 2016, the Czech utility CEZ a.s. decided to use the method of objective trees described in IAEA Safety Report No. 46 for assessment of the level of defence in depth in next periodic safety reviews of Czech NPPs. It was clear that the original objective trees developed more than 10 years ago needs updating in order to reflect all relevant new safety requirements as well as to improve user friendliness of the method. The updating has had also to reflect on-going updating of the Czech nuclear legislation.

It was clear from the beginning that the update will significantly influence the original scope and level of detail of the screening method described in IAEA Safety Report No. 46. For demonstration of the needed scope of updating, the key enhancements to be incorporated based on IAEA Safety Requirements are summarized below.

Main areas of strengthening in the IAEA Safety Requirements for siting include the following items [5]:

- The need to evaluate frequency and severity of external natural and human induced events, with consideration of potential combination of events;
- Establishing the design basis hazard level considering frequency and severity of events with associated uncertainties, considering long term historical data;
- Assessment of the feasibility of implementation of emergency plans, considering potential mutual effects among multiple nuclear and other facilities at one site;

- Periodic review of site specific hazards (every 10 years or shorter in case of significant changes in hazards) with evaluation of implications.

Main areas of strengthening in the updated Safety Requirements for design [6] are as follows:

- Consideration in the plant design of all plant states up to design extension conditions including severe accidents in the plant design envelope;
- Limitation of radiological consequences of accident conditions: no off-site measures needed for any design basis accidents, off-site measures limited in area and time for severe accidents, which are not practically eliminated;
- Strengthening the plant design basis by consideration of external hazards with implementation of sufficient margins;
- Practical elimination of unacceptable radiological consequences (elimination of early or large radioactive releases) to the public and the environment (elimination or minimization of site contamination);
- Reinforcement of the independence of defence in depth provisions, in particular between levels 3 and 4 – implementation of dedicated safety provisions for design extension conditions;
- Stressing the need for margins to avoid cliff edge effects;
- For items that ultimately prevent large or early releases more margins are required, also for external hazards more severe than those selected for the design basis;
- In a multiunit site, each plant unit to have its own safety systems and safety features for design extension conditions, but considering interconnections between the units for enhancement of safety;
- Reinforced capabilities for heat transfer to the UHS; alternative heat sink or different heat transport route is required for conditions generated by beyond design basis external events;
- Strengthening design of the control room with margins against natural hazards exceeding the design basis;
- Implementation of features to enable the use (e.g. hook-up) of non-permanent equipment;
- Reinforced capabilities for power supply in design extension conditions; independent and separated alternate power sources for station black-out accidents, with continuity of power for monitoring;
- Emergency response facilities capable to withstand conditions generated by accidents and hazards;
- Additional measures for spent fuel pool (SFP) monitoring (temperature, water level, activity, water chemistry), cooling and maintaining inventory including use of non-permanent equipment (in order to practically eliminate severe accidents).

Main areas of strengthening in the updated Safety Requirements for operation [7] are as follows:

- Periodic safety review to consider national and international experience, national and international standards and to cover site related aspects;
- Implementing corrective actions and reasonably practicable modifications to reduce likelihood and potential consequences of accidents;
- Strengthening means of communication, availability of information in emergency response facilities and locations with regular testing, validation and training on emergency preparedness;
- Strengthening accident management, degraded regional infrastructure and adverse working conditions, ensuring safe location and maintenance of non-permanent equipment;
- Periodical review and revisions of accident management programme;
- For multiunit sites considering concurrent accidents affecting all units with verification of availability of experienced personnel, equipment, supplies and external support;
- Considering contingency measures such as an alternative supply of cooling water and an alternative supply of electrical power to mitigate the consequences of accidents;
- Ensuring safe and accessible storage of temporary equipment;
- Appropriate competences, systems and technical support, with adequate validation, testing and exercises of accident management, including long-term actions;
- Feedback from operating experience to include emergency responses and lessons learned from other industries;
- Establishing maintenance programmes, training and exercises for non-permanent equipment.

In addition to the IAEA Safety Requirements, other documents taken into account in updating the screening method of the objective trees include:

- IAEA Report on Human and Organization Factors in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant [8],
- IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant [9],
- Post-Fukushima updating of WENRA reference levels for existing reactors [10],
- Recommendations from the post-Fukushima stress tests, in particular from the EU stress tests [11, 12],
- OECD/NEA lessons learned from Fukushima accident published in 2016 in document [13].

All these reference documents in combination with accumulated experience from the previous use of the method were used in systematic updating of all objective trees included in Safety Report No. 46, so that all new safety requirements are now adequately covered.

#### 4. COMPARISON OF OBJECTIVE TREES IN ORIGINAL IAEA METHODOLOGY AND NEWLY DEVELOPED OBJECTIVE TREES

It is clear that the most significant changes in the objective trees resulted from the new safety requirements as well as from the accumulated experience from previous applications of the method. However, it was also necessary to improve user friendliness of the original method. Development of objective trees in Safety Report No. 46 was significantly limited by available hardware and software computational means at the time of the development. The software system had limited flexibility, size of the boxes in the objective trees did not allow to insert sufficiently self-understandable text of provisions, etc. The whole set of objective trees remained just in the paper form, not allowing any further development and improvements. Rigid structure of the objective trees with no flexibility was the main obstacle is broader use of the method.

Old objective trees were developed in Microsoft PowerPoint 97-2003 software. New objective trees are developed in two formats. One of the formats are standard excel tables, easy to be updated and also providing certain visualization of the objective trees. The second format has a typical shape of a tree produced by the Microsoft Office Visio 2007 software tool. Challenges, mechanisms and provisions are more specifically and therefore more understandably formulated. A specific set of provisions is associated with each individual mechanism differently from the past when the same more general provisions were associated with several mechanisms at the same time. Currently available software also allows adding to individual items in the objective trees various attributes of the items as appropriate, such as numbering of provisions or their linking to more specific safety requirements. The available software offers a reasonably simple transfer of an objective tree developed in an excel table into a Microsoft Visio figure and vice versa.

The overall effect of updating of objective trees can be illustrated by some numbers showing that in comparison with Safety Report No. 46 the number of challenges included in the objective trees increased from 95 to 128, number of mechanisms from 254 to 347 and number of indicated provisions to prevent mechanisms challenging the safety functions was nearly doubled, with increase from 941 to 1797.

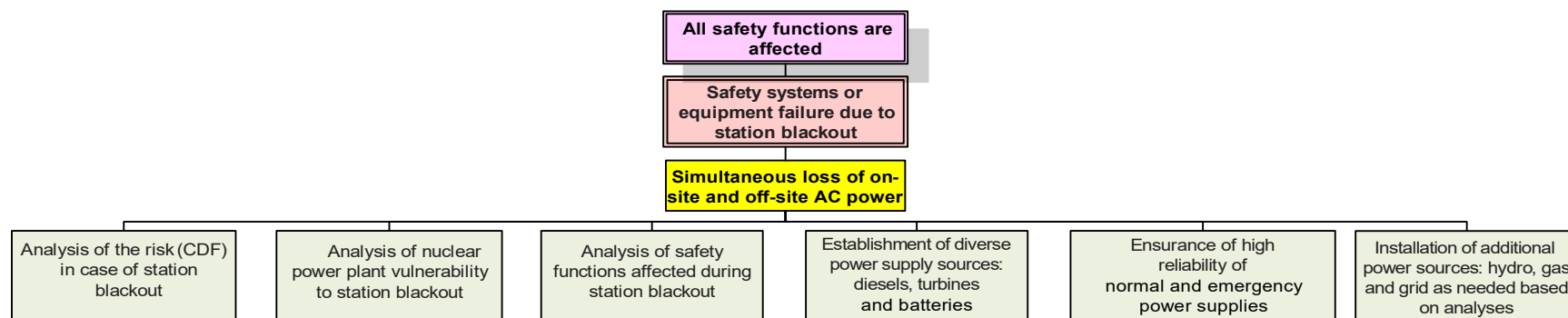


FIG. 2. Objective tree corresponding to the safety principle “Station blackout” in IAEA Safety Report No. 46.

Safety principle - Challenge - text	Mechanism - text	Provision 1	Provision 2	Provision 3	Provision 4	Provision 5	Provision 6	Provision 7	Provision 8	Provision 9	
Station blackout	Safety systems or equipment unavailable due to station blackout	Plant vulnerability to SBO large or unknown	Overview of vulnerabilities under different plant conditions	Assessment of time windows for connection of alternative sources	Assessment of the risk and implications of the RCP seal damage	Identification of means for enhancing capability to withstand SBO					
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO coping capability inadequate	Capability of the turbine island to handle large load rejection	Multiple grid connections at different voltage levels including secure connections	Nearby hydro or a gas power plant, having a black start capability	Alternate AC power source designed for anticipated external events	Nearby hydro or a gas power plant, having a black start capability	Dedicated small AC power sources for specific functions such as battery charging	Mobile diesel / gas turbine generators (medium or low voltage)	Trailer mounted fuel tanks, hoses, fuel transfer pumps, and cable spools	High capacity station batteries (e.g. 12-24 hours) or additional spare battery systems
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions ineffective due to unavailability of information about	Assessment of vulnerabilities of key plant instrumentation under SBO conditions	Procedures for extrapolation of data from remaining instrumentation	Use of dedicated sources of power and coolant with their own instrumentation	Assessment of accessibility of field measurement points	Use of portable self-powered measuring equipment				
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions unavailable due to damage of equipment or infrastructure	Storage of equipment in spaces resistant against earthquakes and flooding	Storage of equipment in light structures minimizing damage of stored equipment	Storage of equipment in different places minimizing risk of damage by same event	Installing water-proof doors sealing the electrical compartments	Sealing external cable raceways to prevent water intrusion	Modifying the plant for connecting alternative sources of power and coolant	Debris removal machines stored in protected areas	Dewatering pumps to remove water from areas requiring access	
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions ineffective due to lack of external support	Provisions for coordination, accepting, deploying off-site resources	Staging areas to receive equipment from off-site resources	Coordination agreements with potential off-site supports	Establishment of regional centers with technical and human resources	Database with external resources capable of supporting plant needs				
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions ineffective due to poor staff performance	Development of accident management strategies for SBO conditions	Development of procedures for actions needed for extended SBO	Improved procedures for restoring the offsite power or connection nearby units	Load shedding procedures to extend battery discharge time	Procedures to connect and power specific buses, operate switches and breakers	Validation of procedures for accomplishment within expected times under harsh conditions	Training of personnel for manual actions needed in case of SBO	Drills that encompass full sequences, including connections of non-permanent equipment	Portable battery or diesel powered lights
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions ineffective due to short mission time	Analysis of limitation of mission time by availability of consumables	Increased on-site availability of consumables (oil, lubrication)	Provisions to replenish consumables for indefinite mission time						

FIG. 3. Excel table corresponding to the objective tree for the safety principle “Station blackout”.

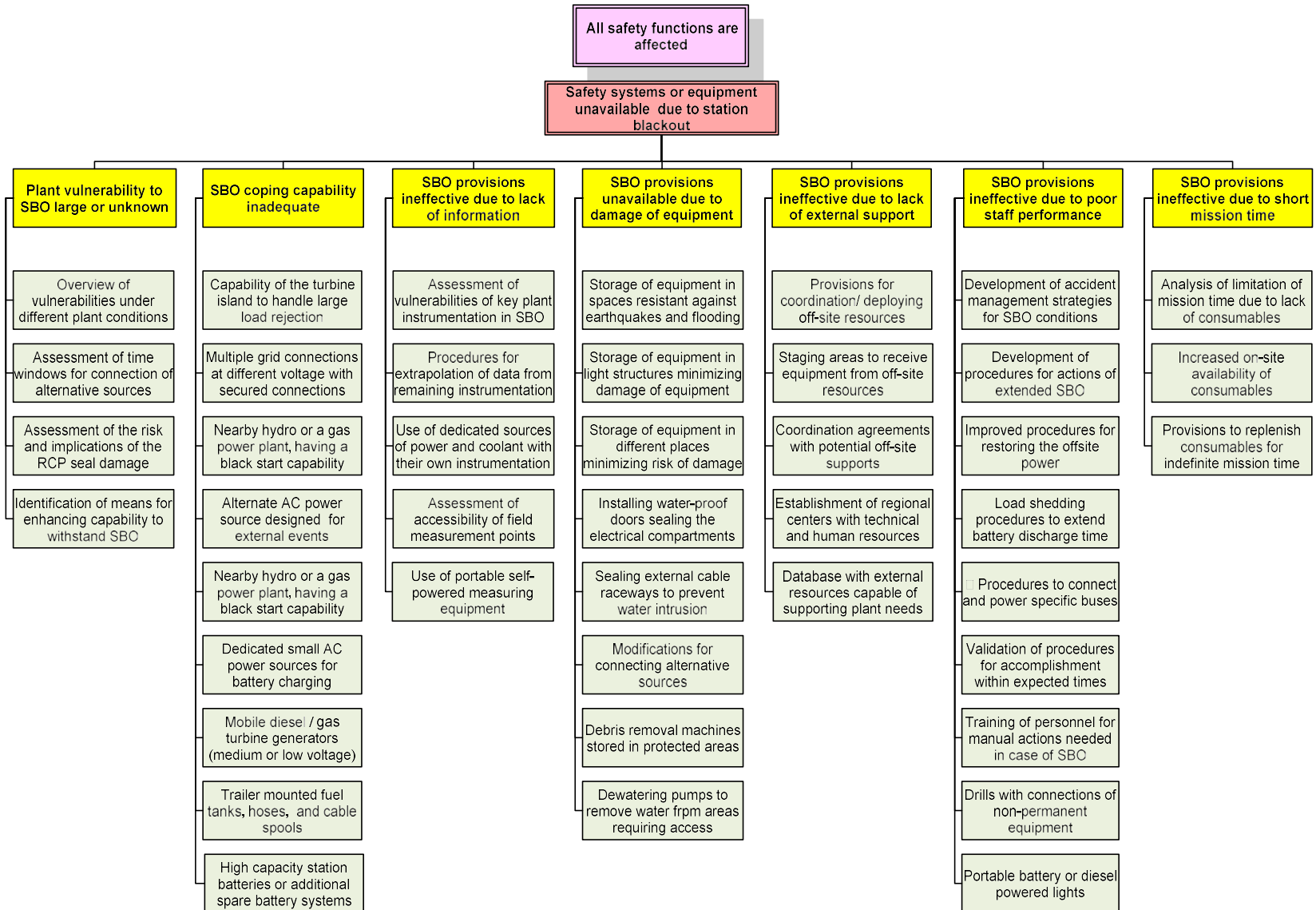


FIG. 4. Updated objective tree corresponding to the safety principle "Station blackout".



All objective trees from the original Safety Report No. 46 were transferred into a new format in excel sheets, thus allowing improving and updating the objective trees taking into account information from various reference sources in the present report. Practically all objective trees were expanded to provide adequate level of details and to reflect new requirements. Some new objective trees were added to reflect completely new requirements, for example the tree for assessment of practical elimination of early or large radioactive releases. The objective trees are at present being verified by CEZ experts in various fields of nuclear safety. It would be very appropriate to involve the IAEA experts in the process thus to improve overall quality and applicability of the method.

The changes discussed above are illustrated in the figures below. Fig. 2 shows one of the “old” objective trees corresponding to the safety principle “Station blackout”, while Fig. 3 shows the equivalent updated excel table and Fig. 4 the new objective tree corresponding to the same safety principle.

These examples demonstrate significant technical enhancements as well as improvements in user friendliness of the method thus providing better conditions for broader use of the method. Similar modifications, although not necessarily so significant, were implemented in all objective trees of IAEA Safety Report No. 46.

## 5. POTENTIAL APPLICATIONS OF THE METHOD

There were examples of application of the objective trees approach in the past and renewed interest in the approach is observed after the Fukushima Daiichi accident. The applications until now demonstrated that the screening method is based on a sound concept and can be effectively used by NPPs, that it helps identifying missing or weak provisions, that understanding of importance of provisions and interactions among provisions/mechanisms by using the method is improved because of complexity and visualization in the form of objective trees, and that self-assessment mode of the review contributes to the safety culture-questioning attitude of the reviewers. The updating of the method by incorporating all new safety requirements and improvements of user friendliness of the method provides a good basis for broader use of the method.

Following applications of the methods may be considered:

- Bottom-up qualitative assessment of availability of identified provisions in any specific NPP, combined with an expert judgments of sufficiency of provisions for preventing challenges to safety functions to take place;
- Use of selected lists of provisions as reminders for verification of availability of necessary measures in specific safety reviews, including IAEA safety review missions;
- Verification of comprehensiveness of safety assessment criteria in periodic safety reviews by comparing the criteria with the list of provisions identified in the objective trees;
- Assessment of severity of deficiencies in safety level identified in periodic safety review by indicating the challenges to performance of safety functions, levels of defence in depth affected and available provisions possibly compensating the deficiencies;
- Use of identified gaps in comprehensiveness of defence in depth provisions for identification of measures for safety upgrading of the NPPs;
- Demonstration of progress in safety upgrading of a given NPP by increasing the number and level of implementation of different safety provisions;
- Demonstration of a comprehensive consideration of defence in depth in the plant Safety Analysis Reports;
- Use the objective trees for training of NPP staff in comprehensive consideration of defence in depth in their day by day operations.

## 6. CONCLUSIONS

The IAEA Safety Report No. 46 provided a feasible framework for assessment of comprehensiveness of implementation of defence in depth provisions, but due to relatively long time since its publication it needed updating and improvements of its user friendliness. The work described in the paper responded to the needs for overall improvements of the whole methodology for screening comprehensiveness of the defence in depth at all levels of defence.



Updating of the challenges, mechanism and provisions in the objective trees took into account strengthening of international and national safety requirements and lessons learned, in particular those reflected in the IAEA Safety Standards, WENRA reference levels and safety objectives, OECD/NEA recommendations for strengthening of defence in depth, and any other post-Fukushima lessons learned, including results of the European and other stress tests.

In the updated method, the original basis of the approach by means of systematic assessment of provisions available to prevent mechanisms and challenges affecting safety functions potentially leading to the damage of the barriers against releases of radioactivity was maintained. The way of illustrating the links between safety objectives, barriers, safety functions, challenges, mechanisms and safety provisions by graphically presented objective trees remained unchanged, providing additional possibility of presenting objective trees in the format of excel sheets easy to be updated.

The updating also included adjustment of the balance between individual objective trees, as well as checking and improvements of the formulation of the items in the objective trees to ensure their validity, correctness and clarity of the formulations.

The user friendliness of the method was improved by developing a computerized version of objective trees, with sufficient flexibility for further corrections and modifications, with a possibility to associate various attributes to individual items of the objective trees, with a possibility of easy updating the objective trees.

Czech electric utility CEZ a.s., offers the method for further international adaptation and broader use for assessment. IAEA is invited to provide the framework for broader international use of the method.

## ACKNOWLEDGEMENTS

The paper has been prepared in close cooperation with the staff of engineering department of the Czech electric utility CEZ a.s.

## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1, INSAG-12, IAEA, Vienna (1999).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of defence in depth for nuclear power plants, Safety Report Series No. 46, IAEA, Vienna (2005).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review for Nuclear Power Plants, IAEA-SSG-25, IAEA, Vienna (2013).
- [4] IAEA International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth – Advances and Challenges for Nuclear Installation Safety held in Vienna, 21-24 October 2013.
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, Specific Safety Requirements, NS-R-3, Rev. 1, IAEA, Vienna (2016).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Specific Safety Requirements, SSR-2/1 Rev. 1, IAEA, Vienna (2016).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, Specific Safety Requirements, SSR-2/2, Rev. 1, IAEA, Vienna (2016).
- [8] IAEA Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, International Experts Meeting, 21-24 May 2013, Vienna, Austria.
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, IAEA, Vienna (2013).
- [10] WENRA Safety Reference Levels for Existing Reactors – Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident, September 2014.
- [11] Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Overview and Conclusions, Presented to ENSREG by the Peer Review Board, April 2012.
- [12] Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Compilation of Recommendations and Suggestions from the Review of the European Stress Tests, Presented to ENSREG by the Peer Review Board, July 2012.

- [13] Implementation of Defence in Depth at Nuclear Power Plants - Lessons Learnt from the Fukushima Daiichi Accident, OECD/ NEA No. 7248, 2016.



# CHALLENGES IN SEVERE ACCIDENT MANAGEMENT

**Chairperson**

**P. DE GELDER**

Belgium



## IN VESSEL MELT RETENTION STRATEGY - STATUS OF WORK FOR VVER 1000 UNITS APPLICATIONS

J. ZDAREK  
UJV Rez a.s., Czech Republic

### Abstract

For NPP units in operation the IVMR strategy was applied only for small power reactors such as VVER 440 MW. For new generation units with large power this strategy was first applied on WEC AP 1000. The same strategy is now applied also for new generation design at Korea and China up to 1400 MW. For existing units with higher power above 600 MW it was for long time assumed that the IVMR strategy is not possible. This approach is slowly changing. At present EC project HORIZON 2020 IVMR is continuing to provide more findings in this direction. Also recent IAEA TM at SNERDI Shanghai clearly identified significant growth of interest about this strategy. The IAEA will shortly issue TECDOC from this meeting and respective findings.

Our UJV Rez Institute is responsible for TASK 4 above mention HORIZON IVMR project with clear goal to build large scale experiment providing external RPV cooling evaluation for SA core melt heat flux distribution. Building of the large scale experiment is supported with small scale experiments. In proposed presentation we would like to present status of small scale experiment results, analytical assessment and status of large scale experiment facility.

### 1. INTRODUCTION

Key conclusions from several recent IAEA TMs are of key importance for strategy of our work:

“It has been highlighted during the IEM and confirmed at the TM that the R&D area regarding in-vessel melt retention and ex-vessel corium cooling/stabilization is one of the highest priority areas, and that more phenomenological knowledge should be gained for the strategic and technological development of the countermeasures to cope with Water Cooled Reactors severe accidents”.

With respect to the In Vessel Melt Retention Strategy is necessary realise following IAEA statement:

“It is commonly recognized that the IVMR strategy achieved by external reactor vessel cooling and/or in-vessel flooding is one of the most effective measures to prevent the progression of severe accidents at water-cooled reactors. Several operating nuclear power reactors (e.g. VVER-440, VVER-1000, Indian PHWR), or new ones (e.g. AP1000, APR1400, CAP1400, KERENA, HPR1000, ACP 1000) use IVMR strategy and have dedicated systems”.

As our presentation will provide status of our work on small and large scale experiment is very important to repeat key conclusions on this topic from the recent IAEA TM at SNERDI Shanghai: Technical Session-1B: External Reactor Vessel Cooling.

Two (2) presentations were given on new large experimental facilities, which are designed, based on the lessons learned from small- and large-scale facilities, to measure critical heat flux (CHF) at the outer surface of the RV lower head under more realistic configurations and flow conditions.

One of the two success criteria of the IVMR strategy is ‘thermal criterion’ to make sure the heat flux from in-vessel molten pool is less than the CHF at the outer surface of the RPV lower head that is determined by external cooling conditions with water flooded in the reactor cavity.

Main factors affecting the CHF include: 1) stability of the natural circulation; 2) geometry of the flow path, 3) surface conditions of RV LH, 4) water subcooling at the inlet of the flow path.

Full height experimental facilities are necessary for validation data, and they should be designed as closely as possible to the real conditions.

Based on the results from small-scale experiments, the most effective measures to increase CHF might be optimization of the flow path and the outer RPV surface conditions of the lower head.

Small scale experiments – Status of Work

Design

It is important to realize size of the small scale experiment, cooling channel configuration and also position of thermocouple used for identification of the boiling crisis. Those data are seen from following two figures.

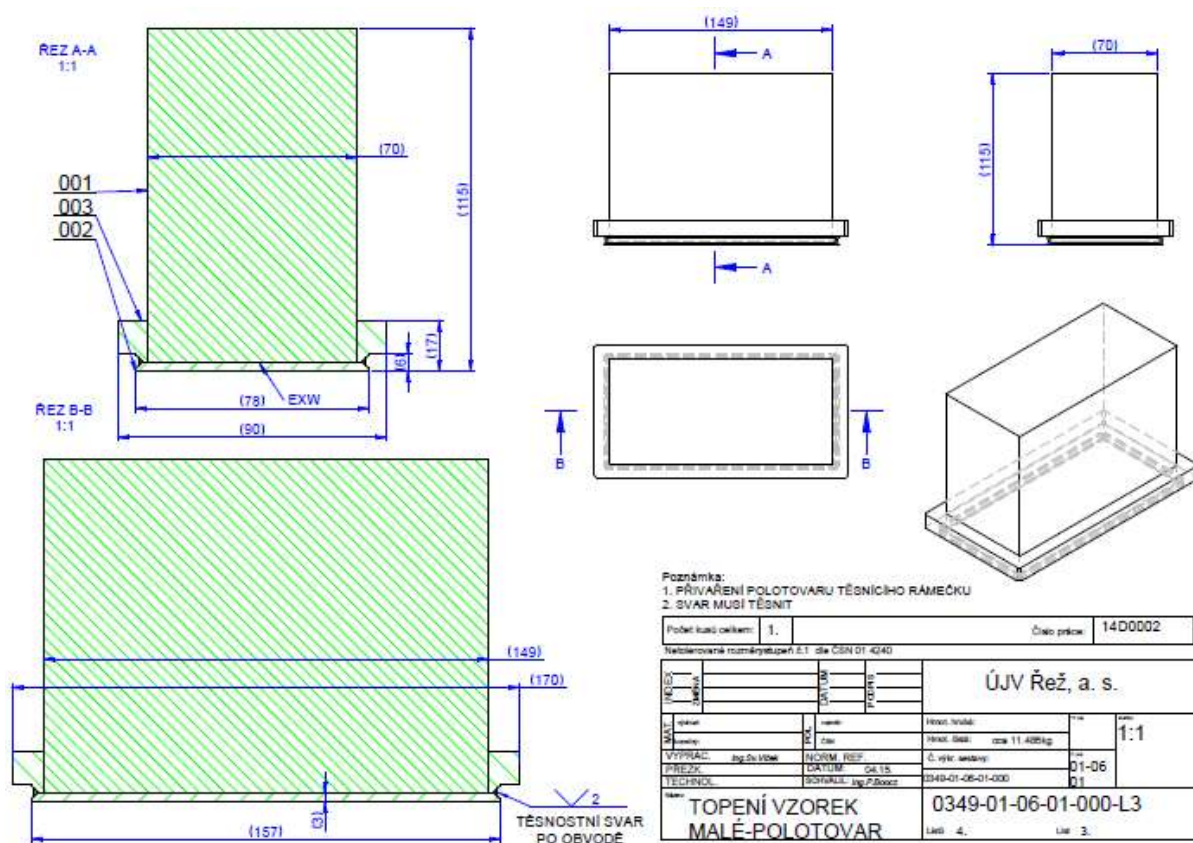


FIG. 1. Dimension of small scale sample. Steel surface explosively welded with Cu bloc.

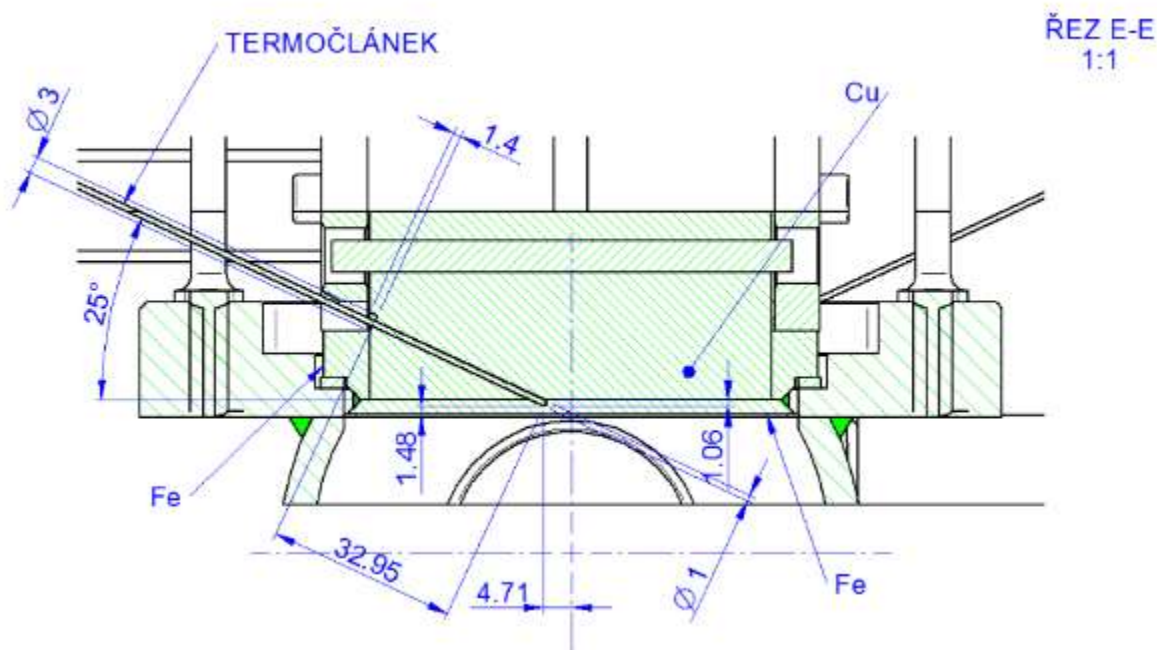


FIG. 2. Detail position of the thermocouple used for boiling crisis identification.

Very recently we have decided to install more thermocouples near the steel surface in order to measure more temperature profile data to get better estimation of the Heat Flux. Tests are in progress and if results will be helpful we will consider similar measurement in the large scale test blocs.

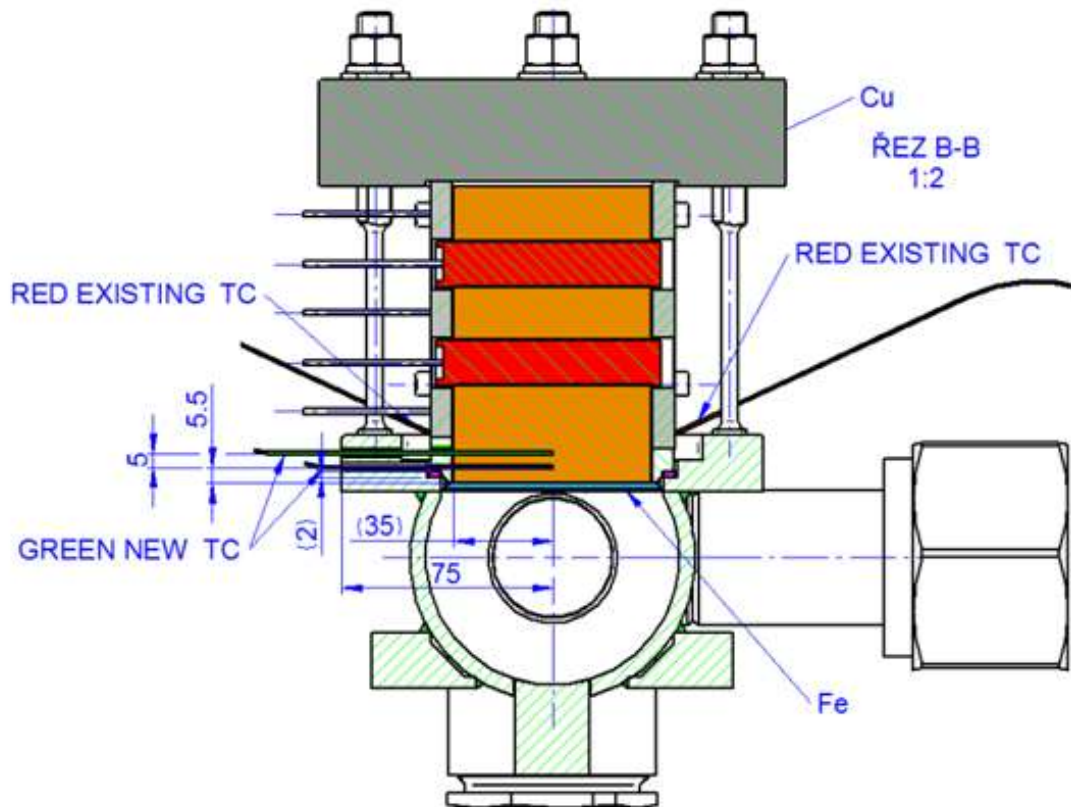


FIG. 3. New thermocouple positions in the small scale sample.



FIG. 4. Test sample with heating patrons and thermocouple position.



### 1.1. Summary of results and lessons learned

Over 130 experiments were performed on the small scale facility. Without technical lessons learned from the design and performance of the small scale tests it will be extremely difficult to build the large scale facility. Most important knowledge is fully verified explosive welding technology between the steel plate and Cu bloc segments. Latest, additional temperature measurement is also very important. Our research effort is also focused on effect of the steel surface. Great design advantage of the VVER 1000 units is an access to the RPV cavity with possibility to identify status of the RPV surface after several years of operation and possibility to apply justified surface treatment on the critical RPV surface where we need to assure most effective heat flux removal. Based on that knowledge and feasibility to do that in real configuration of operated reactor we have decided to apply most effective surface improvement. With great support from the ARL/PSU we are until today testing the “cold spray” technology with different composition of particles. On top of it we are testing our own surface treatment technology. Summary of all results obtained until now are presented on Fig.5. Tests on small scale facility will continue in order to decide representative test matrix on the large scale experimental facility.

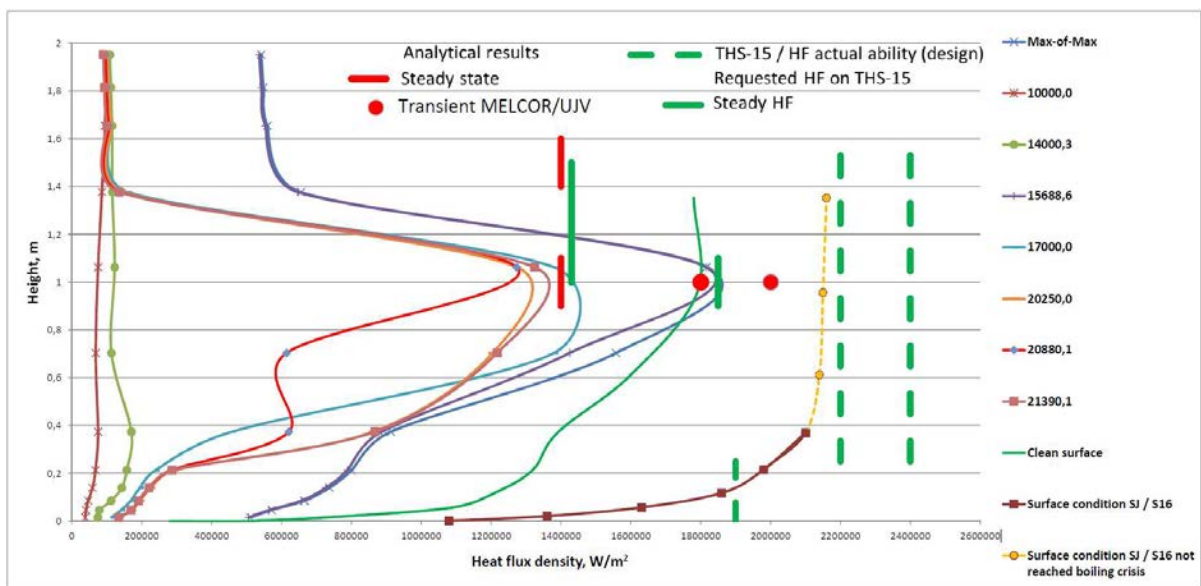


FIG. 5. Summary of experimental results with different surface treatment in comparison with MELCOR/UJV calculation results.

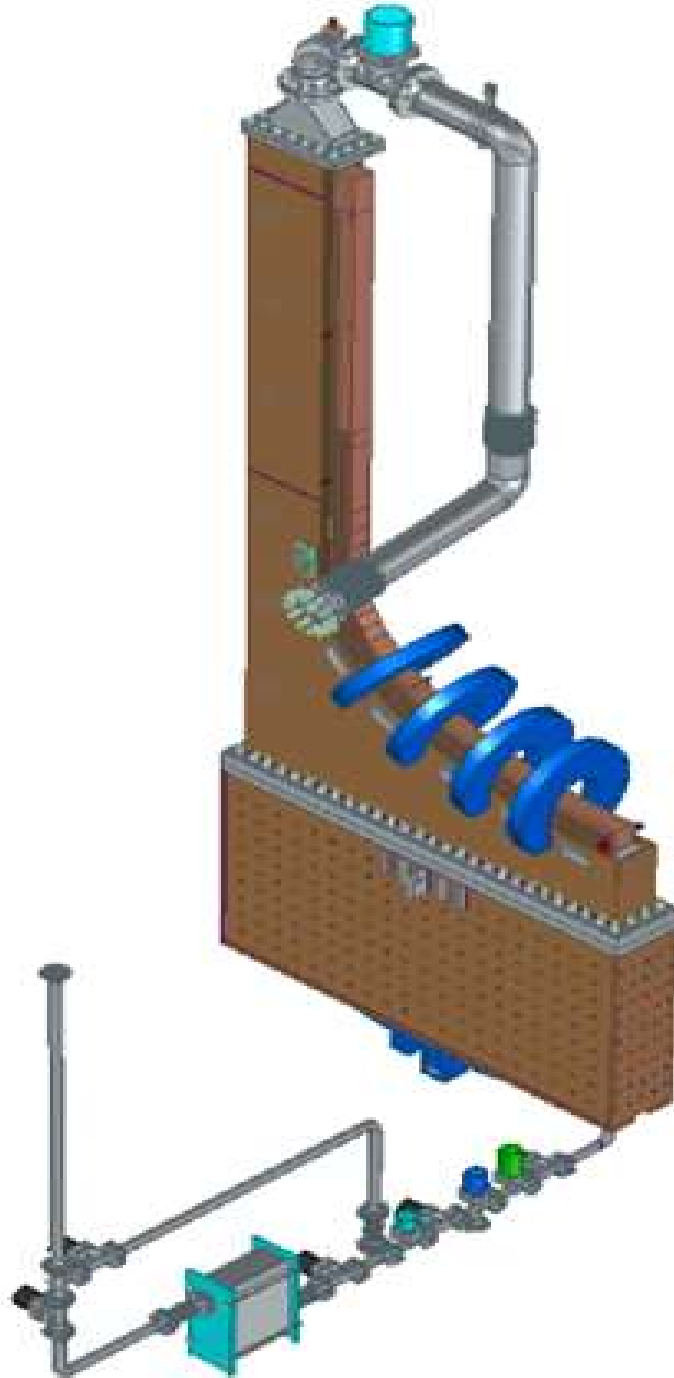
### 1.2. Summary of small scale test results

Design knowledge and experience is of great value for large scale facility. Results of tests, with significant number performed, clearly shows improvement to be reached with respect to the heat flux removal. It is important to stress that tested technology has to be applied on existing VVER 1000 design under operation. Technology applied must not affect performance of the NDE tests from the outside RPV surface and also cannot influence the RPV integrity and overall safety requirements.

## 2. LARGE SCALE EXPERIMENTAL FACILITY THS-15

### 2.1. Principal Design

Fig.6 is providing basic design of the cooling channel. Most important are dimensions between the RPV cavity floor and wall between steel surface simulating shapes of the RPV lower head and cylindrical wall. Also input of the cooling water through the cavity floor and steam release dimension corresponding to the available space between the support ring and the RPV wall. Inside the cooling channel is also possible to install deflector steel plate.



*FIG. 6. Cooling channel basic design.*

Overall design of the large scale test facility THS-15 is seen on Fig.7. To meet all design requirements in existing building it was necessary to plan significant civil reconstruction including drilling holes to existing floor, new installation of electrical cables, and many other activities.

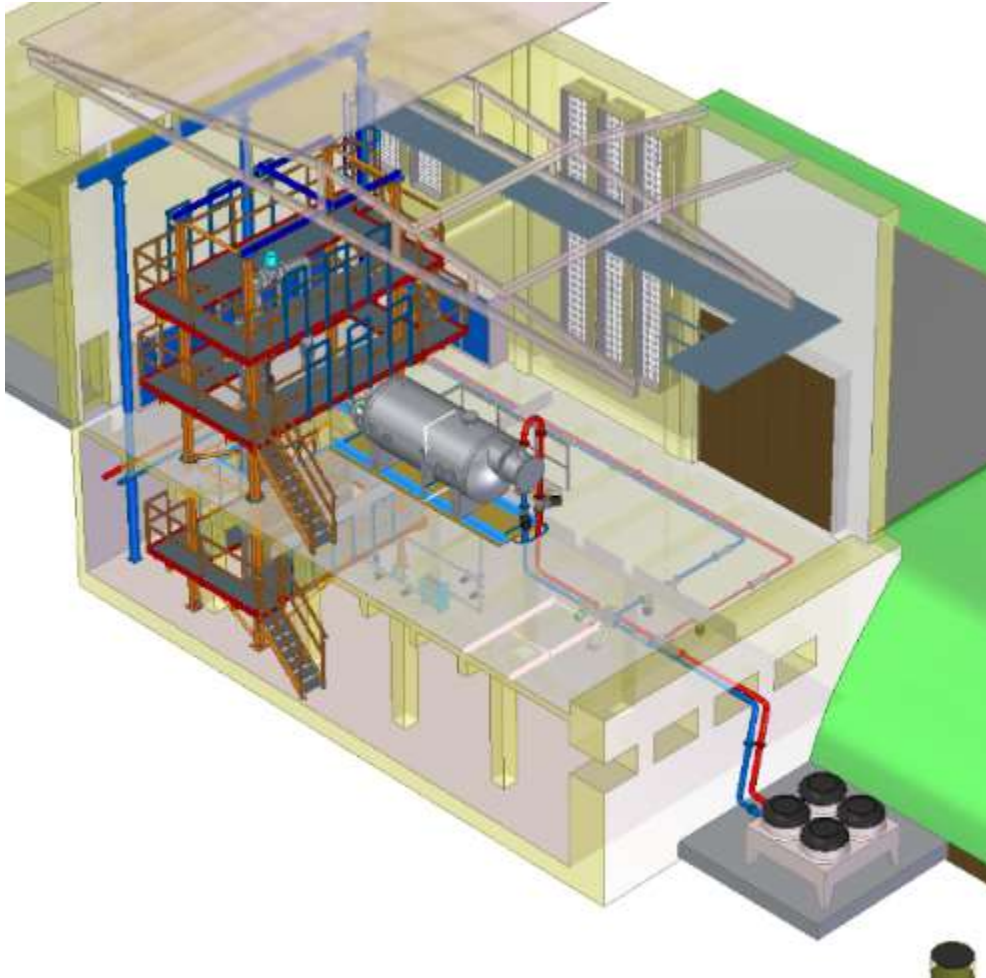


FIG. 7. Large scale test facility THS-15 principal design drawing.

## 2.2. Status of Civil Construction

Installation of new electrical cables started civil construction work. Detail is seen on Fig. 8.



FIG. 8. New electrical cables installation.

In December 2016 all civil construction work was finished. On Fig. 9 is seen drilled rectangular opening in the floor for installation of cooling channel with support construction.





*FIG. 9. Photo of rectangular floor opening for the cooling channel installation.*

### **2.3. Status of Manufacturing of Key Components**

In February 2017 will be finished segments of all heater blocs with drilling of more than 1300 heating patrons. Drilled holes in heaters segments are seen on Fig. 10.



*FIG. 10. Heater segments with drilled holes.*

In January 2017 we plan to install condenser and other key components. Design of the cooling channel was delayed due to new integrity calculations and also due to thorough welding qualification process and tests. Manufacturing will start in February 2017.

### **2.4. Remaining schedule for large scale test facility build up**

Original schedule to finish large scale test facility THS-15 in order to start final set up for the test matrix is planned on April 2017. We are significantly ahead of schedule with respect to the HORIZON 2020 IVMR TASK 4 schedule. However, our Czech Utility would like to make decision about the IVMR application for our VVER 1000 Units at Temelin site in November 2017 and till that time there is a need to have at least basic large

scale tests results. As you could see our schedule to meet this deadline is very hard. Our team is performing with highest responsibility to meet the above deadline with minimum delay.

### 3. ANALYTICAL SUPPORT

Numerical simulation results of corium pool behavior at RPV bottom were performed. Thermal loads on RPV were defined based on obtained results. Calculations were performed using Russian SOCRAT code, HEFEST-ULR code (developed in NRC “Kurchatov Institute”) and west-European ASTEC code. Numerical domain for IVMR task is shown in figure 11 for each code. Taking into account performed analysis of possible corium pool configurations the following configurations were considered: two-layer model (direct and inverse stratification) and three-layer model.

Results of time-highest heat flux densities, performed at KI earlier in the frame of bilateral collaboration between UJV and KI, are shown in figure 12. Figure shows expected thermal load on RPV using conservative and realistic approach. Latest investigations of severe accidents processes allow clarifying decay heat power distribution in corium pool volume. Additionally, decrease of decay heat power in the corium due to fission products release on the previous stages of the accident was taken into account. It allowed us to remove excessive conservatism in our calculations. Calculations results obtained by different codes are benchmarked. Maximum of heat flux density on external RPV surface and residual wall thickness were chosen as key values for comparison. Obtained results are important for the thermal load profile definition for the RPV model of VVER-1000 in the large-scale experiments on THS-15 facility.

Maximum heatflux value was obtained using three-layer model. Predicted value is  $\sim 1.9$  MW/m<sup>2</sup> by HEFEST-ULR code and  $\sim 2.4$  MW/m<sup>2</sup> by ASTEC code. Difference between calculation results is  $\sim 20$ -25%. Such difference of results could be caused by RPV discretization. IVMR studies require very detailed RPV grid. Mesh density used for ASTEC code is probably not-enough for IVR task, but it is one of the code limitations. Poor mesh provides incorrect calculations of gradient functions and thermal resistance, which are significant for heatflux definition.

Another reason of results differences could be uncertainty of used approaches. Obtained difference correlates with HEFEST-ULR code precision. Expected uncertainty of results by HEFEST-ULR code is estimated as 20 % for heatflux value. However, we found these results are eligible and could be considered as a conservative estimation, considering code limitations.

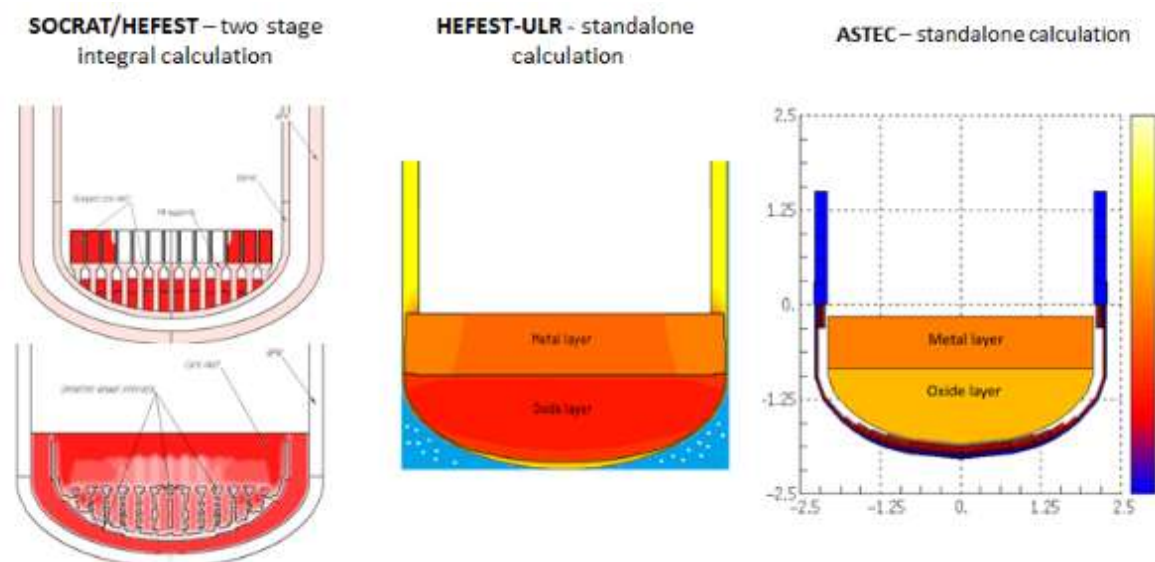


FIG. 11. Used codes for numerical analysis.

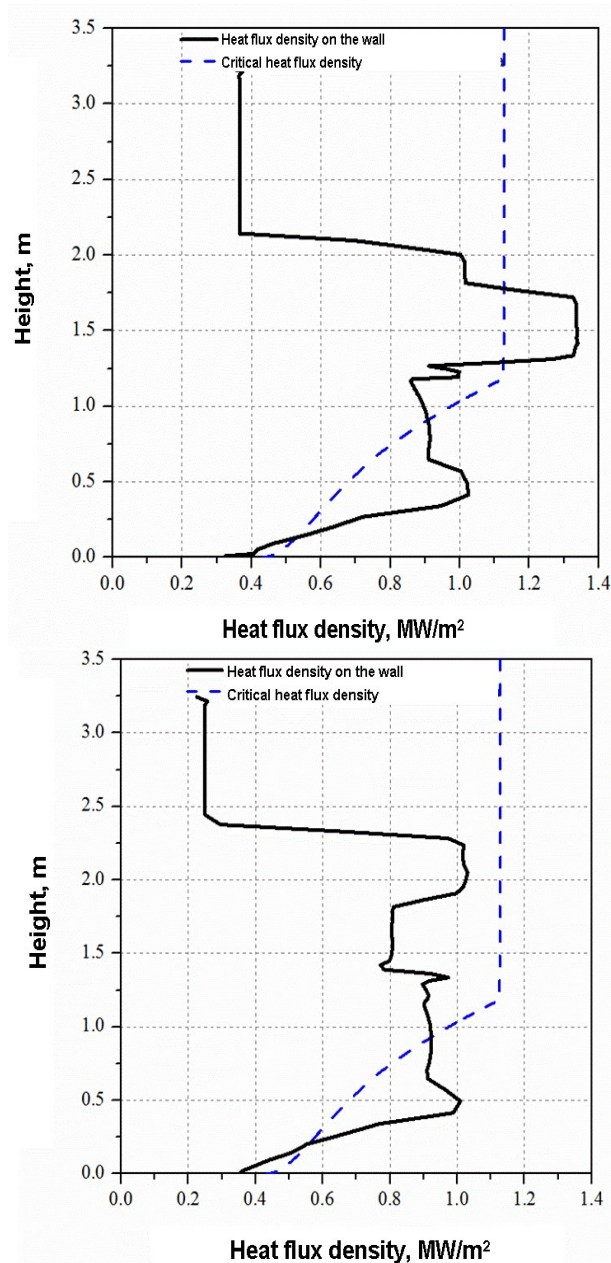


FIG. 12. Time-highest heatflux densities. Conservative and realistic approach. Decay heat is focused in oxide layer  
 a) conservative approach b) realistic approach decay heat considering FP release.

#### 4. CONCLUSION

Overall project is possible to perform thanks to the great team work. Small scale experiments are running in parallel with civil construction work for the large scale facility. As already mentioned, results from small scale tests are providing already significant margin with respect to the calculated heat flux profile calculated by Kurchatov Institute in Moscow. Such a result we have reached thanks to special steel surface modifications. Small scale results are not yet finished and we expect further increase of margin to the calculated heat flux. Building the large scale experiment is a real challenge. It is necessary to mention that at present only two countries are extensively studying the coolability of the RPV outer surface. Even every day technical problem we are progressing forward and focusing to build a reliable cooling channel where we could perform a complex test matrix. During the Conference we will be ready to provide you an update of our team work and results.

## ENHANCING HUMAN RELIABILITY IN SEVERE ACCIDENT MITIGATION THROUGH ADVANCED EXPERT SYSTEMS

M. GAJDOŠ  
Slovenské elektrárne, a.s.  
Nuclear Design Engineering  
Mlynské nivy 47  
SK-821 09 Bratislava 2, Slovak Republic  
Email: martin.gajdos@seas.sk

P. LENHARD  
Inference Tech, s.r.o.  
Sluneční 2377  
CZ-756 61 Rožnov pod Radhoštěm, Czech Republic  
Email: petr.lenhard@inferencetech.com

R. LENHARD  
Inference Tech, s.r.o.  
Sluneční 2377  
CZ-756 61 Rožnov pod Radhoštěm, Czech Republic  
Email: radomir.lenhard@inferencetech.com

T. MAJERSKÝ  
EvenPixel s.r.o.  
Klincová 37  
SK-821 08 Bratislava 2, Slovak Republic  
Email: tmajersky@evenpixel.com

### Abstract

Human factors have played a central role in all major nuclear accidents. The most recent, Fukushima accident, highlighted the need to reanalyse current human factor engineering concepts. A number of actions were initiated by the IAEA to reduce the contribution of human factors to nuclear accidents. An extensive effort is directed towards design considerations of HMI, training, human reliability analysis and other organizational aspects. However, less attention is being paid to increasing human reliability and performance through advanced expert systems for accident management. Management of severe accidents is a complex process where stress and lack of information significantly affect performance of individuals and teams. The paper presents two novel concepts for advanced computerized expert systems for severe accident management support in real accident conditions. The first is focused on the support for evaluation of plant status and subsequent decision making based on advanced machine learning algorithms. The expert guidance is being developed based on current plant data measured during an accident and an extensive set of pre - calculated analytical simulations. The second approach, which is based on applied graph theory and hydraulics, provides technical support centre staff with practical guidance for optimal equipment line-up for the implementation of the selected strategy.

### 1. INTRODUCTION

Management of severe accidents at nuclear power plants is a complex task with large related uncertainties. These uncertainties, in general, are linked on one hand to plant configuration at the onset of the accident, initiating event or hazard causing the accident and the control room operators' and emergency response organisation's (ERO) response to the accident situation. The other source of uncertainties arises from the actual state of the knowledge and understanding of physical and other phenomena evolving in the reactor, primary circuit and containment that are directly related to the core melt scenarios. With these uncertainties in mind it is not possible to develop a procedure-like guidance for management of such states. To address all above specified uncertainties related to severe accident management, severe accident management guidelines (SAMGs) are developed based on an extended set of supporting technical bases and plant specific analyses. The structure and format of SAMGs, however, is of the utmost importance when human reliability comes into question during accident management as complexity of accident situation makes adequate timeliness in decision making very challenging.

Decision making in severe accident management is performed by the Emergency Controller based on evaluations and developments of recommended actions by the technical support centre (TSC) of the ERO. The evaluators' role is to evaluate current status of the plant and propose strategies that are to be decided on and implemented by the control room crew. Evaluations and decisions on strategies are to be made by weighing the pros and cons of strategies under the current accident situation. SAMGs provide an extended guidance on "what" should be taken into account when evaluating plant status to support decision making on implementation of severe accident management strategies. However, the comprehensive "how" part of these assessments and considerations is present in SAMGs in limited scope. This issue is generic in the current format of severe accident management guidelines that are implemented in the nuclear industry around the world. This situation holds to some extent despite the fact that a couple of SAMG enhancement projects were launched and successfully completed in recent years (e.g. the development of consolidated PWROG SAMGs after the Fukushima Dai-ichi accident [1], [2]).

The complexity of evaluating the plant state and decision making in severe accident conditions is also underlined by the limited set of reliable instrumentation. Such a situation can lead to limited knowledge about the plant status. Moreover, instrumentation sensors are placed only in specific areas in general and thus a further "unknown" is brought into the evaluation process. In such situations a paralysis in subsequent decision making may occur as weighing the pros and cons is not supported with sufficient input data. As a result, elevation of personnel stress level may be induced by the need of timeliness in evaluation and decision making especially in situations when the containment boundary is severely challenged or high radioactive dose rates are present on site.

As SAMGs are basically knowledge based, systematic training of TSC personnel may help to provide staff with more confidence in decision making process. However, different decisions may be reached for the same situation depending on the evaluator's and decision maker's knowledge of certain aspects of SAMGs and their technical basis. It is therefore believed that a more rule based decision making tools could provide for more consistent decisions from evaluators and decision makers [2], [3].

## 2. DECISION MAKING SUPPORT TOOLS

To support plant status evaluation and the subsequent decision making process, a feasibility study on the appropriate approach selection and pilot demonstrator was performed [4]. An extensive set of MELCOR analyses of core damage sequences was used as the source of raw data for the development of decision making support tool pilot. In this exercise a CRoss – Industry Standard Process for Data Mining (CRISP – DM) methodology was used. The CRISP – DM concept allows for systematic step by step approach to task and goal definition in each step of the data mining process possessing the advantage of fast and effective project execution. The main goals of the feasibility exercise were as follows:

- Development of adequate mathematical data structures and functions describing containment state in severe accident conditions.
- Development of adequate prioritization criteria of negative aspects of SAMG strategies.
- Development of adequate systematic assessment of negative aspects of SAMG strategies as a function of containment state.

This pilot exercise was carried out with a focus on hydrogen risk concerns. With respect to this condition, the so-called baseline dataset representing containment state in severe accident condition was successfully developed. The vector-like dataset consisted of "independent" parameters representing containment spray operation by the control room crew and MELCOR calculated parameters corresponding to plant measurements used in the SAMG evaluation process. As "dependent" parameters, so-called response parameters were defined. Response parameters were chosen as specific MELCOR calculated parameters (containment pressure, hydrogen concentration in containment volumes where no measurement device is present, etc.) or parameters determined by MELCOR data post-processing (AICC pressure, DDT risk evaluation, etc.). The choice of response parameters is always defined with respect to the symptoms/conditions that represent, or are related to evaluation of, a particular negative aspect of SAMG strategy in concern. The development of containment state functions in severe accident conditions was carried out using application of recurrent CART machine learning algorithm. This algorithm is based on binary recursive division of parametric space represented by baseline datasets. Random forest method as an advanced version of CART algorithm was tested as well to maximise the nonlinear accuracy of the developed model.



Once the developed containment state functions are available, it is possible to weigh negative aspects of SAMG strategies and prioritise their implementation in a systematic and reproducible way. The developed model response is always connected to the desired response variable, e.g. hydrogen DDT risk in our case, and current plant parameters at any time during the accident. Using this approach, statistical predictions of model response of concern are calculated representing the relevance of a particular negative aspect of the SAMG strategy in question. Typical CART diagram for hydrogen risk response with corresponding scatterplot are depicted in Fig. 1.

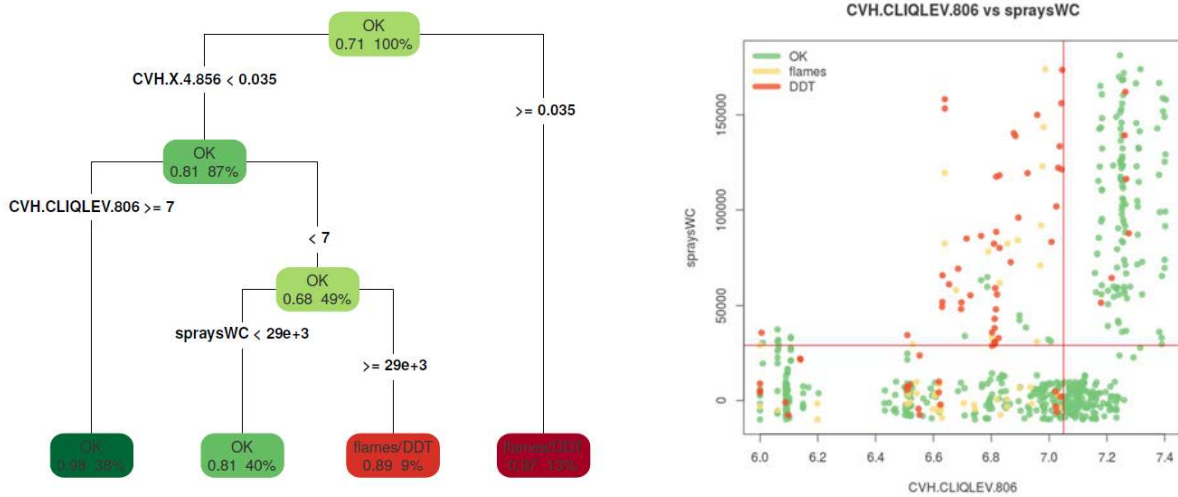


FIG. 1. Left: CART for hydrogen risk response. Right: Scatterplot corresponding to CVH.CLIQLEV.806 and spraysWC nodes in the CART. Variable name legend: CLIQLEV – water level (m), X.5 – oxygen molar ratio, X.4 – hydrogen molar ratio, spraysW and spraysWC – sprays duration (s).

The interpretation of the CART diagram for decision making support is such that TSC evaluators should review branching point values that were calculated by the CART algorithm with current plant parameters. Branching parameters can also correspond to strategy implementation, e.g. triggering of the containment spray. Based on the branching point parameter review the relevance of a particular branch with respect to the current plant containment state is obtained. The statistical evaluation provided by the CART diagram yields the final degree of relevance, or total negative weight, of certain negative aspects (e.g. DDT risk) as a total magnitude of occurrence (percentage value on the right-hand side) with corresponding accuracy value (left-hand figure).

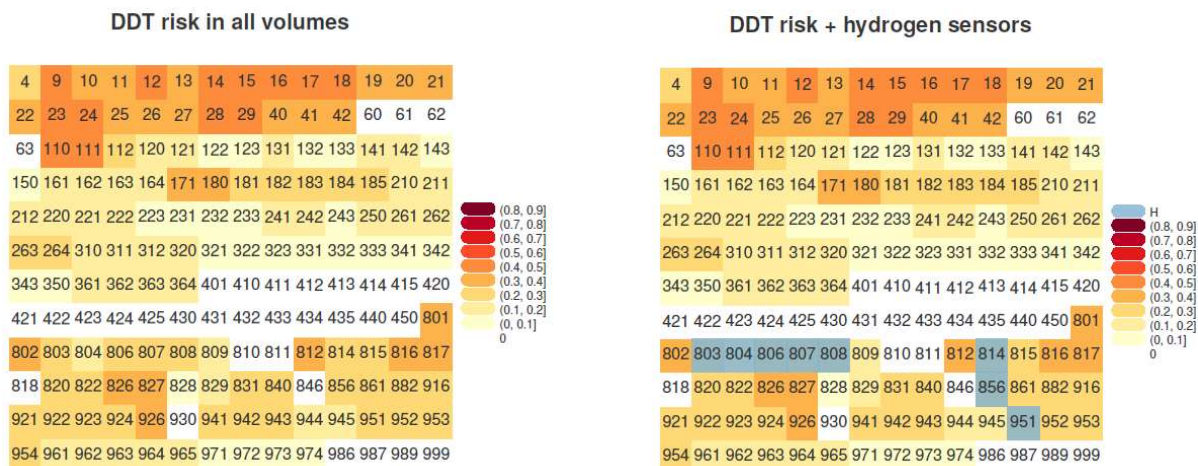


FIG. 2. Hydrogen risk heat maps.

As a model output for further plant behaviour analysis, so-called heat maps were developed. Hydrogen risk heat maps are depicted in Fig. 2 and represent frequency of DDT condition in each containment volume. It is important to stress out that the developed tool can be used, for example, to further optimise measurement device

placement in containment. The risk heat map provides a clear visualisation that the high hydrogen risk region may not be sufficiently covered by adequate set of measurement devices. Such a situation, i.e. lack of knowledge of containment state in specific remote areas, may leave the TSC crew blind to some extent and cause inadequate decision making even with “correct” and clear inputs.

### 3. STRATEGY IMPLEMENTATION SUPPORT TOOLS

Once the decision making process is completed and the optimal strategy for the implementation has been chosen it is important to implement the strategy in a timely and efficient way using the equipment that remains operable at the plant. To support decision making in this field a so-called Configuration Matrix Tool was developed. This tool provides the TSC staff with support in the following areas:

- Assessment of available plant equipment based on external hazard magnitude.
- Quick assessment of potential cliff-edge effects based on external hazard magnitude.
- Development of optimised plant equipment line-up (so-called system configuration) for each particular safety function.

The general idea of the Configuration Matrix Tool can be described in two steps. At first an extensive database of plant SSCs is to be developed consisting of main plant systems (systems that provide safety functions of the plant), supporting plant systems (lubrication, fuel, cooling, pressurised air, electrical supply, intermediate circuits, etc.) and civil structures (with floors and compartments). Then it is possible to search for optimal configurations of SSCs providing for the implementation of a particular SAMG strategy based on the availability and capability of the equipment, time needed to setup/repair of SSCs, etc. The tool output provides user with direct step by step implementation checklist procedure for any SSC configuration.

The building of the SSC database is done using P&ID drawings of plant systems of interest. A specific software tool was developed to allow for semiautomatic parsing of digital P&ID drawings and integration of all P&IDs into the single map of plant systems. Then the database has to be loaded with the parametric data of SSCs, e.g. pipe lengths, pipe diameters, tank volumes, SSC elevation corresponding to plant reference level, SSC location, height of door steps, seismic and extreme external hazard capacity of SSCs, etc. Once the overall SSC database, the so-called plant SSC map, is developed the search for optimal configurations of SSCs is performed by comprehensive search tool based on applied graph theory algorithms. The custom-built search engine allows TSC personnel to specify search and optimization criteria, e.g. type of AM strategy (feed & bleed type, heatsink type, etc.), SSC availability, etc. The search engine output is sorted ascending based on specified optimisation criterion, in general by the lowest hydraulic resistance of the system. Besides this feature, the Configuration Matrix Tool allows for fast deterministic review of provision of safety functions based on extreme external hazard severity. Since the plant SSC map is loaded with SSC capacity data against extreme external events, SSC configuration search can be performed from gradually increasing severity of the extreme external hazard of interest. Evaluator is allowed to see in a clear way at which particular extreme external event severity SSCs are lost. Therefore cliff-edge effects are easily retrieved in a clear and systematic way.

The Configuration Matrix Tool can be also used in support of the standard work management process. Since the search engine provides any found configuration with isolation boundary, work-orders for taking SSCs out of service can be built rapidly and error-free. The basic Configuration Matrix Tool user screen is depicted in Fig. 3.

Using this approach the evaluation of available equipment for a particular SAMG strategy is extensively supported. As time needed to systematically check for available and capable equipment can be significantly decreased by this tool it brings confidence in TSC decision making process, decreases the levels of stress and increasing the reliability of effective implementation of SAMG strategies.

### 4. CONCLUSIONS

To support reliability of human performed actions in severe accident management the factors contributing to uncertainties of the evaluation and decision making processes have to be reduced to allow for effective work environment with limited levels of stress. Uncertainties related to evaluations of plant behaviour and weighing pros and cons of SAMG strategies during decision making can be significantly reduced with expert systems incorporating recent advancement in data science techniques. Data-driven decision making based on extensive set

of pre-calculated analyses of SA scenarios is a feasible option to be widely deployed in ERO of nuclear power plant operators.

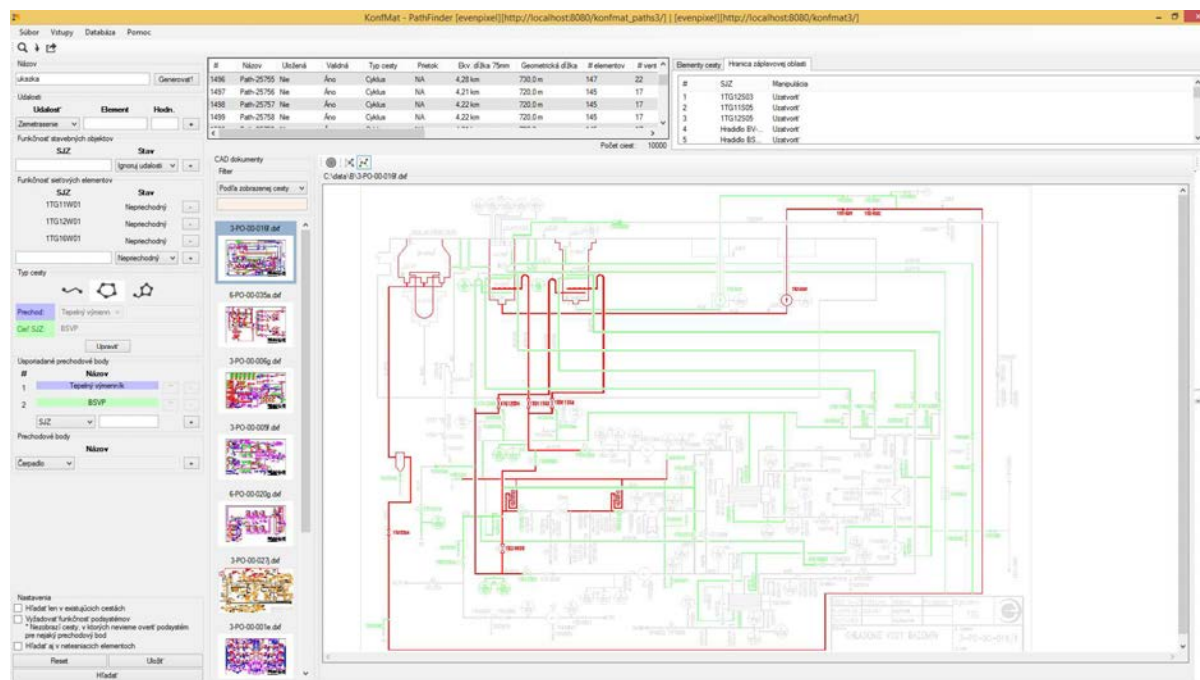


FIG. 3. Configuration Matrix Tool screen.

Once decision making process is completed, timely and effective implementation of selected SAMG strategies can be significantly supported with tools for rapid SSC configuration line-up assessment like the Configuration Matrix Tool. Essential time can be saved in real emergencies using a predeveloped and validated database of potential SSC configurations.

The enhancement of human reliability in accident conditions needs wide deployment of advanced computerised support tools to make the evaluation and decision making process more robust, reliable and time effective. It was demonstrated that the current state of the art of computer and data science allow the development and deployment of such tools.

## ACKNOWLEDGEMENTS

The authors of the paper would like express the gratitude to Peter Juriš and Juraj Jančovič from VUJE Trnava, Slovakia for the preparation of MELCOR data and numerous consultations during hydrogen risk pilot tool development. Deepest gratitude also belongs to Miloš Vančo, Ondrej Krošlák, Peter Lisický and Marek Petric from Slovenské elektrárne for active support during Configuration Matrix tool development and testing. Our sincere thanks go to Robert Prior (R P Safety Consulting Ltd.) for the review and fruitful consultations during the preparation of this paper.

## REFERENCES

- [1] LUTZ, B., “Development of enhanced severe accident management guidance (SAMG)”, NRC Public Meeting, 2013.
- [2] SOLOVJANOV, O., “Westinghouse Post-Fukushima Severe Accident Management Initiatives, “White Paper” and Stress Tests”, Westinghouse, 2011.
- [3] VAYSSIER, G., “Present day EOPs and SAMG – where do we go from here?”, Nuc. Eng. and Tech. Vol. 44 No. 3 (2012) 225 – 236.
- [4] LENHARD, P., LENHARD, R., Mathematical algorithms of expert system – a feasibility study, Inference Tech, Rožnov pod Radhoštěm, Czech Republic, 2016.

## **BWROG – EMERGENCY PROCEDURES AND SEVERE ACCIDENT GUIDELINES (EPG/SAG) REVISION 4 HIGHLIGHTS**

B. WILLIAMSON  
TVA – Browns Ferry  
Decatur Alabama USA  
Email: btwillia@tva.gov

P. ELLISON  
BWROG – GE Hitachi  
Castle Hayne, NC USA

K. KLASS  
Talen – Susquehanna  
Berwick, PA USA

J. LYTER  
Exelon – Peach Bottom  
Delta, PA USA

T. MATSUO, TOSHIHIRO  
TEPCO  
Tokyo, Japan

D. RONIGER  
first Energy- Perry  
North Perry, OH USA

L. SCHULZE  
Xcel – Monticello  
Monticello, MN USA

### **Abstract**

The paper overviews the major changes/updates and recommendations found in the Boiling Water Reactor's (BWR) Owners Group (BWROG) Revision 4 of the Emergency Procedure and Severe Accident Guidelines (EPG/SAGs). The guideline revisions are expected to be available to BWROG Members in 2018. In 2017, the BWROG Emergency Procedures Committee (EPC) is focused on completing and updating the documentation and identifying the documents to be identified as the Revision 4 changes. Once EPG/SAG Revision 4 is formally issued, the utilities in the U.S. will have 3 years or 2 refueling outages to implement Revision 4.

In Revision 4, procedural enhancements have been made to incorporate the ABWR, shutdown/refuel mode guidance, full integration with other plant procedures (FLEX and B.5.b), post Fukushima regulatory requirements, implementation lessons learned (feedback from utility training programs) and continuing insights from the accidents in Japan that occurred in March 2011.

Revision 4 builds on the post-Fukushima lessons-learned incorporated in Revision 3; (issued February 2013, supporting implementation of the U.S. industry's FLEX capabilities). The revision was developed by subject matter experts with BWR backgrounds in operations, engineering, training, risk assessment, severe accident analysis, human factors, emergency operating procedures and licensing. The revision incorporated insights from utilities / regulators / researchers operating or considering construction of BWRs in the following countries: United States, Japan, Mexico, Spain, Switzerland, Taiwan and the United Kingdom. Countries operating BWRs but not participating in the development of Revision 4, include the Nordic Countries and Germany.

After the issuance of Revision 4, the BWROG procedures committee will focus on implementation guidance and will trend towards a maintenance mode of the procedures.

## 1. INTRODUCTION

The BWROG generic procedures and guidelines provide the basis for plant specific emergency actions. The generic procedures and guidelines are continually enhanced in response to lessons learned from world-wide nuclear plant experience, research programs, operator training programs, lessons learned from drills, exercises and other events.

Procedures and guidelines for response to plant design basis events are addressed by Abnormal Operating Procedures (AOP), Alarm Response Procedures (ARP) and Emergency Operating Procedures (EOP). These procedures provide guidance necessary to maintain core cooling while taking the plant from full-power operation to a safe shutdown condition. These procedures have long been part of the plant safety response and are governed by both regulations and industry standards/best practices.

The BWROG procedural guidance is symptom based, generic and responds to conditions as identified from the plant's instrumentation. The BWROG generic procedures are not developed / limited to events based on the results of risk assessment or calculations of postulated accidents. The procedures permit the plant to respond to a wide range of events including those sequences of events whose probability of occurrence is calculated to be very small based on the use of Probabilistic Risk Assessment (PRA/PSA).

The U.S. industry developed symptom based EOPs following the accident at Three Mile Island (TMI) and the Severe Accident Guidance (SAG) was developed after the accident in Chernobyl. The SAGs were implemented as a voluntary initiative that included training and drills. The SAGs enhance the ability of the operators to manage accidents that progress beyond the point where EOPs and other plant procedures are applicable. The SAGs are used by licensed operators in the control room alone and / or with support from the plant technical support staff.

Following the extremist / terrorism actions of September 11, 2001, the U.S. NRC required plants to develop and implement guidance and strategies to maintain or restore core cooling and containment, and spent fuel pool cooling capabilities under the conditions accompanying loss of large areas due to fire or explosion. These requirements led to the development of Extensive Damage Mitigation Guidelines (EDMG or B.5.b) at all U.S. nuclear power plants. The EDMGs are used when the normal command and control structure is disabled and the use of EOPs is not feasible.

Post Fukushima, the U.S. NRC reviewed the U.S. utilities voluntary SAG implementation program activities and identified significant variability in the implementation of the guidelines. Accordingly, the U.S. utilities made a voluntary commitment to the regulator to have the EPG/SAGs Revision 3 implemented by the end of June 2017. This voluntary regulatory commitment was an action to mitigate the use of qualitative severe accident evaluations in the cost benefit assessment used in the U.S. rule making process.

The U.S. NRC initiated an inspection program to ensure that the utilities follow through with the commitment to have effective SAGs in place. The U.S. NRC began the process to develop SAG inspection guidelines in January 2017 and expects to have these inspection guidelines completed for use in the inspection process by June 2017. The first U.S. NRC SAG inspections are expected to begin in late 2017 with a focus to ensure that any plant modifications have incorporated the SAGs into the review process. A more thorough review of the individual plant SAGs is expected to begin with Revision 3 before the implementation of EPG/SAG Rev 4.

## 2. SIGNIFICANT REVISION 4 CHANGES TO THE BWROG EPG/SAGS

Insights from ongoing regulatory programs, R&D activities and further assessment of the lessons learned from the events at Fukushima were utilized to update and improve EPG/SAG Rev 3 to provide the basis for Revision 4 of the guidelines. Some of these updates changed / improved the guidance found in Revision 3 of the guidelines.

The updates for Revision 4 included improved techniques to reduce off site dose by making better use of the suppression pool to scrub fission products. Analysis showed that this improved procedure / method (SAWA/SAWM) was as effective as some of the wet scrubber systems. These changes resulted in different strategies related to drywell flooding that were part of the Revision 3 approved issues. In general, the following are some of the major updates found in EPG/SAG Rev 4.

- ABWR
- Shutdown All Modes

- FLEX Implementation
- Severe Accident Water Addition & Management
- Technical Support Guidelines and Calculational Aids

## 2.1. Rev 4 – ABWR

EPG/SAG Rev 3 addresses the BWR 2 thru 6 designs, the MK I thru III containments and did not provide guidance specific to the ABWR. The committee initiated an activity in 2014 to develop / update specific guidance for the ABWR using insights from the events that have occurred during the Fukushima accidents and improvements that have been developed over the years that were incorporated into Revision 3 of the guidelines.

In this regard, a joint study team was developed, initially lead by the South Texas Project. During the development of the ABWR guidance leadership for the team transitioned to and was subsequently provided by TEPCO. A joint study team that included the ABWR Vendors (Hitachi and Toshiba) and the utilities operating the ABWRs, (TEPCO in conjunction with Taiwan Power Company (TPC) and Horizon Nuclear) along with GEH worked to develop a set of guidelines applicable to the ABWR that considered the different ABWR designs and operational characteristics. The joint study team met several times in Japan, Taiwan and the UK to develop the guidance. The needs / desires and interests of the regulators were also included as appropriate into the symptom based guidance.

The procedures committee members were trained / briefed on the operation of the ABWR and its safety features. The full committee then reviewed the guidance, providing insights, challenges and questions. Considering the ABWR procedure updates from these insights, challenges and questions the full committee subsequently approved the ABWR guidance. The ABWR EPG/SAGs are to be issued as part of the Revision 4.

## 2.2. Rev 4 – Shutdown All Modes

The procedures committee recognized a need to develop EPG/SAGs for all operational modes several years ago. This was reinforced by the events at Fukushima (1F5), hurricane Sandy (US) and the desires of the regulators of several of the committee members. The committee developed a program plan to develop this guidance and the work is expected to be complete and issued as part of Revision 4 of the guidelines. The shutdown guidance is flow charted and symptom based; consistent with the current EPG/SAGs.

EPG/SAG Rev 3 was developed for Modes 1 to 3, with the guidance for cold shutdown and refueling to be addressed in Revision 4. Revision 3 contains most of the general guidance that was needed for Mode 4 (Cold Shutdown) while the refueling guidance (Mode 5) required further development.

The committee completed the Mode 4 guidance (cold shutdown) based on removing guidance not relevant for Mode 4 and added other items as needed. The updates for Mode 4 guidance included:

- Entry conditions and exit overrides; clarifying when to exit (re-pressurization for use of steam driven injection systems),
- Actions to take for inadvertent criticality (multiple rods drift out),
- Refining actions in support of feed and bleed for temperature control,
- Added steps to help maintaining NPSH for Low Pressure ECCS.

The flow-charted Mode 5 Guideline focuses on the maintenance of the NUMARC 91-06 Outage Safety Functions.

## 2.3. Rev 4 - Flex Implementation

Many of the procedure committee members have initiated or have programs in place to supplement installed safety equipment with portable equipment (FLEX) that can be used for the mitigation of beyond design basis accidents. In this regard, TPC developed an ultimate response guideline (URG) to address the need to respond to certain types of external events. The procedures committee conducted a review of this guidance, agreed that it was effective and subsequently incorporated key features of it into the EPG symptom based guidance.

The symptom based EPG guidance was updated to better facilitate the use of low-pressure / low-flow pumps in recovering the plant to a safe condition and to allow a smooth transition from installed safety equipment to portable equipment. The guidance was updated to provide updated water levels bands and pressure bands from which emergency depressurization can occur and not uncover the core or exceed 1500°F peak clad temperature

when transiting to a low flow pump. In addition, the maximum cool down rate was also modified to permit this transition.

This FLEX Implementation guidance was made available to the procedure committee members to assist in FLEX implementation as part of the Revision 3 approved issues and will also be included in Revision 4 of the guidelines.

#### **2.4. Rev 4 - Severe Accident Water Addition And Management (SAWA/SAWM)**

The BWROG procedures committee worked with the BWROG Fukushima response committee on several topics of mutual interest. One of these topics was improving the performance of the containment systems to retain radionuclides or reduce the offsite dose and land contamination resulting from a severe accident. In this regards, Revision 3 of the guidelines were subsequently updated to implement a strategy to better make use of the hardened wetwell vent installed in most BWRs with a MK I or II containment design.

The EPG/SAGs containment flooding strategy was re-evaluated and modified to consider new insights related to quenching of fuel debris in the lower cavity of these designs. The flooding strategy was modified to permit the use of FLEX equipment to supply an initial high flow rate of water with a preferred injection point into the vessel and then reduce it to just enough to maintain debris coolability. This strategy preserves the hardened wetwell vent and provides for a longer-term use of the suppression pool to scrub radionuclides to reduce the offsite dose and land contamination. This strategy, when implemented, was shown to be as effective as some of the containment filter systems. Thus, flooding of the containment is less of a preferred option early in the accident progression in some of these types of events.

This strategy is an approved issue as a supplement to Revision 3 of the guidelines and is part of Revision 4. For those plants with an existing filtered containment vent, it adds additional scrubbing over that provided by the filter to further reduce offsite land contamination. This strategy is referred to as SAWA/SAWM.

#### **2.5. Rev 4 - Technical Support Guidelines And Calculational Aids**

Post Fukushima reviews of pre-regulatory commitment SAG programs by the committee members and regulators indicated a wide range in variability in the plant specific guidance documents. One area of concern were the Technical Support Guidelines or TSGs. Utilities had a range of different guidance documents, varying from a few pages to several hundred pages with a range of different degrees of understanding of the materials.

Because of this variability, the procedures committee developed a generic more detailed TSG document that was applicable to the committee members, added improved calculational aids to supplement the prediction of accident progression and to supplement the interpretation of the plants instrumentation response. These calculational aids are keyed to decision points in the guidance document and can be used to improve the decision-making process during beyond design basis accidents.

To foster a better understanding of severe accidents within the BWROG membership, the procedures committee developed a TSG Workshop. This workshop has been attended by over 350 utility personnel and is focused on providing fundamental information on the SAGs, severe accident phenomena, the TSGs and supporting calculational aids. As part of this workshop, the events and details of the Fukushima plants (Case Studies 1F1 to 1F3) instrumentation readings are reviewed and compared to this information. Workshop participants can use the TSG documents / flow charts and calculational aids to provide insights for their plants and training programs.

The procedure committee is collaborating on fundamental research that improves the TSG calculational aids, to provide for a more user friendly format that will enhance their effectiveness during events along with drills and exercises.

### **3. SIGNIFICANT REVISION 3 CHANGES TO THE BWROG EPG/SAGS**

The following items provide a short summary of the changes to the EPG/SAGs because of the early lessons learned from the assessment of the Fukushima accidents.

The BWROG EPC made several significant and minor changes to the EPG/SAGs that were approved for issuance in Revision 3 of the guidelines. These changes were based on the early lessons learned from the accident

at Daiichi and resolution of open items in the EPG/SAGs since the last revision. The following paragraphs provide a short summary of these updates. The major changes found in Revision 3 of the guidelines involved:

- Station Blackout Event (SBO)
- Spent Fuel Pool Control
- Secondary Containment Hydrogen Control
- SAG Strategies related to Containment Flooding
- Emergency Management Guideline

### 3.1. Rev 3 - Station Blackout Enhancements

*Objective* - Coordinate SBO procedures (AOPs) with EPG/SAGs; Avoid loss of Reactor Core Isolation Cooling (RCIC) High Pressure Coolant Injection (HPCI) from Reactor Pressure Vessel (RPV) depressurization; Permit use of EDMG (B.5.b) coping procedures

*Changes* - Limit RPV depressurization to allow extended RCIC operation; Permit local system operation; Permit defeating isolations; Adjust containment limits; Reduce primary containment pressure to maintain core cooling

*RPV Depressurization* - Core cooling is highest priority; If RPV depressurization will result in loss of systems needed for core cooling: Terminate depressurization; Maintain RPV pressure as low as possible; Applies to all depressurization steps

*EDMGs & FLEX* - Authorize use of EDMG coping strategies and FLEX procedures for: RPV injection systems: HPCI; RCIC; RPV pressure control systems; Safety Relief Valves (SRV); Isolation Condenser (IC) [Note B.5.b is a term also commonly used in the U.S. industry for EDMG coping strategies]

*Defeat Interlocks* – RCIC: High RPV water level; High exhaust pressure: Isolation Condenser; High area temperature

*Adjust Containment Limits* - Heat Capacity Temperature; Limit Pressure Suppression Pressure; Drywell design temperature

*Reduce primary containment pressure to maintain core cooling* - Reduce primary containment pressure to permit use of low pressure Portable Pump (FLEX); maintain pressure below the Pressure Suppression Pressure to avoid loss of RCIC / HPCI.

### 3.2. Rev 3 - Spent Fuel Pool Control

*Objective* - Coordinate Spent Fuel Pool control actions with RPV and containment control strategies and address Institute of Nuclear Power Operations (INPO) recommendations (IER L1-11-2)

*Changes* - Add Spent Fuel Pool level and temperature control sections to Secondary Containment Control

- **Level** - Maintain normal level using normal makeup systems; Use alternate makeup systems if necessary to maintain level above the Technical Specification Limited Condition for Operation (LCO); Isolate/repair leakage paths; Use portable sprays (FLEX)
- **Temperature** - Control Spent Fuel Pool temperature below the Technical Specification LCO using: Normal Spent Fuel Pool Cooling; Supplemental cooling methods; Cross-connects and alternative cooling lineups (FLEX)

### 3.3. Rev 3 - Secondary Containment Hydrogen Control

*Objective* - Provide guidance on controlling secondary containment hydrogen; Hydrogen accumulation in secondary containment is expected during severe accident events

*Changes* - Secondary containment hydrogen control section added to the SAGs; Monitor and control secondary containment hydrogen concentration: Operate secondary containment ventilation; if secondary containment ventilation cannot be operated: Operate Stand by Gas Treatment (SBGT); Create a natural circulation path.



### 3.4. Rev 3 - Sag Strategies

*Objectives* - Remove heat from the RPV; Retain core debris in the RPV; Maintain primary containment integrity; Scrub fission products from the containment atmosphere; Minimize radioactivity releases

*Changes* - Primary containment flooding is implemented when RPV breach by core debris has been determined, when a large break of recirculation system exists or when Pressure Suppression Capability cannot be restored. Otherwise, Pressure Suppression Capability is maintained to be able to address a Design Basis Large Break LOCA or RPV breach by core debris.

### 3.5. Rev 3 - Emergency Management Guidelines (EMG)

Revision 3 included an optional procedural guideline (EMG) for managing the site response to complex, large scale emergency events. The guideline provides a consolidated overview of emergency response objectives and mitigation strategies with references to more detailed procedures. It is primarily intended for use by the Emergency Director in the Technical Support Center (TSC) but may also be referred to by other Emergency Response Organization (ERO) personnel. The EMG summarizes applicable requirements and guidance in: EPIPs (Emergency Plan Implementing Procedures), Security procedures, Abnormal operating procedures, System operating procedures, EOPs/SAGs, TSGs (Technical Support Guidelines), and B.5.b tools. Several plants have implemented this tool, although there is not a requirement to do so.

## 4. FURTHER INFORMATION

### 4.1. Author Information

Bill Williamson (TVA-USA) is Chairman of the BWROG Emergency Procedures Committee and has more than 30 years' experience in reactor operations at the Browns Ferry Nuclear Power Plant.

Phillip Ellison (GE-Hitachi - USA) is the EPC's project manager with more than 30 years' experience in reactor safety topics including PRA//PSA, thermal-hydraulics, severe accident analysis and model development. He received the PhD in Nuclear Engineering from Northwestern University

Ken Klass (Talen Energy - USA) is an EPC Vice Chairman with more than 30 years' experience in nuclear operations and is the Emergency Procedure Coordinator for the Susquehanna Nuclear Power Plant.

Jay Lyter (Exelon - USA) is an EPC Vice chairman with more than 30 years' experience in nuclear operations and is the Exelon Corporate Procedures Coordinator for the BWR Fleet.

Toshihiro Matsuo (TEPCO - JAPAN) currently chairs the EPC's ABWR Procedures Committee with more than 20 years of nuclear plant safety and operational experience.

Dan Roniger (First Energy- USA) is an EPC Vice Chairman with more than 30 years' experience in naval and commercial reactor operations and is the emergency procedure coordinator at the Perry Nuclear Power Plant.

Logan Schultz (Xcel Energy - USA) is an EPC Vice Chairman with more than 20 years' experience in reactor operations at the Monticello Nuclear Power Plant.

### 4.2. Bwrog Emergency Procedure Committee Background

The BWR Owners' Group Emergency Procedure Committee focuses on generic issues affecting Emergency Procedures and Severe Accident Guidance (EPG/SAG). The committee, resolves issues resulting from development and implementation of EPG/SAG, resolves EPG/SAG implementation issues as they occur, facilitates a uniform understanding of EPG/SAG and their technical basis, improves the regulators' understanding of EPG/SAG and their technical bases and provides a forum for information sharing.

In general, the BWROG emergency procedure committee members are experts in plant operations, engineering, training, procedural development, accident mitigation and response. The committee members stay current in fleet wide issues, R&D programs and regulatory activities. In this regard, committee members identify open issues in the generic guidance and bring these items to the committee for resolution. The following issue resolution categories are used by the BWROG Emergency Procedures Committee to resolve these issues:

- APPROVED - Consensus on a change to the EPG/SAGs. Implementation of approved changes is the responsibility of member utilities with due consideration given to applicability to their plant, safety significance and improvement in operator response to plant emergencies.
- ACCEPTED - Consensus agreement on an interpretation of the existing guidelines. Because of this interpretation, it is concluded that changes to the EPG/SAGs are not required.
- CLOSED - Consensus resolution cannot be reached and it is subsequently determined by the EPC or BWROG Prime Representatives that resources should no longer be applied towards issue resolution.
- WITHDRAWN - The category is used for issues which for some reason have subsequently been determined to not meet the screening criteria or are addressed by another issue.

The BWROG Emergency Procedures Committee is cooperating with other industry initiatives and addressing items associated with these initiatives. Note – Any utility member or non-member can bring an emergency procedure issue to the EPC for review and discussion.

#### **4.3. Information Contained in this Paper**

This document is a summary of BWROG publicly available information, publicly available technology or the results of fundamental research, that has been compiled by the authors, for use by the IAEA. The paper summarizes items of interest to those involved in fundamental research associated with emergency operating procedures and severe accidents.

### **5. CONCLUSION / SUMMARY**

The paper overviewed the major changes/updates and recommendations found in the Boiling Water Reactor's Owners Group Revision 4 of the Emergency Procedure and Severe Accident Guidelines. For more detail on the guidance please contact one of the authors above.

The guideline revisions are expected to be available to BWROG Members in 2018. In 2017, the BWROG Emergency Procedures Committee focused on completing and updating the documentation and identifying the documents to be identified as the Revision 4 changes. Once EPG/SAG Revision 4 is issued, the BWR utilities in the U.S. will have 3 years or 2 refueling outages to implement Revision 4.

In Revision 4, procedural enhancements have been made to incorporate the ABWR, shutdown/refuel mode guidance, full integration with other plant procedures (FLEX and B.5.b), post Fukushima regulatory requirements, implementation lessons learned (feedback from utility training programs) and continuing insights from the accidents in Japan that occurred in March 2011.

The BWROG EPC continues its activities to review and address improvements to the BWR generic emergency procedures.

### **ACKNOWLEDGEMENTS**

The EPC acknowledges the support of the BWROG Chairman Lesa Hill (Southern Nuclear) and the supporting utilities in fostering BWR procedure improvements. The BWROG Emergency Procedures Committee includes utility members operating or constructing BWR plants from the U.S., Japan, Mexico, Spain, Switzerland United Kingdom and Taiwan.



## PROGRESS ON SEVERE ACCIDENT MANAGEMENT

**Chairperson**

**J. ŽDÁREK**  
Czech Republic



## ACTIVITIES ON SAFETY IMPROVEMENT OF CZECH NPPS IN SOLUTION OF SEVERE ACCIDENT ISSUES

J. DUSPIVA  
ÚJV Řež, a. s.  
Husinec, Czech Republic  
Email: jiri.duspiva@ujv.cz

### Abstract

The safety upgrade of existing power plants was very strongly accelerated after events at Fukushima Dai-ichi NPP with a focus on two main areas – prevention and mitigation of severe accident.

The preventive actions included hardware provisions for alternate response plans and the mitigation actions include an increase of capacity PARs, assessment of equipment functionality, In-Vessel corium Retention (IVR) at VVER-440/213 units. The only remaining issue is a solution of the corium stabilization for VVER-1000/320 units.

There are two possible strategies to be applied at the VVER-1000/320 for the corium stabilization – IVR and Ex-Vessel Corium Cooling (EVCC) and both are under investigation in the ÚJV Řež. The application of the IVR would be preferred if several technical issues would be solved as feasible at the existing plant as well as the functionality of strategy will be confirmed analytically and experimentally.

The EVCC strategy is also investigated using the analytical approach for the identification of possible strategy steps. The feasibility of some technical modifications was evaluated and the experimental program for the support of the solution with the refractory lining in the cavity and spreading space is under preparation.

### 1. INTRODUCTION

The ÚJV Řež, a. s. supports both Czech NPPs in the severe accident field including accident management. As the response to the Fukushima Dai-ichi accident the strengthening of the NPPs preparedness on the severe accident termination and mitigation of the consequences was emphasized and the ÚJV collaborated in preparation of the countermeasure application. Preparation of severe accident strategies identified a set of various needs on the data or high uncertainty reduction, which can be solved only via. new tasks of the research activities. Those can be subdivided into several base topics, each of them can be subdivided into many others.

The first set of the applied measures were related to the prevention of the accident progression into severe one. The definition of retrofiting came out from the observations of the Stress test [1], which were summarized into the National Action Plan [2]. The utility prepared the Program for Safety Enhancement for both Czech NPPs, which was endorsed by the authority (State Office for Nuclear Safety). Within these activities several measures were implemented between 2013 and 2015 with careful monitoring of post Fukushima design modifications in Russia and also by other VVER technology operators. As examples of the implemented measures the process of “hardening” of the design included modifications of batteries charging, SBO diesel generators, back up supply to SG, primary circuit, and spent fuel pool, fire brigade building reinforcement, mobile equipment for water supply & heat removal and so on.

The second part of activities is focused on the mitigation of already progressed severe accident. The already implemented measures are the increasing of the passive autocatalytic recombiner capacity to deal with the hydrogen sources from the severe accident at all units of both Czech NPPs (finished in 2015), implementation of modifications for the in-vessel retention strategy at the Dukovany NPP or assessment of equipment functionality under severe accident conditions.

There are some issues related to the severe accident management program, which are not yet solved. The most important issue is the corium localization at the Temelin NPP (VVER-1000 units) and related issues of the long term containment condition maintenance, as it is influenced by the corium localization strategy. This presentation is focused mainly on the activities related with the solution of the corium localization at the VVER-1000 type of unit. The other activities on the remaining topics of the severe accident management are foreseen in the upcoming periods with specific focus on the topics of the maintain of the containment integrity issue and reduction of fission product releases, which are the most important objective of the severe accident management for not only existing, but also for the newly constructed power plants. From this point of view the solutions applied at new units can be transferred and implemented at already existing units in operation, but with some limitations

due to their design solution. Solution of corium retention is such case, because it is possible to use some already gained experience for both kinds of strategies (IVR and ExVC), but they must be re-evaluated for existing design solution (mainly of the containment) of the VVER-1000/320 unit.

## 2. PREPARATORY ACTIVITIES TO CORIUM LOCALIZATION SOLUTION

As described in the introduction, the UJV provides long term support to both Czech NPPs and this support has been focused, among others, also to investigation of possibilities of the solution of corium retention for the VVER-1000 type of reactors.

The first activities on the corium localization were focused on the issue of the termination or at least slow down of corium concrete interaction during the ex-vessel phase. This preference has several reasons. The most important was that it was not expected to make any principal civil engineering or new system implementing activities in relation to severe accident management before the Fukushima event. So the limitation to existing systems and design was very strong and determined possibilities of potential solution. One of the important limitations was that the cavity was always expected as dry and any possibility of its flooding for the IVR strategy were unrealistic. The idea for the corium spreading to the neighbouring room of the reactor cavity to reduce corium layer thickness, increase of surface for cooling was the favourable one. The UJV participated in several international projects (SARNET, SARNET2, OECD MCCI and MCCI2) with the aim to collect sufficient mass of knowledge for an evaluation of feasibility and efficiency of such solution.

As a response to the more extensive interest to the severe accident management the studies of more alternative solutions were launched including in-vessel corium retention with external reactor vessel cooling by flooding of cavity room. The first project (duration in second half of 2013) [1] was focused on the summarizing of recent state of the art on this strategy of corium localization, preliminary study on possibility of flooding of reactor cavity, development of the first modelling capabilities using the CFD code FLUENT for corium modelling and RELAP5 code for the vessel cooling issues. The specific intention was focused on the possibility of increasing of critical heat flux (hereafter CHF) using the high velocity particle coating (hereafter HVPC). Continuation of activities in 2014 [2] were focused on the extension of analytical approaches for the modelling of corium behaviour with estimation of heat flux distribution to the reactor wall and the cooling of external surface of the RPV under various conditions – simple flooding of cavity, application of deflector for enhancement of cooling conditions (and increase of CHF) with various dimensions.

In parallel to activities for the CEZ utility, the UJV participated in the benchmark on evaluation of the heat flux distribution to RPV wall for the VVER-1000 reactor under coordination of JRC IET Petten [3]. The main objective of the analytical studies was to ensure that the corium could stay in the RPV with external cooling during a severe accident and would reduce significantly the loads on the last barrier in the defence in depths (containment). Thus, the risk of fission product release to the environment is reduced. Starting from 2012, several research institutes and utilities in Europe (and also in the Russian Federation and Ukraine) started some work on this topic. The preliminary results of these first investigations highlighted that large uncertainties (especially in the area of modelling activities) were existing regarding IVMR for VVER1000. This highlighted the need to start an activity supporting the assessment of these uncertainties and one way envisaged was to set up an international benchmark on computer code calculations for “In Vessel Retention for VVER 1000”. JRC-IET was asked by UJV Rez, a. s. to organize this international benchmark on computer code calculations for “In Vessel Retention for VVER 1000” with the target of providing preliminary results on the feasibility of this mitigation strategy in case of severe accident for such kind of reactor type. Two kinds of analytical tools were used CFD (CFX, NEPTUNE CFD, and FLUENT) and mechanistic/lumped parameters codes (ASTEC, SOCRAT, MAAP, PROCOR, and MELCOR). The results provided by all contributing partners in the benchmark were processed and compared. They were relatively significantly scattered due to several reasons, regardless most of the participants used the same basis of the input deck and prescribed initial and boundary conditions. This confirms very important user effect and requirement on deep comparison of not only results, but also used input data, models and model input parameters.

In the meantime the interested for this topic has continued to grow and several other EU institutions joined this benchmark especially because the subject of IVMR is also applicable for other types of NPPs, expanding the work as initially planned. A larger project on the topic was prepared in 2014 and proposed to the H2020 call

NFRP-01-2014: “Improved safety design and operation of fission reactors”, in order to expand the level of knowledge reached so far.

### 3. PROJECT ON CORIUM LOCALIZATION AT TEMELIN NPP

The project on the complex approach to the solution of the corium localization for the Temelin NPP was initiated in 2015 with duration up to 5 years. This project has six main topics, which covers not only the corium localization itself, but also some related phenomena and processes. Each of the topics will be described below in chapter 3.2. The conditions to be applied during the development of severe accident measures are in chapter 3.1.

The solution of the project is interesting in two points of view. The first one is the set of requirements for the solutions of proposed measures. This is the main outcome for this conference. The second one is the technical solution itself, which is more interesting for other operators of the same type of reactor. The next subchapters will focus on these two areas.

#### 3.1. Requirements for severe accident measures

Generally, it is possible to simply express that the new equipment dedicated for the severe accident conditions have to fulfil two main requirements – to be simpler than existing systems and to have reduced requirements to operating staff and energy supply. The main reasons of such prescribed requirements is very nature, because the events which will cause that the unit will progress to severe accident must be very strong and several safety systems with numerous redundancy had to fail, so the equipment which should survive such severe conditions must be different in design, based on simple technical solution (design) and its control must be as simple as possible, because due to severe conditions it will be very complicated to carry out any operation. The solutions to be proposed and potentially implemented at the Czech NPPs have to comply not only two basic requirements, but to fulfil also other conditions:

Effectivity – quantified benefit to safety, it means to prevent the release of fission products or at least to reduce (minimize) fission product releases and the physical fruitfulness has to be confirmed with sufficient margin. The quantification of the term “sufficient margin” is the critical point and the international expert community should prepare any proposals, which would be implemented into national legislations. As example, the safety margin to critical heat flux in case of the IVR strategy. This is not yet quantified, but the EC H2020 IVMR project has one of the expected outcomes to prepare at least the first estimation based on the uncertainty of the phenomena and processes they influence this issue.

- Reasonable technical feasibility – this means that the proposed solution has to be relatively simple and the implementation process don’t need to provide complicated and risk technical work on important components of the unit.
- No negative impact to reactor operation – it is absolutely impossible to implement any new measure which would influence safety of reactor operation or which would influence safety of activities carrying out during outages. Also the solution which is very complicated and requires to carry out many operations (like dis-assembling and re-assembling) during each outage are too risk to be implemented.

Simplicity – this follows the common requirements, because the personal staff capacity could be limited during severe accident occurrence as all severe events occurred in the worst time. The unit can have limited accessibility due to damages caused by initiating events (external events) or as the consequence of an accident progression including also its severe phase.

- Independency of functionality assurance – these conditions has to be fulfilled at least partly, because any unit is equipped with several safety systems, which are redundant, but all of them had to fail to progress into the severe accident. If all such systems failed there is very - very low probability that the system designed on the identical technical solution survives regardless it is dedicated for severe accident. So, the solution using different technical solutions – like passive operation with need of electricity from batteries for activation only or any other approach – are the best approach for the new measures for the severe accident. The recent IAEA standards don’t require the passive solutions for the severe accident measure, but the preference of such solution has to be emphasized. The final design of solutions is always determined with the design of reactor unit itself and much more flexibility is in case of new designs than for the existing units in operation.



- Consistency of approach with other utilities and original designer – this condition is prescribed by the CEZ utility and it is focused on solution of VVER units, as in case of VVER-440/213 the solution of corium localization is practically unified with some negligible details of some particular technical solutions, the VVER-1000/320 still has no common agreement also due to very low activity of original designer, as the legislation in Russian Federation don't require any solution for severe accidents at units in operation.

As the CEZ utility recently solves the severe accident management at existing reactors in operation, it is very difficult to fulfil all prescribed conditions together and some of proposed solutions don't comply with any condition, but as an exception and comply with most of them.

### 3.2. Solution of severe accidents for VVER-1000

As introduced in the introductory paragraph of the chapter 3 the project consists of six main areas/topics related to severe accident processes to be managed. The progression of the severe accident is subdivided into three main phases concerning the approaches to corium localization. The first phase has duration starting with the entry to the SAMG (identified with core exit temperature exceeding 650 °C) and ending with corium relocation to lower plenum and draying out remaining water here. This phase is understood as the potential to inject water into the reactor vessel and terminate the progression of severe accident inside of the RPV. The second phase covers similar phase but the corium is hold inside of RPV with external cooling of the pressure vessel (strategy IVR). This phase is terminated with the lower head failure. The last phase solves corium coolability after corium ejection from failed RPV.

The first topic is the primary circuit depressurization under severe accident conditions. This phase was solved in 2015 as the NPP prepares the modifications of the relieve and safety valves control and the analytical support had to confirm if a depressurization using various combination of one or two of three valves is sufficient for fast depressurization of the primary circuit within prescribed criteria. The criteria were defined for the applicability of the IVR strategy as this strategy requires more efficient and mainly faster depressurization than the case of the ExVC strategy. The analyses were performed with the MELCOR code and confirmed that the system is sufficient to depressurize primary circuit to predefined level before starting of corium relocation to lower plenum for the postulated SBO scenario. The remaining issue is qualification of the valve operation, because of its cycling under severe accident conditions with very hot media flowing through including aerosols.

The second topic solves the injection of coolant into the RPV with degraded core, i.e. during the early phase of the core degradation. The several analyses were performed with the MELCOR code for various types of equipment for water injection (various mass rate and head dependence) as well as various times of injection activation. The analyses confirmed that if the injection is initiated before RPV dry out it is possible to cool down the debris bed, but after the formation of molten pool in the lower plenum the prevention of lower head failure with cooling of corium is impossible. The conclusion [4] is that there is a time window for the application of the injection of water into RPV with high probability of success of severe accident termination in range from 4 to 7 hours depending on the initiating event and other severe accident scenario definitions. The open issue related to these analyses is the re-criticality due to injection of non-borated water. This issue is planned to be investigated starting from 2017 as the continuation of activities already done.

The third and fourth topics are related to the IVR and ExVC strategies and they will be described in independent subchapters.

The fifth topic is related to solution of the containment response to severe accident loads and long term issues of the severe accident. Some activities were performed in past within previous projects for the Temelin NPP [5] on the evaluation of efficiency of some approaches to containment pressure reduction using various systems (spray system, fire sprays, filtered venting). Additional activities are foreseen in upcoming period.

The last topic is focused on the severe accident initiated in the spent fuel pool. As the SFP is located inside of the containment the access for the application of any measures is very limited and several preventive measures were implemented to inject additional coolant via. various ways. The first scoping analyses were already performed in past [6]. The updates are expected in future for an evaluation of impact of applied measures for severe accident management.

### 3.2.1. Activities of IVR Strategy

The introducing activities were focused on feasibility of the water supply to the cavity for the cooling of RPV. Fig. 1 shows the cut of the VVER-1000/320 containment, which demonstrates with the red line the hermetic border. The hermetic part consists of the containment and recirculation sump which is located below the base-mate of the containment and all water is drained below the containment base-mate. This design feature strongly determines the solution of the coolant supply as the closed coolant circulation loop is not possible and water has to be injected using the external source (with also possibility of a suction from the inside of containment – recirculation sump, but always with active pump in this case). The proposed solution is based on the two subsystems. The first one is dedicated to fast initial flooding of cavity and is based on pressurized tanks of sufficient volume to fill the cavity and appropriate parts of the cavity venting system TL05, which is used as the injection line. The first two tanks are for initial delivery of water and remaining two are equipped with control of injected mass rate to maintain water level in cavity and enable to use this system for the first about six hours of its operation. This time range is important, because it enable sufficient time for activation of the second fully active system for long term water supply. This system is proposed as new with capability to operate for 72 hours without any external support. The critical point of the water supply is the leak-tightness of the cavity and also the necessary modifications of the cavity venting system TL05, because it has to be equipped with new nine closing valves to prevent any cooling water losses. Generally the solution is feasible, but does not comply with some of prescribed conditions, mainly on simplicity and low risk of possible failure under severe accident conditions.

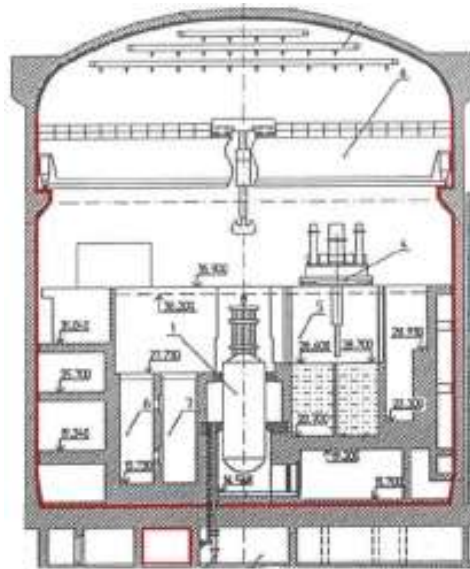


FIG. 1. Cut of VVER-1000/320 containment (red line highlights hermetic zone including recirculation sump).

The second issue which has to be solved is capability for the escaping of steam produced in cavity to other parts of the containment, it is to steam generator boxes in the case of the VVER-1000/320 type of reactor. The utility investigated the size of the gap between the RPV and supporting ring with the conclusion that the flow area in this location is sufficient, the flow areas among the boxes of thermal and biological shielding seems insufficient, but the boxes are removable and in case of the strategy implementations some pieces could be replaced with modified ones to enable sufficient flow area for steam with approach of rupture discs or something similar. This is feasible and can comply with prescribed conditions.

The third topic was focused on the feasibility of the increase of CHF using the deflector. Several requirements are defined for such new equipment and the proposed solution solved all of them. The critical point of the deflector application is requirement that it has to be removed at the beginning of each outage and re-assembled at the end of the outage due to non-influence of activities to be performed during the outage. At the Temelin NPP during each of outage the special measurement sensors are removed and re-placed on the outer surface of the RPV and the special manipulator device is used. Its operation is in conflict with the installed deflector in cavity, so the deflector should be removed. Similar situation, but with 6 year period is related to the

ultrasonic testing of the reactor vessel. The study confirmed the feasibility, but the risk of any incident during removal and re-assembling of the deflector during each of outages is in-acceptably high.

The specific intention was done for the preliminary study of consequences of IVR strategy failure with corium ejection into flooded cavity. The recherche on phenomenology was prepared, because in past this part of severe accident phenomenology was not in high interest as the flooding of cavity was not expected as possible measure. The study was focused on the phenomenology of potential loads to reactor cavity due to molten fuel coolant interaction. The second study was introductory analyses of structure behavior with specific intention to doors between reactor cavity and neighboring room. As the load profile was generic, taken for the recherche performed, the plant specific activities in the area of FCI are foreseen.

The last activities are focused on physical verification of the IVR strategy as the key evaluation of the strategy feasibility. Several analytical works were performed for evaluation of heat flux profile to reactor vessel wall as the basic knowledge on the VVER-1000/320 behavior. The second part of activities was focused on support of experimental program for evaluation of critical heat fluxes specific for the VVER-1000/320 configuration, as the lower head has a semielliptical shape.

The first part of experimental program was performed at the small scale facility BESTH2 (Fig. 2) and consists of about 120 tests carried out including set of tests for reproducibility evaluation. The construction of large scale facility (called THS-15, see Fig. 3). The facility has scale 1:1 for height and slice geometry of 3.8° of angle section of real cavity. The first tests are will be performed at the end of 2017.



FIG. 2. Scheme of heating section and photo of heating section of BESTH2 facility [7].

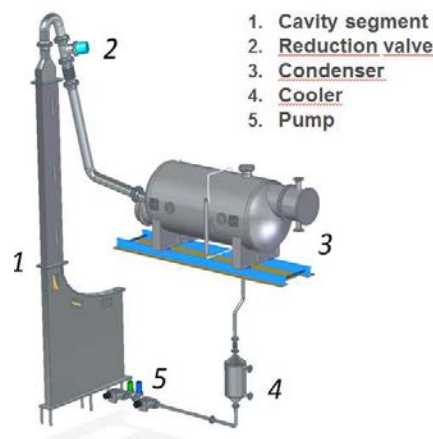


FIG. 3. Scheme of THS-15 facility under construction in UJV Rez, a. s. [7].

### 3.2.2. Activities of ExVC Strategy

Also, the strategy of ex-vessel corium cooling has a progress since the first analytical studies. Additional calculations were performed for the evaluation of impact of application of various measures starting with case without any measure, to be used for the evaluation of efficiency of other measures, than the corium spreading is assumed with and without cooling by top flooding, and also cases with the application of refractory liner in cavity as well as in the spreading space of room GA302. The supporting activities were focused on evaluation of feasibility of the modification of doors between reactor cavity and spreading room GA302 to allow much faster melt-through of doors and spreading. The second supporting activity was focused on feasibility of lining of the cavity and spreading space. Here the solution was prepared independently for each of rooms because the condition on non-influence of systems during operation (venting system TL05 in cavity) or during outage had to be followed. The last part of activities was focused on the selection of possible refractory material candidates, with the aim to define candidates to be experimentally tested concerning their withstanding in contact with corium due to possibility to form crust on border, but also with potential of refractory material dissolution by frozen corium material.

## 4. CONCLUSIONS

The activities on development of solution for the corium localization at existing and under operation type of the reactor, like VVER-1000/320, are very complicated due to looking for solutions determined by already existing design and systems for reactor operation or used during outages. The transfer of knowledge or solutions from units of Gen-III or Gen-III+ is limited mainly due to design differences. But retrofit of existing unit is very important due to common requirement on safety enhancement, but also for case if the new unit is building at the same site with already operating units. All units have to be equipped with measures on very similar level of safety as the severe accident at one unit of the site influences other units. The unit with significantly lower level of safety (in this case severe accident management measures) can easily counterwork the new unit. From this point of view the old units, originally ranked as Gen-II has to be hardened to be on similar level with Gen-III. Afterwards such hardened reactor should be reclassified to Gen-II+ or Gen-III- category.

## ACKNOWLEDGEMENTS

The author would like to acknowledge to partners in the project on corium stabilization from the CEZ utility as well as from the UJV Rez, a. s., which provided activities in sections of presented project.

## REFERENCES

- [1] DUSPIVA, J., Evaluation of state of the art in area of corium stabilization for Temelin NPP, UJV Report, UJV Z-3999-T (in Czech), January (2014).
- [2] BENČÍK, M., VYSKOČIL, L., ŠAFAŘÍKOVÁ, V., Cooling of Pressure Vessel of Reactor VVER-1000 after Cavity Flooding, UJV Report, UJV Z-4047-T (in Czech), June (2014).
- [3] SANGIORGI, M. et. al., In-Vessel Melt Retention (IVMR) Analysis of a VVER-1000 NPP, EUR 27951, Luxembourg: Publication Office of the European Union, JRC101823, (2016).
- [4] DUSPIVA, J., Evaluation of impact of timing of injection initiation and equipment used for cooling of degraded core inside of pressure vessel of Temelin NPP during severe accident, UJV Report, UJV Z-4656-T (in Czech), November (2016).
- [5] KOTOUČ, M., Pressurization of the NPP Temelin containment during severe accidents: ultimate evaluation of the analyzed strategies for containment depressurization, UJV Report, UJV Z-4052-T (in Czech), June (2014).
- [6] KOTOUČ, M., Analysis of severe accident scenarios with loss of cooling and loss of coolant in SFP at Temelin NPP performed with MELCOR 1.8.6 code, UJV Report, UJV Z-3876-T (in Czech), December (2013).
- [7] DUSPIVA, J., R&D Activities to Resolve IVR Strategy for VVER-1000 Reactor, IAEA I3-TM-52206, TM on Phenomenology and Technologies Relevant to IVMR and ExVCC, Shanghai, China, Oct 17-21, 2016.

## **PROPOSAL, DESIGN, IMPLEMENTATION AND SAFETY DEMONSTRATION OF SEVERE ACCIDENT MANAGEMENT MEASURES AT VVER440 IN SLOVAKIA**

J. BALÁŽ  
VUJE a.s.  
Trnava, Slovakia  
Email: Jozef.Balaz@vuje.sk

M. CVAN  
VUJE a.s.  
Trnava, Slovakia  
Email: Milan.Cvan@vuje.sk

### **Abstract**

During the past two decades large effort was dedicated in Slovakia to upgrade the operating VVER440/V213 units to cope with severe accidents. The concept is based on In Vessel Retention (IVR) strategy, but the upgrades - now in finalization phase - were complex and harmonized within all aspects, both safety (prevention, mitigation, releases) and feasibility (availability of equipment, realization costs). The complex of hardware upgrades is composed of eight groups, as e.g. IVR, primary circuit depressurization, long term heat removal, severe emergency sources of coolant and power supply etc. The paper briefly summarizes the long way already passed - initial conditions, approach in design concept, scope and interrelations of individual measures, up to safety demonstration of the efficiency of the severe accident management using adjusted severe accident management guidelines. Selected specific topics are described in more detail to point out the obstacles and list of most important contributions to safety of the units is presented.

### **1. INTRODUCTION**

Extension of the safety assessment of the nuclear power units in operation started in Slovakia during the late 90s. Initially the effort was focused to understanding of the overall response of the VVER 440 units to severe accident conditions - development of basic models and simulation of such accident scenarios in frame of PHARE project [4, 5]. Consequently, all necessary steps were undertaken to cover complete scope of the evaluated safety extension to severe accidents - from probabilistic assessment of events, core and plant damage states and creation of large and full scope database of severe accident analyses point of view, up to the quantification of potential impacts of severe accidents on the environment.

At the beginning of 2005, the level of knowledge was considered sufficient enough to start - in parallel with continuing analytical effort - with systematic identification of weaknesses of the VVER 440, V213 units regarding and ability to control of severe accidents. This systematic identification was aimed on compilation of objectives, strategies, specific procedures and necessary needed systems, which would allow either, enhance protection of the units or an efficient management of severe accident scenarios.

During the first decade of 20th, four units of VVER440 (V213) reactors were in operation in Slovakia. At that time the decision was taken to complete another two units of the same design, but with design extension up to the 4<sup>th</sup> level in depth, i.e. to modify the design in such a way, that it would also satisfy as much as reasonably possible the requirements relevant for newly built units. It required activities aimed to proposal and design systems for protection and mitigation [6, 7] of severe accident, which resulted in design and realization of the complex of measures on units in operation and also on units in completion phase. Application of such measures enabled development and introduction of efficient Severe Accident Management Guidelines.

### **2. SELECTION OF APPROACH**

As required and as specific for severe accidents, the philosophy of the approach to proposal and development of a set of technical measures, dedicated to the severe accident management, shall emphasise protection of the environment and the limitation of consequences on the environment. Thus, the main objective

of the strategy shall be to protect the containment integrity and to control the atmosphere pressure inside of the containment, especially from the long term point of view.

Analyses of diverse scenarios and considerations of potential measures showed that effective limitations of consequences of severe accidents on opened reactor or in the spent fuel pool are difficultly applicable, if ever and the effort in this case should be better focused on practical elimination of such events via implementation of the extraordinary robust and reliable prevention technical and management means.

Evaluation of the complex set of severe accident scenarios with simulation of diverse potential systems for their control shown, that the principal requirement is to prevent reactor pressure vessel damage (to make ex-vessel phases of severe accident practically eliminated). If this goal is not reached then the phenomena as high pressure melt ejection, steam explosions, excessive hydrogen production and containment pressurization in long term may cause present insolvable challenges in proposal mitigation measures.

Another specific outcome of the evaluation was in conclusion that the set of measures needs to be complex, dealing with all identified challenges, and well balanced to provide optimum set of means to control any hypothetical severe accident scenario, without impact to design basis safety.

The design phase of individual systems followed the evaluation. At the beginning it was ascertained, that the qualification of newly designed systems and equipment is a very important and difficult problem. Systems needed to be qualified to environmental conditions, specific for developed severe accident such as very high radiation, high temperature and pressure, exposure from hydrogen burning, flooding etc. Generic approach to qualification use to lead to requirements that are not applicable on corresponding equipment, due to commercial unavailability on the market. Developed methodology of qualification of the equipment, dedicated to severe accident management helped to bridge these obstacles.

Compilation of the overall mitigation strategy represented a task which was consisting of design of particular highly reliable technical means and appropriate procedures dedicated to cope with severe accident challenges, to allow the staff an efficient control of the accident, and to provide them properly reliable technical means for, in expected environmental conditions.

This effort, concerned the both, the development of the systems and the application of them at units, had resulted in practical application of 4th level of defence in depth, as full scope extension of the original design basis.

### 3. APPLIED SOLUTION CONCEPT

The need of practical elimination of the possibility of the severe accident occurrence on opened reactor or spent fuel pool led to proposal of supplementary independent systems dedicated to coolant delivery in to points of interests (opened reactor and spent fuel pool), supplementary cooling systems, dry risers and organization measures within Severe Accident Management Guidelines framework. All these measures were assessed from reliability and disposability point of view. Taking in to account mainly these criteria they were further developed in detail design level.

The matter of severe accidents management and control at the power states of the plant had shown more difficult. Too demanding requirements, which come from expected environmental loading conditions for the equipment located inside of the containment caused, that survivability and reliability of such equipment, without any regard on its possible qualification could not be assured during the all expected period of the accident (at least one year). The solution of the issue led to final formulation of mitigation strategy, development of “qualification” methodology for equipment dedicated to operate in severe accident conditions and to dividing of accident management in to a few separate stages.

#### 3.1. Mitigation strategy

Following are the basics of the severe accident control strategy, developed on the basis of existing and newly added systems.

- To depressurize the primary circuit via independent, highly reliable and appropriately capable system in order to prevent scenarios characterized by the high pressure inside the primary circuit, typically resulting in the high pressure corium discharge into the reactor pit;

- To acquire sufficient sources of coolant to flood the reactor pit in order to take over the control of severe accident;
- To install supplementary external sources of the coolant
  - to prevent transition of any accident to the severe fuel damage;
  - to quench and cool down the core and/or;
  - to decrease pressure inside of the containment and;
  - to increase coolant amount inside of the containment.
- To flood the reactor pit, to prevent permanent coolant losses and to provide access for the coolant to reactor pressure vessel;
- To retain degraded core inside of reactor pressure vessel and to set up sufficient heat sink from the core through reactor pressure vessel wall (In Vessel Retention);
- To manage hydrogen control inside of the containment, via recombination and ignition of the hydrogen and other combustibles and inertisation of the atmosphere to prevent fast flame propagation in case of burning and to prevent detonation;
- To set up sufficient heat sink from the containment and to assure appropriate tightness of the containment hermetical boundary;
- To install the system which would prevent possible dangerous underpressure inside of the containment during particular accident regimes;
- To assure appropriate measurement of necessary parameters required for the proper decision making process.

### 3.2. Methodology of “qualification” of the equipment for Severe Accidents

Difficulties experienced during a selection of the equipment capable enough to operate inside the containment in severe accident conditions, for generally defined period of the time of the accident lasting, insufficient commercial availability of such equipment and frequent questions of the designers led developing team to release qualification methodology [8]. The methodology addresses and summarizes procedures to quantify requirements for the equipment dedicated to operate in severe accidents conditions. It simultaneously provides designer, how to proceed in selection of particular equipment.

This methodology distinguishes between really required active mission time of the particular system (equipment) and its passive part (passive mission time), in which it is necessary to maintain the system operable in the standby mode. The overall required mission time is by this manner significantly reduced, resulting in significant reduction of the total absorbed radiation dose and the heat and pressure exposition. This approach is based on the fact, that once the intended safety function of the particular equipment or system is completed the operability of this system is not required anymore. Therefore, the real mission time requirement can be derived from the time frame in which the execution of required action can be assumed effective and reliable. This approach is furthermore supported by the fact that if the relevant action is executed over such timeframe, it may miss their purpose (e.g. delayed primary depressurization leads to primary break) and may lead to the overall strategy failure.

The methodology requires take in to account the particular place of installation of the equipment (from which the environmental loading conditions are derived) and the affiliation of the equipment to the mitigation system (what respond the question of needed mission time). The methodology then instructs designer directly qualify the equipment if possible. If it is not, the methodology comprehensively instructs designer how to relocate the equipment on a less exposed place of installation and what are dependencies of such relocation, accompanied with. If neither this option is applicable, designer is instructed how to protect the equipment and how to handle with high radiation exposure and hydrogen burning effects.

The approach and description of the methodology will be included also in the TECDOC [11] which is in preparation phase.

### 3.3. Separation of accident management in to stages

In order to allow better understanding of real needs of mission times of systems dedicated to severe accident management and control, the accident management process was divided in to a few stages of the accident management. Mentioned dividing which describes expected use of mitigation systems is demonstrated on following figure (Fig. 1.):

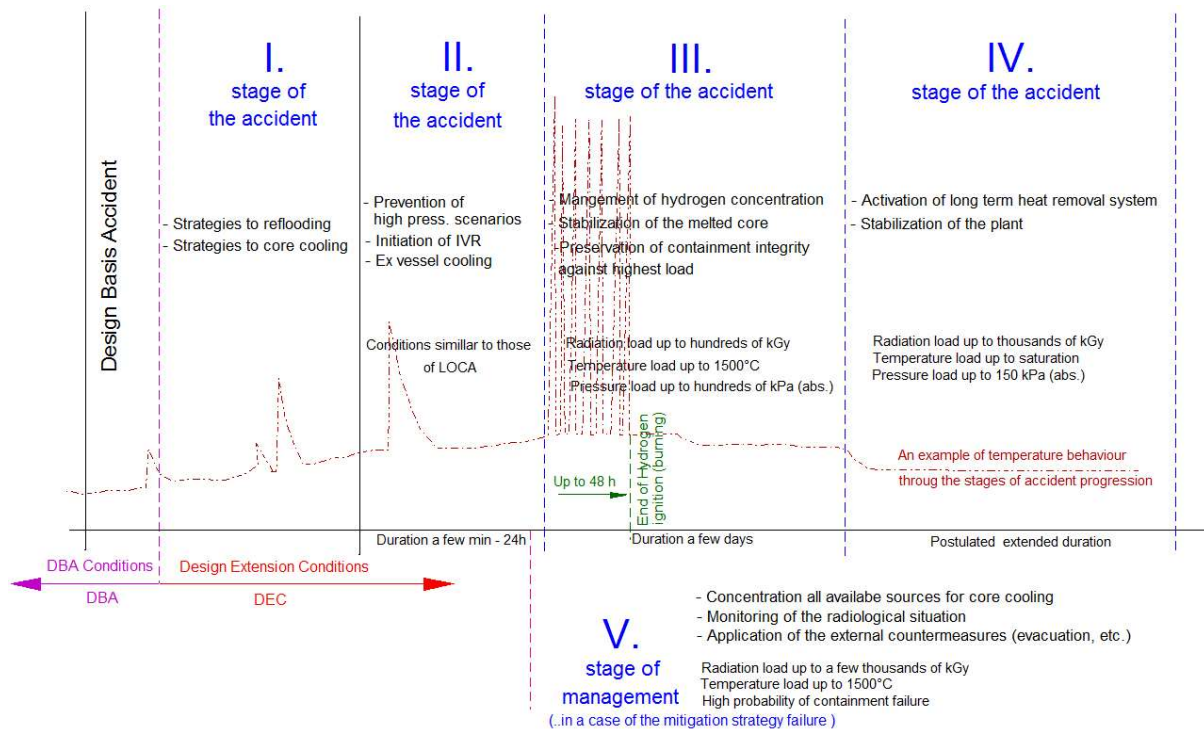


FIG. 1. Separation of the Severe Accident into Stages.

#### 4. SAFETY DEMONSTRATION OF PROPOSED MEASURES

Following implementation of the technical resources in to the plants, these new abilities have been incorporated into the Severe Accident Mitigation Guidelines (SAMG). The real characteristics of systems, their intended application within the SAMGs including were used for integral assessment of their impact and contribution to the enhancement of safety of enhanced units. It included the comprehensive check of the Severe Accident Mitigation Guidelines (SAMG) [9], simulating evolution of diverse severe accident scenarios, including desired operation of mitigation systems. Also, it was checked whether the operating personal is able to identify transition to severe accident, based on available information and whether it is able to mitigate sufficiently the severe accident consequences. The probabilistic safety assessment level 2 was used for selection of scenarios included into the verification scope.

The severe accident management and control represents a process of decision making being carried out in very specific conditions, limited scope of information, high psychological stress, limited access to the most systems inside of the plant and limited possibility of the manual check of corresponding equipment e.g. in case of monitoring lost its monitoring. Moreover, for certain crucial manipulations the limited timeframes exist. That is why the validation process of the both SAMGs and dedicated mitigation systems has also to prove, that it is reasonable to assume, that operating personal gets sufficient information and is provided sufficient time to execute desired manipulations.

The verification and validation of SAMGs consisted of assessment of simulated response of operating personal using analyses of the scenarios, operating and emergency procedures and considering estimated response times and decision making delays.

Consequently, decision making processes was analysed and assessed to judge its feasibility. Deterministic analyses used for this process (integral simulations of variations of diverse scenarios of severe accidents) took in to account estimated, verified and postulated delays in decision making trees gained during previous stage of the assessment. Consequently, the efficiency of the systems was evaluated.



## 5. CONCLUSION

Extension of the design basis of existing Slovak units to severe accidents was long and a complicated way, which has been passed by Slovak nuclear operator and all supporting companies and teams. It was truly iterative process, based on very large analytical basis, putting together views, knowledge and effort of large number of diverse experts, resulting in installation of additional systems and completed by development and introduction of effective SAMGs. The final integral evaluation of the effort and state of the units regarding satisfaction of both legal and functional requirements (completed recently) stated, that all goals of the upgrade of units have been reached and that units satisfy safety requirements, relevant even for newly built reactors. VUJE expert team was participating intensively for the entire duration of the activities and proved its capability to deal with complex and complicated tasks.

## REFERENCES

- [1] CVAN, M., PHARE 4.2.7.a Task 6 Code and Model Qualification Report, rev.2, internal report, VUJE, Trnava, 1997.
- [2] ROHAR, M., LOCAs to Qualify MAAP Mass and Energy Release Curves during Blowdown Phase rev.3, internal report, VUJE, Trnava, 1996.
- [3] PRIOR, B., Analysis of BOBA and Severe Accidents without Operator Actions, internal report, Westinghouse Energy Systems Europe SA, 1997.
- [4] CVAN, M., PHARE 4.2.7.a Task 8/9 Summary Report, rev.3, internal report, VUJE, Trnava, 1997.
- [5] PRIOR, B., PHARE Project 4.2.7.a /93: VVER-440/213 Beyond Design Basis Analysis and Accident Management Final Report and Project Summary, internal report, Westinghouse Energy Systems Europe SA, 1998.
- [6] CVAN, M., et al., Súhrnná záverečná správa projektu UTR 9075, internal report, VUJE, Trnava, 2003.
- [7] CVAN, M., et al., Návrh patrení a modifikácií projektu pre riadenie ťažkých havárií, internal report, VUJE, Trnava, 2004.
- [8] BALÁŽ, J., et al., Určenie parametrov prostredia v miestnostiach a priestoroch pre zariadenia SAM 3. a 4. blok JE EBO, internal report, VUJE, 2013.
- [9] STOJKA, T., et al., 8SG/0004 Validation of Severe accident management guidelines - SAMG, internal report, VUJE, 2014.
- [10] JANČOVIČ, J., et al., Hlavná správa projektu „Vypracovanie komplexného deterministického zhodnotenia Projektu implementácie SAM - Riadenie ťažkých havárií“, internal report, VUJE, 2013.
- [11] DUCHÁČ, A., et al., Assessment of equipment capability to perform reliably under severe accident conditions, TECDOC, IAEA, in preparation.

## SEVERE ACCIDENT MANAGEMENT AT PAKS NPP

G. VOLENT  
MVM Paks NPP Ltd.  
Paks, Hungary  
Email: volent@npp.hu

### Abstract

MVM Paks NPP Ltd. operates four WWER-440-213 type pressurized water reactors. The first reactor started the commercial operation in 1982 and the fourth unit was connected to the grid in 1987.

The safety enhancement has a long history at Paks NPP. Only four years after Unit 4 engaged in the operation the first safety enhancement project was launched. The safety re-assessment using state-of-the-art safety evaluation tools were performed at the beginning of 1990s. The safety enhancement was continued by evaluation of seismic hazards and necessary reinforcements were implemented.

Preparation for the severe accident management had been launched at Paks several years before Fukushima accident. In the frame of severe accident management, Paks NPP implemented technical modifications, introduced Severe Accident Guidelines (SAG) and improved its emergency preparedness.

After Fukushima accident, MVM Paks NPP Ltd. performed a targeted safety re-assessment taking into accounts ENSREG requirements. As a summary, the targeted safety review, thanks to earlier performed safety enhancement projects, has not revealed any such deficiency at Paks NPP which may question the design basis or may require urgent measures. However, the targeted safety review suggested 46 measures for further safety improvement. Realization of the suggested measures is under way, 33 among them have been done.

### 1. INTRODUCTION

Currently Hungary has only one nuclear power plant at Paks site. MVM Paks NPP Ltd. operates four WWER-440-213 type pressurized water reactors. The first reactor started the commercial operation in 1982 and the fourth Unit was connected to the grid in 1987. The original electrical output of Units was 440 MWe each but as a result of power uprating modifications performed in the primary and secondary sides of the Units, the capacity has been increased to 500 MWe each. The Paks NPP produces approximately fifty percent of domestic electricity production during the past few years.

The service life of the Units is 30 years. The service life extension of Units is under way. The permits for further 20 years operation of Unit 1-3 have been granted and the service life extension will continue on Unit 4.

### 2. SAFETY ENHANCEMENT

The safety enhancement has a long history at Paks NPP. Only four years after Unit 4 engaged in the operation the first safety enhancement project was launched. The aim of the project was to re-assess the safety corresponding to the standards of the 1990s by using state-of-the-art safety evaluation tools. The safety enhancement continued with the evaluation of seismic hazards and the design basis earthquake. Preparation for the severe accident management (SAM) had been launched at Paks several years before Fukushima accident.

Regarding earthquake, the seismicity of the site was under estimated during the technical design of Paks NPP. Comprehensive geological assessment of the site showed that the expected peak ground acceleration of the design basis earthquake is one order of magnitude higher. Qualification and reinforcement measures were implemented during the 90s. All systems, structures and components of the NPP ensuring the basic safety functions during and after an earthquake have been identified and classified into seismic safety classes. Necessary reinforcements were designed and implemented.

### 3. SEVERE ACCIDENT MANAGEMENT

The evaluation of safety from the aspect of large discharge was completed by the end of 2004. There are three key elements of the severe accident management:

- Technical modifications;

- Introduction of severe accident management guidelines;
- Emergency preparedness for severe accidents;

Among the technical modifications external cooling of the reactor vessel has been realized. Huge amount of boric water is stored within the containment of VVER 440-213 Units. Approximately 1200 m<sup>3</sup> water is stored in localization tower and the coolant from primary circuit can be also used to fill up the 270 m<sup>3</sup> reactor cavity. In case of severe accident, water from the localization tower will be discharged to the floor of the containment and water will drain to reactor cavity by gravity. The passive process of external cooling of the reactor vessel starts to work.

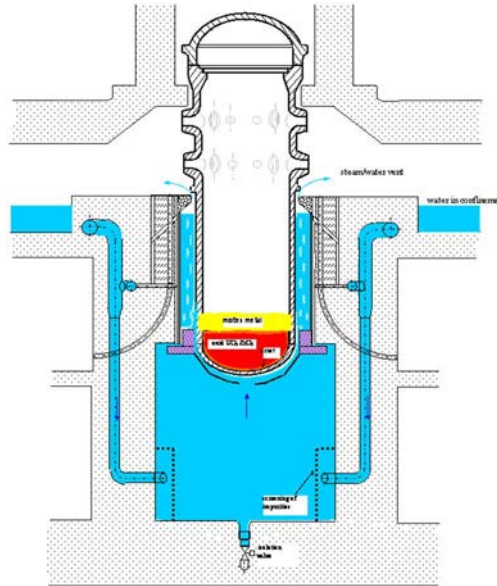


FIG. 1. Schematic diagram of external cooling of reactor vessel.

A severe accident measuring system was installed to measure primary circuit and secondary circuit parameters required for the execution of intervention defined in the severe accident management guidelines. The construction of the measuring system guarantees its operability under severe accident conditions. Batteries and later a mobile diesel generator can supply electrical power to the measurement.

The severe accident management requires the operation of the above-mentioned measuring system and the actuation of certain valves. Among them the most important ones are the pressurizer valves, discharge valves of the localization tower and the valves discharging water collected on the floor within the containment. After the batteries are exhausted energy supply is provided by mobile severe accident diesel generators.

Sixty passive autocatalytic severe accident recombiners for hydrogen management were installed in the containment of each unit. Modification of the cooling circuit of spent fuel pool to prevent the coolant loss due to pipeline rupture was also performed.

The severe accident management guidelines were developed with the involvement of Westinghouse. The system consists of eight Severe Accident Guidelines, four Severe Challenge Guidelines, two Severe Accident Exit Guideline and seven Computational Aids. The operational personnel and the personnel of Technical Support Centre are trained to use the guidelines.

Emergency preparedness was also modified because of severe accident management. The Emergency Response Centre was extended by Technical Support Centre. The training of Emergency Response Organization was extended by severe accident drills and tabletop exercises.

#### 4. TARGETED SAFETY RE-ASSESSMENT

In the frame of post Fukushima actions, MVM Paks NPP Ltd. performed a targeted safety re-assessment taking into accounts ENSREG (European Nuclear Safety Regulators Group) requirements. The re-assessment of

design basis regarding the natural hazards and the safety margins regarding the performance of the safety systems to prevent the prolonged loss of the electrical power and heat sink have been achieved. In addition, the safety re-assessment also covered the evaluation of severe accident management and emergency preparedness.

The re-assessment of design basis regarding external hazards resulted that:

- Re-assessment justified the compliance of earlier implemented seismic safety measures;
- The external flooding of the site can be excluded because elevation of the site and the formation level of embankment on the opposite side of Danube is lower;
- The lowest predicted water level of the river Danube of ten to minus four per year frequency is 84.65 m. The essential service water pumps can be started and operated up to 83.5 m. In addition, lowering of water level is a gradual and long-lasting process and Paks NPP has a four stages action plan to ensure back-up supply for essential water systems;
- Other external hazards such as extreme weather conditions were also assessed but these external hazards do not challenge the safety of the plant.

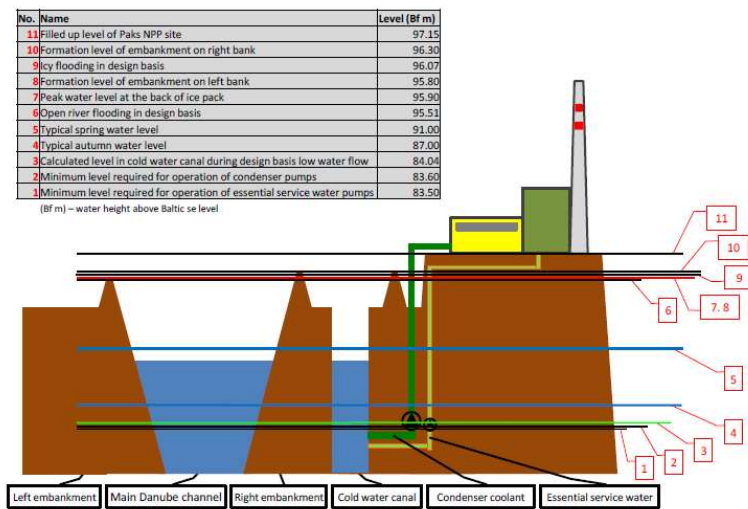


FIG. 2. Levels at the site of Paks NPP.

Regarding the evaluation of safety margins, the review scope included all of the potentially important hazards of natural origin. The re-assessment resulted:

- The on-site alternative and justified off-site electrical power supply routes are available, however the assessment identified further possible alternatives;
- The loss of ultimate heat sink might be happened due to beyond design base earthquake or rather a combination of beyond design basis events. Immediate actions are not necessary, however further measures were suggested;
- The plant shall prepare for simultaneous accident management in more than one unit;
- Emergency preparedness can be improved by some new tools, systems and procedures.

## 5. CONCLUSIONS

As a summary, the targeted safety review, thanks to earlier performed safety enhancement projects, has not revealed any such deficiency at Paks NPP which may question the design basis or may require urgent measures. This conclusion was confirmed by the regulator and the international peer review committee. However, the targeted safety review suggested 46 measures for further safety improvement. is under way, 33 suggested measures have been done.

Some important measures which are still under way:

- Construction of a new fire station;
- New backup emergency response centre;
- Preventing long term over pressurization of containment.

## REFERENCES

- [1] Nemzeti Jelentés a Paksi Atomerőmű célzott biztonsági felülvizsgálatáról (National Report about the targeted safety review of Paks NPP), Országos Atóenergiia Hivatal, 29 December 2011.

## LESSONS FROM SAMG EXERCISES FOR EXISTING AND NEW REACTORS

G. VAYSSIER  
NSC-Netherlands  
Hansweert, The Netherlands  
Email: george.vayssier@nsc-nl.com

B. LUTZ  
(retired Westinghouse, USA)  
Lutz Consultants,  
Asheville, NC, USA  
Email: boblutz1630@gmail.com

### Abstract

Many NPPs have procedures/guidelines to mitigate severe accidents, so-called Severe Accident Management Guidelines (SAMG). These, however, are a tool that only can help operators to mitigate such accidents, as the plants have not been designed to cope with severe accidents. Advanced reactors have features specifically designed to mitigate consequences of severe accidents. In addition, passive systems are used, decreasing the dependency on AC-power. In this way, large releases should be 'practically eliminated'. However, hardware features and SAMG are only one side of accident mitigation; equally important is the associated organisation. Severe accidents may create havoc and chaos on the site, yet in exercises observed such situations were hardly trained. Often, people were not really exposed to far-reaching scenarios, or they had no pre-defined functions, or worked in rooms without protection against radioactive releases. Staff used laptops to follow plant data, without capability to recharge the batteries. Generic SAMG appeared to be badly understood, despite training by the vendor. Instruments were read at face value, where staff did not consider possible deviations caused by the hostile environment of the instruments. Some SAMG required recognition of vessel failure, without proper tools for the staff to do that. In the paper, such experiences are described, the role of mitigative features and how they affect SAMG. "Anti-severe-accident features" seem to have only marginal value without proper organisation and training.

### 1. INTRODUCTION

The design basis of nuclear power plants (NPPs) includes a number of accidents which must be controlled within specified design criteria. Operators use a set of Emergency Operating Procedures (EOPs) in order to control the accident. Usually, these EOPs go beyond the plant design basis, i.e. they also support the operator in these – unlikely – accidents. For example, a main steam line rupture (PWR) is covered by appropriate EOPs, but should also a tube suffer a rupture in the affected steam generator – which is an accident usually beyond the design basis – then still appropriate EOPs are available to the operator to support him/her.

Should the accident progress to core damage, then EOPs usually are not valid any longer, and many plants have specific guidelines in place, so-called 'Severe Accident Management Guidelines', SAMG. The prime objective of these guidelines is to protect remaining intact fission product barriers and mitigate any releases, should these occur. As such accidents are (far) beyond the design basis, success cannot be guaranteed, and much then depends on the possibility to repair failed components, to hook on portable equipment. This uncertain outcome is also the reason why these counter measures are shaped as guidelines rather than as procedures, as it may occur that the operator must deviate from the written guidance, due to the accident evolution.

The IAEA has developed guidelines for Member States to assist in building a package of SAMG, [1]. An essential part is the training on the application of SAMG, which is done in exercises /drills, where an accident is 'played' and the NPP applies the SAMG. Severe accidents can be extremely complex events, with much damage to the plant, possibly including fires and explosions, loss of control room, loss of staff, loss of control of the site. Hence, the Emergency Response Organisation (ERO) may face extreme difficulties in mitigating the accident. In subsequent sections, examples are given of exercises/drills at various plants and the lessons learned.

Advanced NPPs (Generation III) have a number of features that mitigate the consequences of core damage / core melt. A typical example is a core catcher, which is designed to prevent the corium material to interact with the cavity (PWR) or drywell (BWR) concrete, which otherwise could generate large masses of CO<sub>2</sub>, which may

ultimately fail the containment. Examples of core catchers are the melt trap in some larger VVERs, the BiMAC in some BWRs and the melt spreading room in the EPR. The APWR possesses a passive containment cooling device, which removes the decay heat from the core debris. Vessel meltthrough is prevented by external cooling of the reactor pressure vessel (RPV), a technique also in use in a number of Generation II NPPs.

Yet, although such features are extremely helpful, they do not replace the SAMG: appropriate guidance still is needed to mitigate the accident, and exercises/drills to train the accident mitigation using the guidelines.

## 2. EXPERIENCES IN EXERCISES / DRILLS

A number of exercises/drills have been attended and assessed by the authors. Some were so-called RAMP-missions by the IAEA (RAMP = Review of Accident Management Programme, for which guidelines have been developed in [2]. Note: RAMP is now a part of the IAEA DSARS programme, where DSARS = Design and Safety Assessment Review Service). Other missions were bilateral, i.e. on invitation from a regulator or an NPP to NSC Netherlands.

Some of the reports are in the public domain, notably a RAMP mission to Krsko NPP, Slovenia [3], a RAMP mission to Ignalina NPP, Lithuania [4], a NSC Netherlands mission to Point Lepreau, New Brunswick, Canada [5]. The lessons learned as reported here include, however, also other NPPs, for which the reports are not in the public domain.

The assessments were based on IAEA documentation, such as [1] and [2], but included also experience the second author has obtained in watching exercises/drills in various plants. This experience has been included in a draft revision of [2], for which no published document existed during the reviews. It must be noted that the NPPs and regulators gave full cooperation, even where they exposed themselves to a critical review.

The assessments included the underlying documentation, such as the national regulation, the SAMG, their background documentation, underlying analysis such as PSA (Probabilistic Safety Analysis), documentation on verification and validation of the SAMG. In principle, the tasks as delineated in [2], were performed:

- Definition of overall AMP and its compliance with the national requirements;
- Quality and extent of accident analysis to support the AMP;
- Assessment of plant vulnerabilities;
- Development of severe accident management strategies;
- Evaluation of plant equipment and instrumentation;
- Development of AM procedures and guidelines;
- Verification and validation of the procedures and guidelines;
- Integration of AMP and NPP emergency plan;
- Staffing and qualification;
- Training needs and performance; and
- AMP revisions.

The following are the major findings of the various reviews:

### *1. Improper use of the generic SAMG product*

It appeared that one plant had used a generic set of SAMG as the basis for their plant-specific SAMG, yet appeared not to have understood the basic principles of the generic methodology. SAMG appeared to be mixed up with EOPs, where these two have a different focus (notably protection of fission product boundaries versus restoring core cooling), different characteristics (verbatim procedures for EOPs, guidance nature of SAMG) and different basis (largely intact core versus degraded/molten core). Some approaches indeed do not close their EOP upon entrance into SAMG, but then have a clear resolution in case of conflict. It also appeared that what was labelled to be a severe accident guideline, in fact was an EOP.

The particular plant had undergone training by the vendor, but apparently did not fully comprehend the SAMG approach.

Another plant had used elements of a generic product, but was unable to demonstrate a technology transfer from the vendor of that product to the NPP. Such a transition is extremely important, as the fundamentals of the generic approach must be transferred appropriately to the specific plant. For example, in a number of plants

(PWRs), a creep rupture of SG tubes is risk relevant and placed high on the priority list, whereas in other plants other FPB challenges are more relevant.

Some plants had not really transformed the generic SAMG to the plant-specific SAMG, which is, however, an absolute 'must' for the development of proper SAMG. Some even used plain generic data for the transition from EOP to SAMG, where this always is a plant-unique / plant-specific value, to be obtained from proper analysis.

### *2. Improper or incomplete Technical Basis*

The technical basis includes the vulnerabilities of the fission product boundaries (FPBs), the strategies that mitigate the challenges to the FPBs, and the effect of the different strategies during the various plant damage states. An excellent (generic) Technical Basis for PWRs and BWRs is in the EPRI Technical Basis Report, Vol. I, [6]. Various plants had no proper Technical Basis, e.g. it was unknown what the strategies would do during the various phases of the accident, notably whether they would be beneficial or detrimental under particular plant conditions. Some plants had used only one or two accident scenarios to develop their SAMG – far less than the number of severe accident initiators from both internal and external causes. The IAEA Safety Guide on Severe Accident Management, [1], has an Appendix with examples of scenarios to be considered, which is already ~ 30 for internal causes. Best is, of course, using the plant PSA, although care must be exercised that PSAs have been designed to estimate risk, not to define the best possible actions under SAMG.

### *3. Improper transition EOP – SAMG*

A key element is the transition from EOP to SAMG. First, it must be defined on which parameters such transition should be based (i.e. which threshold must be exceeded so that the EOPs are terminated and the application of the SAMG starts). Second, the transition must be made known to all involved, so that also organisational issues can be initiated, e.g., the transfer of decision making from the shift supervisor to the assigned decision maker (usually the plant manager, or operations manager). It appeared various times that the transition was unclear and, when it happened, it was not announced (so still many did not know).

In one case, it was established that the transition EOP-SAMG was placed at vessel failure. This is, of course, a fully inadequate transition point and is so for two reasons: 1. A massive release of fission products occurs already long before vessel failure, so that protection of fission product boundaries becomes the prime objective. 2. The meltthrough may not be monitored by the TSC, as it is difficult if not even impossible in a number of cases.

### *4. List of auxiliary equipment incomplete or absent*

A major advantage is to have an overview of all available water sources and the way the water can be brought to its destination: the RPV, the cavity, the drywell floor. This should include temporary connections, such as via hoses, fire trucks, etc. Similar should be available for the power sources. In the exercises observed, such knowledge was not available in a structured way and had to be improvised on the spot.

### *5. Use of equipment that has been damaged by the accident or is not qualified for the prevailing environmental conditions;*

SAMG includes the equipment which is to be used during the mitigation efforts. During the development of the plant specific SAMG, the development team should investigate whether the equipment foreseen can be anticipated to remain functional under the prevailing conditions. This should include the instrumentation. For example, if a containment is to be flooded, instrumentation may get lost, or a connection to the containment vent may be flooded. In a number of cases, such analysis was not made.

### *6. Not considering the impact of the severe accident environmental conditions for the instruments which are read to initiate SAGs*

A very serious error which was often observed is neglecting of the impact of the severe accident environment on the plant instrumentation. Instrument were read at face values and action initiated on the basis of these values. For example, the SG water level measurement depends on the containment pressure – ignoring this gives false information on the SG water content. This was also the trigger of the TMI-s accident, as operator believed the RPV was full, because the pressuriser was full. Similar in one of the Fukushima units, where it was erroneously believed the RPV level was still appropriate.



*7. Not considering the potential negative consequences of planned mitigative actions.*

Unlike in EOP-domain, planned actions can also have negative consequences. An example is using the containment spray, which is always beneficial in EOP-domain, but can in SAMG-domain de-inert an initially inert containment atmosphere and so cause a hydrogen explosion. Also, the various SAMG approaches warn for such negative consequences. In the exercises observed, however, the question of potential negative consequences of proposed actions was seldom – or not at all – asked. Apparently, the mindset of TSCs was still in EOP-domain, where such questions are not relevant, as the outcome of planned actions is well-known beforehand.

*8. Lack of understanding the available time windows for mitigative actions.*

A severe accident has a certain evolution: various phenomena occur in a time sequence. For example, an early threat to the FPBs is a SG tube creep rupture, a later threat is the RPV meltthrough, and an even later threat the failure of the containment by overpressure (assuming no earlier failure due to hydrogen explosion). This gives a certain sequence of the needed counter measures, where these also are bound to a certain time limit. In a number of cases, however, it was observed that the TSC had no feeling for the available time for mitigative actions. For example, it took them 1.5 hours to re-establish the feeding of the steam generator – which time is not available under the threat of an SG tube creep rupture. It must be said that here the generic SAMG mostly does not give guidance either – this insight is really to be developed on a plant-specific basis.

*9. Lack of integration between the various procedures*

NPPs usually have procedures/guidelines of various types for accidents: for the operator using the EOPs, for the TSC (mostly) for SAMG, including the use of portable equipment (sometimes called FLEX, for 'flexible response', and the guidelines are FLEX Support Guidelines), plus the Technical Support Guidelines (TSG) for functioning of the TSC, for the ERO the emergency preparedness (EP), including response to extreme external events (mostly called Extensive Damage Mitigation Guidelines, EDMG). The complete set is then: EOPs, SAMG, TSG, FSG, EP, EDMG. Proper integration of these procedures/guidelines is essential, yet in observed exercised this integration was often not complete. A weak point is often notably the transition between EOPs and SAMG. Also often it was assumed that the TSC was already available at the beginning of the severe accident. Whereas in most cases the TSC staff is on call, and must come to the site. Often, no guidance was available what to do in between the exit of the EOPs and the beginning of execution of the SAMG under advice from the TSC. Note that this even happened in the generic approaches: in only one approach, such guidance was generically available, then called 'Severe Accident Control Room Guidance' (SACRG).

*10. Lack of proper verification and validation*

Once the SAMG have been written, they should be verified and validated. Verification should confirm that the latest insights have been incorporated, and that analyses are adequate and state-of-the-art. Validation means that the SAMG can be executed by trained staff. In a number of cases, verification and validation (V&V) were not adequate or not done at all. Absence of V&V is equivalent to absence of SAMG *at all*. A good practice is to involve sister plants in the V&V process, as well as in exercises/drills. In a number of cases, the V&V was very limited or practically absent. It also happened that the V&V included only a number of the severe accident guidelines. In one exercise, it was observed that only *one* SAG had been addressed.

*11. No SAMG on the system level*

A number of plants do not have SAMG on the system level – they use 'handbooks' or other documents that treat the phenomena of severe accidents, but without guidance on the system level. Although insights in such phenomena are helpful to select the proper strategy, it ultimately must be decided to take actions on the system level – but this requires threshold data, beyond which the system must be put into action. Where NPPs select this approach, it must be made clear by many exercises that it functions. Where this functioning must be demonstrated by all involved plant staff – the accident management should not be dependent on individual taste.

*12. Lack of proper training and exercises/drills*

A serious error which was observed a number of cases is that exercises/drills were executed on a *light* accident scenario. Plant staff was not really exposed to the complex conditions of a fully developed severe

accident, i.e. with large-scale core melting, large failure of supporting systems, loss of staff, loss of containment, etc. Including the shift of personnel and overnight duration. Apparently, the objective was to be ready before lunch time or before normal working hours were over. Such exercises cannot be seen as realistic training of the aspects of a severe accident.

In a number of cases, it appeared that training and exercises were only held *seldom*, say once per six years. Or that initial training was adequate, but no structured refresher training.

### *13. Lack of maintenance of SAMG*

Insights in severe accident have evolved over the time. In-depth research started after the TMI-2 accident and continues until today. Yet, some SAMG programmes have been observed to be based on the insights of 20-30 years ago. It also occurred that a certain generic SAMG was revised, but the NPP SAMG was still based on the old version. In one case, the Rev. 1 of a SAMG package had been on the shelf for 15 years, without anybody taking action – even not the regulator.

### *14. Lack of proper command and control*

In a number of cases (i.e. mostly) decision authority regarding the execution of SAMG actions shifts from the shift supervisor to another (usually: higher) level of authority, being a dedicated Site Emergency Director, for example the plant manager. In a number of cases it was not clear who ultimately was responsible for the final decision making on proposed actions. Or the shift of authority was not announced and, hence, not known to all involved.

### *15. Lack of staff responsibility and training.*

Not all NPPs had a clear description of the various functions in the ERO – some had no function description at all. Training programmes for these functions were then also lacking. It was even sometimes said: ‘we do training on the job’, which means in practice there is no training and people learn only from the exercises themselves. It also happened that people were aware of their function and authority, but did not follow their function. As examples: decision makers were busy in evaluation, ERO staff responsible for repairs was thinking about mitigative options or people started communications on a purely improvised manner. In a number of cases, the TSC had no staff member being an expert in severe accidents.

In addition, it should not be forgotten, that SAMG is guidance, i.e. no procedures which must be followed verbatim (as most EOPs). That is, the developers have included that deviation from the written guidance may be possible, or even needed. Such training was never observed, neither had exercises been designed in such a way that deviations should be considered, or even must be considered - for instance, if suddenly all instrumentation is dead.

### *16. Lack of communication between the TSC and the Control Room staff*

It is of vital importance that these two groups understand each other. The control room staff are licensed operators, the TSC staff are experts in various disciplines (e.g., reactor physics, thermal hydraulics, PSA, system engineering, electrical and instrumentation). Apparently, these two groups use different language. It is therefore beneficial if the TSC staff member who is assigned to communication with the Control Room, is him-/herself a licensed operator. In a number of exercised, this appeared to be not the case.

In addition, communication between the TSC and the Control Room should be regularly. It happened, however in one exercise that such communication did not occur *for hours*.

### *17. Lack of prediction of potential source term*

As severe accidents can result in large releases, one of the prime tasks of the ERO is to estimate the potential source term, to be communicated to the authorities, for their responsibility in protecting the public. In none of the observed exercises this was even tried. The focus apparently remained fully with regaining control of the plant, rather than protecting the public (and the plant staff).

### *18. Lack of emergency provisions at the ERO rooms/building*

In some of the exercises it was observed that plant staff in the Technical Support Centre (TSC) followed the evolution of the accident and the impact of mitigation measures on their laptops. As there was no emergency

power for the TSC, the laptops would run out of power in just a few hours, and all mitigation would come to an end. The building where the ERO gathered had neither emergency power, nor protection against radiation. During one exercise, it was concluded that the area within 4 miles from the plant had to be evacuated – whereas the ERO personnel – not being protected – did not move. Another plant, next to the shore, had an ERO building with rooms below ground level. As flooding is one of the severe accident initiators that must be considered, the plant would lose its ERO already at the beginning of the accident. Here only one conclusion can be drawn: an NPP that has no protection of its ERO facilities and no emergency power either *has no functioning SAMG at all*.

### 3. BENEFIT OF ADVANCED REACTORS

The development of advanced light water reactors (Generation III) has brought important improvements: these reactors have been *designed* to mitigate core damage accidents. This does not make the severe accident a design basis accident, as it is not possible to place stringent limits on the consequences of accidents where the accident evolution has still large uncertainties. And also because significant damage may have occurred on mitigating systems, which makes full control not possible. Yet, core catchers, such as the melt trap of new VVERs, the melt spreading room of the EPR, the BiMAC of some advanced BWRs have large benefits. Notably the complex events which occur in the case of vessel meltthrough have been largely eliminated.

These design usually also are equipped with passive systems, which makes the operator less dependent on active safety systems, such as emergency power, active emergency cooling water systems.

But many other challenges of FPB remain: SG tube creep rupture, hydrogen (if not mitigated by passive devices such as the Passive Autocatalytic Recombiners) and the massive release of fission products to the containment. In addition, some of these passive systems (notably check valves, squib valves) have a relatively bad operating experience and, hence, their probability of failure is non-negligible. And challenges by severe external events remain: earthquakes, fires, explosions, flooding. Hence, SAMG remains essential also for these advanced designs.

In addition, SAMG should be defined even for the least probable accident, according to [1], as long as such SAMG can be meaningfully developed. I.e., some of those mitigative systems may fail, and appropriate SAMG should be in place to mitigate those failures. Yet, from a risk perspective, plants may decide not to do this, as the investment is large and the anticipated benefit small.

The lesson of this consideration is that SAMG is and remains highly relevant, also for these advanced designs.

### 4. LESSONS LEARNED

The experiences assembled in the past reviews as assembled in Chapter 2 indicate that the development of a SAMG programme requires a large commitment of the NPP management to have it developed, staffed, trained and maintained. The development of SAMG is by far not a side line activity, to be undertaken if all other duties have been completed. An additional responsibility rests here on the utilities, as SAMG is often outside the regulated regime and, hence, no in-depth involvement of the regulator can be anticipated.

Doubtless, the Fukushima-Daiichi accident will not be the last severe accident in the upcoming times: somewhere, at some plant, another severe accident will occur – no plant is immune to severe accidents. Hence, the proper development, application, training and maintenance of the plant SAMG programme is of utmost safety importance: the next severe accident must find us prepared.

### 5. CONCLUSIONS

The development of an adequate SAMG programme is a large task with many pitfalls and other chances for failure, as reported in Chapter 2. It requires an in-depth programme, full commitment of the licensee, regular training and adaptation to new insights that develop. It is recommended to follow the IAEA Safety Guide in Severe Accident Management, [1], in all aspects<sup>1</sup>. Essential subparts of a SAMG programme are described in [7]. Third

---

<sup>1</sup>This document is at present under review, for inclusion of the lessons learned from the Fukushima-Daiichi accident.

party assessment by the IAEA in a RAMP mission (now part of the DSARS) or other group of qualified review experts is highly recommended.

## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Guide NS-G-2.15, IAEA, Vienna (2009).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for the review of accident management programmes in nuclear power plants, IAEA Service Series 9, IAEA, Vienna (2003).
- [3] REPORT OF THE RAMP (REVIEW OF ACCIDENT MANAGEMENT PROGRAMMES) MISSION to the Krško Nuclear Power Plant, Slovenia, IAEA TC Project RER/9/061, November 2001.
- [4] REPORT OF THE RAMP MISSION (REVIEW OF ACCIDENT MANAGEMENT PROGRAMMES) to the State Nuclear Power Safety Inspectorate (VATESI), IAEA TC Project LIT/9/006.
- [5] VAYSSIER, G., LUTZ Jr., R.J., BASIC, I., Review of Severe Accident Management at Point Lepreau Nuclear Generating Station, NSC 14/01, Rev. 1, January 2014.
- [6] HENRY R., et al., “Severe Accident Management Guidance Technical Basis Report”, EPRI TR 101869, Vol. 1 and II, Electric Power Research Institute, Palo Alto, CA, USA, October 2012.
- [7] VAYSSIER, G., “The Five Essential (“Key”) Elements of Severe Accident Management - to be Developed as Part of a SAMG Industry Standard”, paper presented at the ENS Topsafe Meeting, IAEA Vienna, February 2017.



**CROSS-CUTTING ANALYSIS AND PERSPECTIVES RELATED TO  
SEVERE ACCIDENT MITIGATION**

**Chairperson**

**K. ARAJ**  
Jordan



## **DEVELOPMENTS FOR NUCLEAR POWER PLANT SAFETY**

### ***Overview of Technology Developments for Continuous Improvements of Nuclear Safety***

T. YAMAMOTO

Nuclear Energy Systems Division, Mitsubishi Heavy Industries, Ltd.

Tokyo, Japan

Email: totofumi\_yamamoto@mhi.co.jp

A. OHNUKI

Nuclear Energy Systems Division, Mitsubishi Heavy Industries, Ltd.

Kobe, Japan

H. SHIMIZU

Research & Innovation Center, Mitsubishi Heavy Industries, Ltd.

Hiroshima, Japan

#### **Abstract**

Since Fukushima Daiichi Accident in 2011, improvements and strengthening of nuclear safety have been discussed and implemented in Japan. To strengthen nuclear safety with the concept of Defence-in-Depth, prevention of accidents is essential as well as mitigation of severe accidents. Several research and development (R&D) programs have been conducted to improve the safety of nuclear power plants (NPP) under the government support program in Japan. For instance, core cooling properties using steam generators under station blackout condition were verified. For instance, an evaluation method for a seismic isolation system considering beyond the design conditions has been established. This paper reports an outline of the results of typical R&D programs and discusses the direction of R&D to improve NPP safety.

#### **1. INTRODUCTION**

Since Fukushima Daiichi Accident in 2011, strengthening of nuclear safety has been discussed and implemented in Japan. To strengthen nuclear safety with the concept of Defence-in-Depth, prevention of accidents is essential as well as mitigation of the consequences of accidents. Several research and development (R&D) programs have been conducted to improve the safety of nuclear power plants (NPP) under the government support program in Japan since 2011.

#### **2. STRENGTHENING OF OVERALL NUCLEAR SAFETY**

Based on the lessons learned from Fukushima Daiichi Accident, the needs for technology development were discussed to strengthen NPP safety. According to the concept of Defence in Depth, the middle and long term direction and the technology developments were surveyed. This survey excluded near term countermeasures for NPP. The results of the survey for PWR plants are summarized in Table 1. As typical results, the core cooling measures using steam generators and the seismic isolation system for nuclear installations are shown in the following chapters.

#### **3. ADVANCES FOR CORE COOLING MEASURE USING SG SECONDARY-SIDE DEPRESSURIZATION**

##### **3.1. Background and R&D Activities**

In light of the lessons learned from station blackout (SBO) accidents of Fukushima Daiichi reactors, it is important to line up various cooling measures for the reactor core and containment. A reliable alternative safety measure has been developed to cool the reactor core under a small break loss-of-coolant accident (SBLOCA) of PWR using SG secondary-side depressurization, as shown in Fig. 1. This safety measure adopts an early SG



secondary-side depressurization to promote an early activation of accumulators (ACCs) and low-pressure injection (LPI) system.

For PWR plants, the SG secondary-side depressurization was investigated as a core cooling measure by Asaka et al. [1-3]. The study focused on the effectiveness of accident management (AM) by an operator action under total failure of a high-pressure injection system during SBLOCA, and the timing to open SG depressurization valves was relatively late such as 10 min after the event initiation. In contrast to the AM measure, the activation timing of this safety system adopts the period just after transmission of the Safety Injection (SI) signal.

TABLE 1. TECHNOLOGY DEVELOPMENTS BASED ON THE CONCEPT OF DEFENCE-IN-DEPTH (PWR)

Levels of DiD	Objective	Direction to strengthen safety functions	Technology developments
Level 1	Prevention of abnormal operation and failures	Earthquake-resistance	- Seismic isolation system - Enhancement of seismic evaluation method for steam generator
Level 2	Control of abnormal operation and detection of failures	Maintain subcriticality to cold shutdown only with control rods	- New core internals with many reactor control clusters - Enhancement of CFD analysis for core internals
Level 3	Control of accident within the design basis	Diversity for reactor core cooling	- Enhancement of core cooling capability by steam generator - Air cooling system/equipment
Level 4	Control of severe plant conditions	Cooling of melting core	- In-vessel retention for large reactor

There is no systematic validation database to assure the feasibility of the safety measure and therefore we planned to perform several tests using the ROSA/large-scale test facility (LSTF) [4]. The test parameters are (a) break size, (b) cooling capacity at each loop, (c) effect of dissolved nitrogen gas in ACC water and (d) onset timing of SG secondary-side depressurization.

The safety of an actual reactor should be checked by an analytical method that is validated using several appropriate databases. Therefore, the applicability of safety assessment code M-RELAP5 has been investigated using the test data. M-RELAP5 has been developed by Mitsubishi Heavy Industries, Ltd. (MHI) to analyze SBLOCA and SBO of PWR for licensing safety calculations. MHI specifically selected the best-estimate thermal-hydraulics code, RELAP5-3D [5], as the base code of M-RELAP5, and modified it by incorporating conservative models such that the code is applicable to licensing safety calculations [6].

In this chapter, we show some typical results for SBLOCA obtained in this project and the applicability of M-RELAP5. Then the impact for safety advances from this project is described.

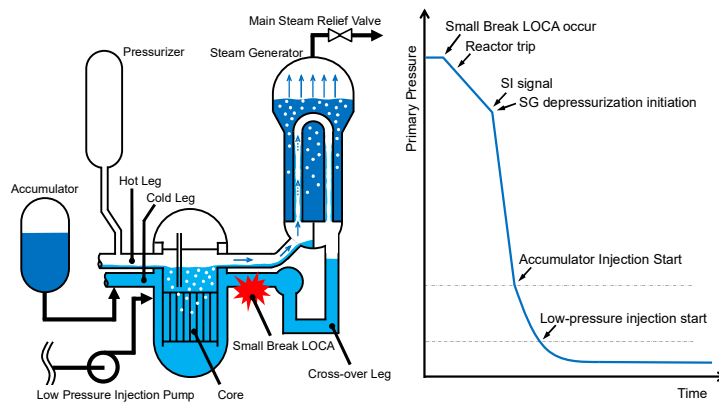


FIG. 1. Schematic of the safety measure against SBLOCA using SG secondary-side depressurization.

### 3.2. Typical Results

The test conditions were selected to cover typical phenomena encountered during SBLOCA. The tests were performed at several break sizes, i.e. 2-in., 4-in., 6-in., 8-in. and 10-in, which show the break diameter in an actual reactor. In this section, show the results for the 8-in. break test case where the highest PCT (Peak Clad Temperature) was recorded.

Fig. 2 and Fig. 3 show results up to 500s for the 8-in SBLOCA test. The break valve opened at 0s and then primary pressure reduced shortly thereafter due to the loss of primary coolant. After that, scram signal and safety injection signal initiated at 13s and 16s, respectively. SG secondary pressure increased due to the main steam isolation valve closing upon receiving the scram signal and then dropped rapidly after SG depressurization valve opened. Primary system remained cooled by the SG secondary side and the primary pressure decreased along the SG secondary pressure decreasing thereafter. The primary pressure decreases to the actuating level of ACC at about 350s which is earlier than the case without secondary-side depressurization.

After the break initiation, the core inventory was decreasing due to the break flow and the core began to uncover and heat-up from about 280s as shown in Fig. 3.3. Coolant injection from ACC initiated when the primary pressure became lower than the ACC pressure. Clad surface temperature shifted to decline and the heat-up was ended when the core was completely recovered.

M-RELAP5 code predicted well the overall trend of thermal-hydraulic response observed in the test. On the other hand, the code overestimated the clad surface temperature including PCT. In the calculation, some amount of condensed water accumulated along SG U-tube hot leg side and maintained due to so-called counter current flow limitation (CCFL) along the SG U-tubes. This condensed water increased the static head along the U-tube and contributed to push down the core liquid level. As the result, the code evaluated the higher PCT than the test. From the point of safety evaluation, M-RELAP5 code can give a conservative evaluation.

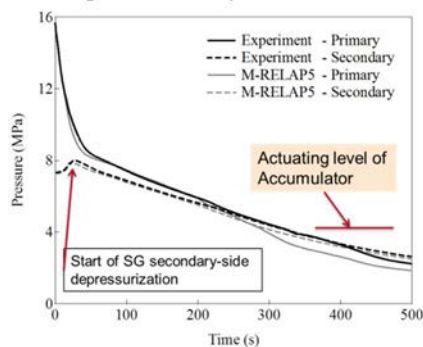


FIG. 2. Comparison of primary and secondary pressures between test and M-RELAP5.

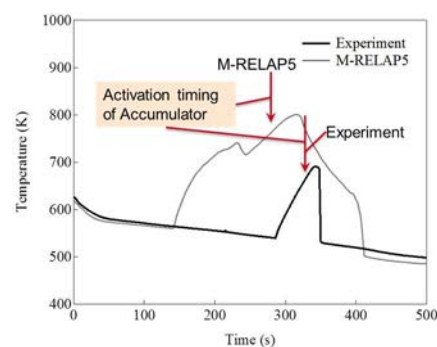


FIG. 3. Comparison of PCT between test and M-RELAP5.

### 3.3. Impact for Safety Advances

As described in Section 3.1, several sensitivity tests for break sizes, cooling capacity at each loop, effect of dissolved N<sub>2</sub> gas in ACC water and onset timing of SG secondary-side depressurization were performed. It was confirmed that M-RELAP5 is applicable to those several test parameters and is revealed to keep conservative predictions.

The results of this project provide technical evidence that the AM measure can be activated without any concerns regarding several uncertainties. This contributes to enhance the reliability of the AM measure and is useful for refining the time-margin for operator action in future.

## 4. DEVELOPMENT OF SEISMIC ISOLATION SYSTEM FOR NUCLEAR FACILITIES

### 4.1. Purpose of developing the seismic isolation system

In order to secure the integrity of reactor buildings against huge earthquakes in the future, base isolation systems are effective approaches and could also realize the standard design not to depend on site conditions.

At the aim of adopting a seismic isolation system to nuclear facilities, this project studied the following items; (1) obtaining highly aseismic performance by installing base-isolation, (2) grasping the ultimate strength of isolator based on the full-scale breaking tests, and (3) establishing the evaluation of “a residual risk” for phenomena exceeding the design conditions.

#### 4.2. Contents of developing the seismic isolation system

In this project, the ground motion for seismic study used an artificial wave enveloping general Japanese NPP sites, which of the maximum acceleration was  $800 \text{ cm/sec}^2$  and the maximum velocity was  $200 \text{ cm/s}$ . The study isolators adopted a lead rubber bearing (LRB) of 1600mm diameter, which was one of the largest scale in Japan. As shown in Table 2, this project studied characteristic tests of full-scale isolators, design seismic evaluation of base-isolated building, verification tests of crossover piping between base-isolated and non-base-isolated buildings, and residual risk evaluation against huge earthquakes in the future.

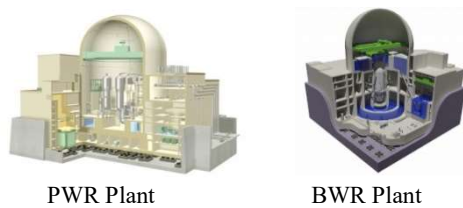


FIG. 4. Base isolation concept for NPP.

TABLE 2. DEVELOPMENT PROCESS

FY2008-2011	FY2012	FY2013	FY2014	FY2015
Preliminary Survey		Revise the Guideline "JEAG4614"		
	Rubber Bearing Breaking Tests			
	Cross-over Piping Tests			
	Study on Seismic Evaluation Method for Base-isolated Building			
		Establishment of Seismic Evaluation Method including Residual Risk Evaluation		

#### 4.3. Overview of development results

It was confirmed that the seismic isolation system is applicable to actual NPP's facilities such as the base-isolated buildings, and this project completed infrastructure improvement for deployment to actual NPP. The development results are overviewed as follows.

##### 4) Characteristic tests of full-scale isolators

As shown in Fig. 5, static breaking tests using the 1600mm-dia. LRBs were performed for the first time in the world. These tests determined various characteristics such as the breaking capacity, and this project created a design restore model combining horizontal and vertical, the schematic diagram for full-scale breaking capacity and so forth.

##### 5) Design seismic evaluation of base-isolated building

Actual isolator specifications were decided by seismic design after studying ground motion, and seismic integrity was investigated based on the beam model and 3D-FEM model of base-isolated building as shown in Fig. 6. As a result, this project conducted a combined evaluation between horizontal and vertical for isolator, the rational design of isolated pedestal and so forth based on the testing results conducted by this project.

##### 6) Verification tests of the crossover piping between base-isolated and non-base-isolated buildings

The seismic relative displacement of crossover piping between these buildings was absorbed by routing design. This project verified the integrity of crossover piping by shaking tests using 1/10 scale routing as shown in Fig. 7 and the static-loading repeated tests using 1/4 scale piping, and reflected these test results in the crossover piping design.

##### 7) Residual risk evaluation

As the PRA method, this project studied the fragilities of base-isolated buildings based on various failure modes such as the failure probability of seismic isolators as shown in Fig. 8, and evaluated the validity of these fragilities.

##### 8) Conclusion and further work

Developing the base of the seismic isolation system in this project expanded the flexibility of the aseismic design to NPP's facilities. In future, further work is required to improve high damping isolators in preparation for further huge earthquakes, and examine fail-safe devices against earthquakes beyond the design basis.

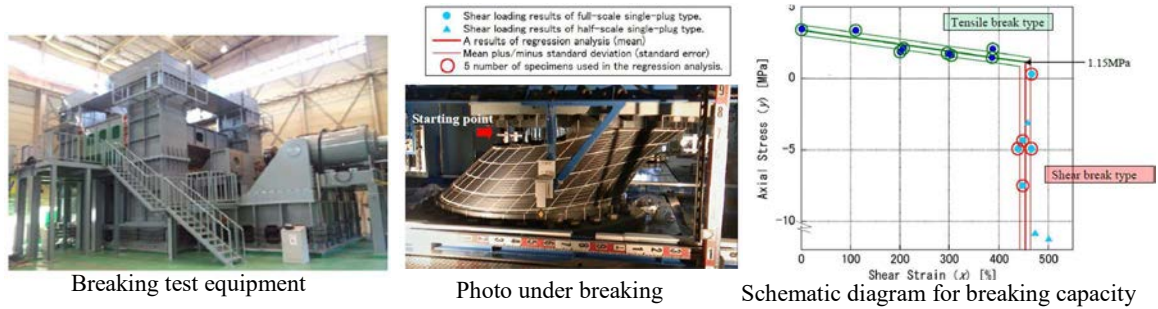


FIG. 5. Breaking tests of full-scale isolators.

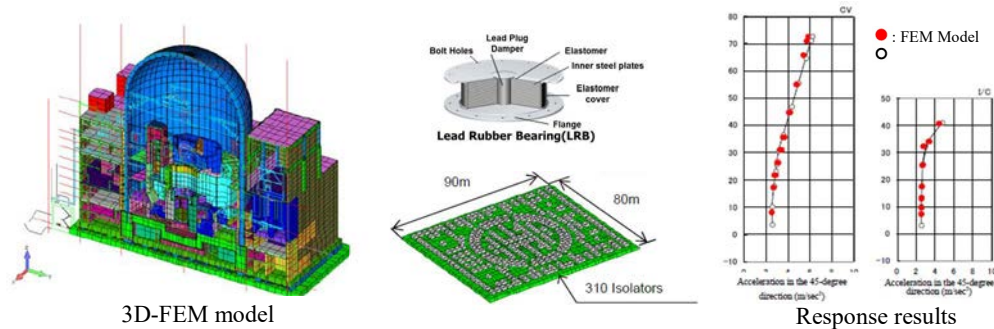


FIG. 6. 3D-FEM model of base-isolated building.

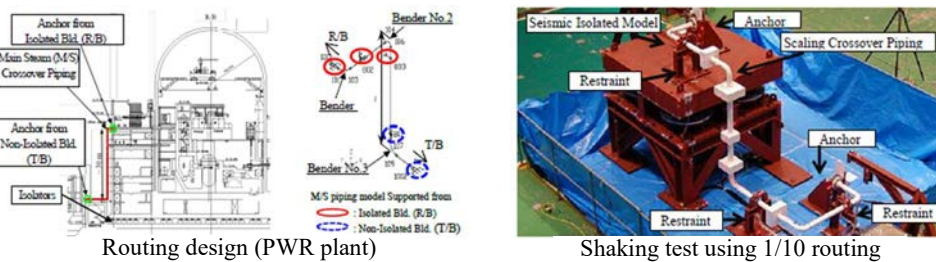


FIG. 7. Verification tests of crossover piping.

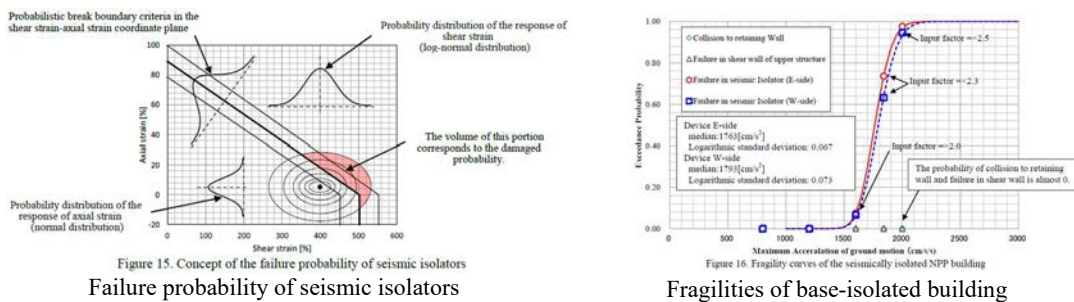


FIG. 8. Fragility evaluation of a quake-absorbing building.

## 5. SUMMARY

Based on the lessons learned from Fukushima Daiichi Accident, several technology developments to strengthen NPP safety have been completed in March 2017. The results will be considered for continuous improvement of NPP safety.

## REFERENCES

- [1] ASAKA, H., KUKITA, Y., Journal of Nuclear Science and Technology, Vol. 32, No.2 (1995) 101-110.

- [2] ASAKA, H., et al., *Journal of Nuclear Science and Technology*, Vol. 35, No.2 (1998) 113-119.
- [3] ASAKA, H., et al., *Journal of Nuclear Science and Technology*, Vol. 35, No.12 (1998) 905-915.
- [4] The ROSA-V Group, JAERI-Tech 2003-037, Japan Atomic Energy Research Institute (2003).
- [5] RELAP5-3D Code Manual, INEEL-EXT-98-00834 Revision 2.4 (2005).
- [6] MIWA, H., et al., NURETH-15, Pisa, Italy, May12-15, 158 (2013).
- [7] NUCLEAR STANDARD COMMITTEE, “Seismic Design Guidelines for Base-Isolated Structures of Nuclear Power Plant (JEAG4614-2013),” Japan Electric Association, Japan, 2013.
- [8] NUCLEAR STANDARD COMMITTEE, “Technical Code for Structure Design of Nuclear Power Plants (JEAC4601-2008),” Japan Electric Association, Japan, 2009.
- [9] JAPAN SOCIETY OF SEISMIC ISOLATION, “Design Guideline for Connection between Structure and Devices”, 2009.
- [10] MATSUOKA, S., TAKEUCHI, Y., et al., “Development of an Evaluation Method for Seismic Isolation Systems (Parts 1, 2)” 13th World Conference on Seismic Isolation, Energy Dissipation and Active Vibration Control of Structures, 2013.
- [11] SUZUKI, Y., et al., “Development of an Evaluation Method for Seismic Isolation Systems of Nuclear Power Facilities (Parts 1 to 11),” (Proc. of the ASME 2014).
- [12] KUBO, T., et al., “A Seismic Design of Nuclear Reactor Building Structures -Applying Seismic Isolation System in a High Seismicity Region – A Feasibility Case Study in Japan-”, Korean Nuclear Society, Nuclear Engineering and Technology, **46** 5 (2014) 581-594.
- [13] SHIMIZU, H., et al., “Development of Evaluation Method for Seismic Isolation Systems of Nuclear Power Facilities”, (Proc. 23rd Int. Conf. (SMiRT-23), **8** (2015), paper id. 119, 275, 291, 327, 344, 486, 611, 265, 293 and 259.

## **REGULATORY ASPECTS OF THE TARGETED SAFETY RE-ASSESSMENT AND THE EXPERIENCE GAINED FROM THE REGULATORY OVERSIGHT OF THE TSR RELATED ACTIVITIES**

A. SIKLOSI  
Hungarian Atomic Energy Authority  
Budapest, Hungary  
Email: siklosi@haea.gov.hu

### **Abstract**

On October 31, 2011 Paks NPP finished the so-called “stress tests” and submitted the Targeted Safety Re-assessment report to the Hungarian Atomic Energy Authority (HAEA). Based on the report the HAEA issued a resolution with several obligations for safety improvements and modifications for the licensee. The licensee’s action plan to fulfill these obligations contained deadlines for the 2011-2018 period, and during the last few years a considerable amount of regulatory experience was gained from the oversight of the related activities. This paper gathers and highlights the main experiences and findings, from a regulatory point of view, gained from the supervision activities of the licensee’s actions to fulfill these obligations, and also presents the amendments that were made to the Hungarian legal framework (mainly to the Nuclear Safety Code) after Fukushima to comply with the new international recommendations and trends.

### **1. INTRODUCTION**

The HAEA was able to identify good and bad practices based on the information and experience that accumulated during the supervision of the implementation of the corrective actions defined by the licensee and the HAEA. The aim of this paper is to list and give a brief description on these experiences in order to provide a source of information for any interested parties for harmonizing and/or amend existing regulations and regulatory practices.

Beside the main conclusions from the ongoing regulatory task of supervising the implementation of the corrective actions defined within the scope of the Targeted Safety Re-assessment this paper includes the regulatory experiences gathered from the on-site inspections.

### **2. BACKGROUND**

After the Fukushima Dai-ichi Accident the lessons that were learned have been evaluated in every country and by every utility operating nuclear power plants all over the globe in order to determine any and all possible risk factors that the nuclear facility may represent to the public and/or the environment. On 25<sup>th</sup> of March 2011 ENSREG, the nuclear advisory group of the European Commission was requested to provide a standardised methodology for the integrated risk and safety reviews of the NPPs operated within the European Union. Based on the requested methodology the Paks NPP done the re-assessment in two parallel processes. The first process addressed the nuclear safety issues (especially targeting the external events in their assessments and evaluations) while the second process addressed security issues.

The TSR of the Paks NPP was reviewed, approved and the case of the re-assessment was closed by Hungarian Atomic Energy Authority (HAEA) with the HA5444 resolution, which requested the licensee to propose a time schedule for the corrective actions to address the problems and deficiencies identified during the TSR by the licensee which was complemented by several further request made by the Authority. The licensee submitted its planned time schedule for these corrective actions which was approved by the HAEA with the HA5589 resolution and ordered the licensee to implement the corrective actions according to the approved schedule.

Within the scope of the TSR overall 46 corrective actions were identified and requested by the authority to be implemented in the 2011-2018 time period therefore some of these actions are still ongoing tasks at the moment of submission of this paper [1].

The defined tasks covered issues in almost all nuclear safety related areas, such as:

- General issues (e.g.: safety culture, review of the fulfilment of the regulatory requirements, etc.)



- External hazards and their assessments (e.g.: reassessment of external hazards and the evaluation of the risk of external hazard combinations)
- Emergency response (e.g.: Enhancement of Severe Accident Management Guidelines, Severe accident exercises, training of severe accident managements, etc.)
- Loss of safety systems (e.g.: alternate heat sinks, instrumentation and monitoring equipment improvement, improvement of ventilation capacity, enhancement opportunities for DC power supply, etc.)
- Etc.

During the planning phase of project, the tasks were scheduled the following:

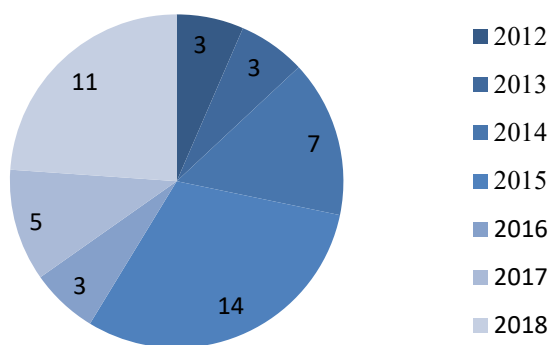


FIG. 1. Original schedule for the task completions.

## 2.1. Current Status of the Implementation of the National Action Plan

The status of the implementation of the National Action Plan is continuously monitored by the Regulatory Body to ensure that the notions of the HAEA and the licensee are met. The following tasks were completed and approved by the HAEA until 2016: 1.1, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.11, 1.13, 1.14, 1.17, 1.19, 1.20, 1.21, 1.22, 1.23, 1.24, 1.32, 1.33, 1.34, 1.35, 1.36, 1.37, 1.40, 1.41, 1.42., 1.43, 1.44, 1.45, 1.46 [2].

It can be said that most of the tasks were or are planned to be finished as scheduled. At the moment there are 15 remaining tasks within the framework of the NAP which are considered to be in the following status: regarding their compliance with the set deadlines:

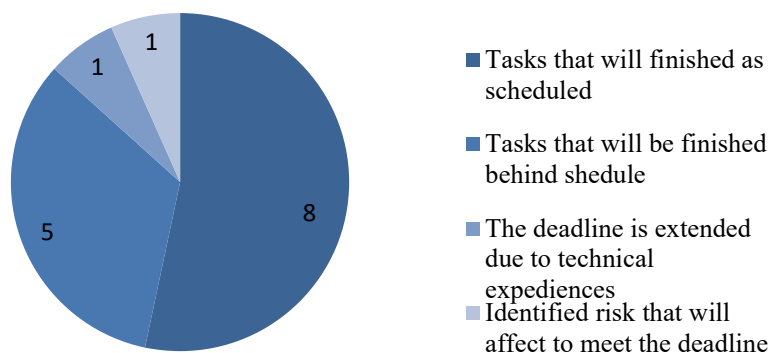


FIG. 2. Current status of the remaining tasks.

The basic approach of the HAEA is that in all cases where a task is not completed as scheduled, an assessment shall be carried out by the licensee to assess and evaluate the risk impact of the non-fulfilment and the

HAEA decides on further steps, using the validation tools as necessary. From the 5 tasks in question 3 was identified as a potential threat to the nuclear safety of the NPP, therefore the HAEA requested the licensee to carry out a comprehensive safety assessment for these cases.

### 3. REGULATORY EXPERIENCES AND IDENTIFIED GOOD PRACTICES

#### 3.1. Deficiencies in Planning

In the case of such a huge project it is of course almost inevitable to avoid all minor or even more marginal delays in the implementations as the project goes on, but it is in both parties interest to limit these delays as much as possible. The HAEA understood even in the beginning of the project the presence of these possible delays during the execution of the project there it required from the licensee to assess and evaluate the possible risk impacts of the delays. Overall from the 46 defined corrective actions 7 were finished ahead of schedule (in some cases even 1 or two years earlier), but in the case of 5 tasks the licensee reported and requested to extend the deadline.

An obvious case of the deficiency in planning was task 1.31 where the regulatory body requested the licensee to develop and install a backup data storage (so-called “Informatics Mirror Storage”) at the Protected Command Centre and the Backup Command Centre containing the necessary scope of data (such as technical documentation, personal data, etc.) The problem with the implementation of this backup storage was that the deadline for Task 1.31 was 15.12.2015 while the construction work of the Backup Command Centre to house the data storage was re-scheduled to 2018. Since there was no way to install the backup data storage before the completion of the building itself, the deadline of task 1.31 was extended after 2018 as well.

Overall there are two main conclusions that can be drawn from the regulatory experiences regarding the planning phase of such a project:

A special attention has to be addressed by the reviewers not just for the practicability of the proposed periods to implement the required tasks themselves but if possible a most comprehensive review of any and all preliminary condition that may affect the completion of the task shall be evaluated in a manner that it considers possible changes to the plans to finish the necessary preliminary tasks. In order to be able to review the schedule in such manner it is important that the licensee and the regulatory body consults on these issues before the review itself is done.

Ultra-conservative approaches shall be avoided during the setting of the deadlines, and the regulatory body should review the deadlines not just from the point of sufficiency but also from the point of practicability.

Since the tasks were defined based on their relevance to nuclear safety in order to correct these deficiencies any deviation from the approved schedule could represent a risk impact on the nuclear power plant, it was considered as a good practice by the HAEA to require the safety assessment and evaluation of these deviations from the licensee.

#### 3.2. Continuous inspection of the task implementations

Even in the beginning of the project a decision at the regulatory body was made that the completion of the set tasks shall be monitored and supervised continuously as the implementation goes on. Based on this pre-defined approach the HAEA executed sometimes even 6-7 inspection per year in this field. This sort of intense inspection schedule have given the licensee and the regulatory body a platform for consultation therefore it helped the interested parties to always have almost up-to-date information about the current status of the tasks and activities as well as it helped to converge the different point of views about the implementation of the set tasks.

### 4. CHANGES MADE TO THE HUNGARIAN LEGAL FRAMEWORK AFTER FUKUSHIMA

In parallel with the implementation of the tasks in the National Action Plan the HAEA began the review of the Hungarian legal framework based on the lessons learned from Fukushima and the new international experiences and the amended recommendations made after Fukushima. The review was mainly based on the following documents:



OECD/NEA Nuclear Safety Response and Lessons Learnt, The Fukushima Daiichi Nuclear Power Plant Accident,

IAEA, Mission Report, The Great East Japan Earthquake Expert Mission

WENRA RHWG, Updating WENRA Reference Levels for existing reactors in the light of TEPCO Fukushima Dai-ichi accidents lessons learned

IAEA GSR Part 1

IAEA GSR Part 4

IAEA SSR-2/1

IAEA SSR-2/2

IAEA NS-R-3

The regulatory review identified several deficiencies within the legal framework and based on the international experiences and recommendations the following amendments were made to the Hungarian regulations:

It is now required to consider the cliff-edge effect especially during the assessment of external events and also to consider the effects of the possible combinations of such hazards;

It is now required from the licensee to obtain and operate mobile equipment (e.g.: diesel generators)

It is now required to consider, assess and evaluate to possible interaction between the unit on a multi-unit site during external;

It is now required from the licensee to install and operate a Backup Command Centre in addition to the previously existing Protected Command Centre;

The new regulation requires the licensee to develop plans for the radioactive waste management after an accident;

The definitions and the requirements for Design Extension Conditions were clarified;

It is now required from the licensee to obtain the necessary equipment and develop the necessary guidelines and procedures for the severe accident management after a large release has taken place.

## REFERENCES

- [1] HUNGARIAN ATOMIC ENERGY AUTHORITY, National Report of Hungary on the Targeted Safety Re-assessment of Paks Nuclear Power Plant, Budapest, 2011.
- [2] HUNGARIAN ATOMIC ENERGY AUTHORITY, National Action Plan of Hungary on the implementation actions decided upon the lessons learned from the Fukushima Daiichi accident, Budapest, 2012.

# **RELAP/SCDAP SENSITIVITY STUDY ON THE EFFICIENCY IN SEVERE CORE DEGRADATION PREVENTION OF DEPRESSURIZATION AND WATER INJECTION INTO STEAM GENERATORS FOLLOWING SBO AT A CANDU-6 NPP**

E. DINCA

National Commission for Nuclear Activities Control (CNCAN)

Bucharest, Romania

Email: elena.dinca@cncan.ro

D. DUPLAC

“Politehnica” University of Bucharest

Bucharest, Romania

## **Abstract**

The paper takes into consideration the issue of severe accidents prevention that became a serious and continuous concernment of the nuclear stakeholders, mainly after Fukushima Daiichi nuclear accident. The efficiency of the preventive measures considered to be applied needs to be verified, including by analytical calculations. One of the most challenging events for all nuclear power reactors is Station Blackout (SBO) that can conduct in some conditions to the loss of safety functions and as a consequence to a severe accident. Therefore, prevention of severe accident in this case has been sustained with different measures to avoid loss of reactor decay heat removal. The paper considers a CANDU-6 NPP in a SBO event and simulates the application of the main preventive actions at different moments after reactor shutdown in order to determine by this sensitivity study how long these measures are still efficient in removing reactor decay heat. The considered actions in a SBO case at CANDU-6 consists in maintaining the Steam Generators (SGs) as an efficient heat sink, by SGs depressurization and their subsequent gravitationally feeding with cooling water from the dousing tank, a passive large source of water present in CANDU-6 project. Simulations to verify by calculation this heat sink efficiency have been performed using RELAP/SCDAP/MOD3.6(a) computer code and CANDU-6 NPP specific models. Calculations performed for this sensitivity study showed that SGs can be in this case an efficient heat sink for a long period of time, till three hours since the SBO event initiation, so even after the SGs drying-out.

## **1. INTRODUCTION**

After Fukushima Daiichi nuclear accident, all European countries operating nuclear power reactors passed through a “stress-test” their Nuclear Power Plants, a re-assessment of nuclear safety in conditions of extreme external events and severe accidents. A number of general recommendations and country and plant specific recommendations resulted from this safety re-assessments, including measures for severe accident prevention and mitigation for existing reactors. These recommendations resulted in National Action Plans, containing actions, both for regulatory bodies and NPPs with the aim to increase the plants robustness and a better preparedness for severe accident management. Cernavoda NPP, from Romania, having two operating units equipped with CANDU-6 reactors has also taken measures for severe accident prevention, including for those resulted from the most challenging accident sequences, as SBO is, and also for verification and validation of the accident management measures considered in Emergency Operating Procedures (EOPs) and Severe Accident Management Guides (SAMGs).

In case of a Station Black-Out event at a CANDU-6 NPP, when all alternative power sources are lost, the reactor cooling can be lost too, if accident management measures are not considered in due time, and the damage of the reactor core is foreseen. The SBO event without any accident management measures was analysed many times, including by the authors of this paper (as in [7-9]) and the CANDU-6 plant systems behaviour is known. The sensitivity analysis presented in this paper has the aim to verify by calculation if the application of the management measures provided as in the SBO’ EOP or much later have success in ensuring an efficient heat sink for decay heat removal for a long-time period. The analysis determines also the time limits for the application of these measures, consisting in SGs depressurization and addition of water from the dousing tank by opening the Boiler Make-up Water system isolation valves.

The Romanian regulatory body, National Commission for Nuclear Activities Control (CNCAN), together with “Politehnica” University of Bucharest, performed calculations independent (by the designer and utility) and

alternative (to the calculations performed using CANDU specific codes) in order to verify the efficiency of SGs heat sink in removing the decay and avoiding severe accident in case of a SBO. SGs depressurization followed by water addition from the dousing tank into SGs were considered in this sensitivity study to be credited at different moments after SBO initiation, starting with 35 minutes - as it is stated into EOP for SBO, and till 3 h from the event initiation (about 1 h after SGs dry-out). The judgement of the efficiency of SGs in case of SBO was based on the behaviour of the primary circuit and reactor core, as a response to SGs make-up at different moments.

To perform this analysis, the best-estimate computer code RELAP/SCDAP/MOD3.6(a) was used together with CANDU-6 specific models. Different cases were considered in the analysis, with simulations performed for 20,000 s to 45,000 s, depending on the analysed case.

## 2. SHORT DESCRIPTION OF THE CANDU-6 REACTOR AND SAFETY FEATURES

CANDU-6 reactors are somehow different comparing with PWR or BWR reactors, from more design considerations. CANDU reactor is located in a horizontal calandria vessel (CV), around 6 m long and 6 m in diameter, containing 380 fuel channels linked with inlet and outlet feeders, attached to the inlet and outlet large headers, which are part of the Primary Heat Transport System (PHTS). CANDU6 reactor uses natural uranium as nuclear fuel, heavy water as reactor coolant inside the fuel channels, and heavy water as moderator, outside of the fuel channels but inside the calandria vessel. Each fuel channel is composed by a 6 m long pressure tube (PT) contained in a calandria tube (CT), the two tubes being separated by CO<sub>2</sub> for thermal isolation. PHTS is composed by 4 passes through the reactor, in 2 eight-shape independent loops, each having 180 fuel channels, 180 inlet feeders, 180 outlet feeders, 2 Reactor Inlet Headers (RIH), 2 Reactor Outlet Headers (ROH), 2 Steam Generator (SG), 2 primary pumps and large pipes for connection. Reactor inlet and outlet headers, SGs, pumps and large pipes are all located above calandria vessel with fuel channels inside. The two loops are interconnected and both are connected to the pressurizer, but in case of a LOCA they can be isolated, one by the other and also by the pressurizer. 4 Liquid Relief Valves (LRV) ensure the primary overpressure protection, discharging primary coolant into degasser condenser (DGC), when their pressure setpoint of 10.24 MPa(g) is reached. The ROHs normal operation pressure is 10 MPa (a). If the pressure increases in DGC over the setpoint of 10.16 MPa(g), two Relief Valves (RV), spring actuated, open and close to reduce the DGC tank internal pressure, discharging steam or/and heavy water into containment atmosphere.

The overpressure protection of the four SGs, vertical type with integrated preheater, is ensured by 16 Main Steam Safety Valves (MSSV), organized in 4 groups, both spring and pneumatic actuated. These MSSVs can also be used for a fast depressurization of SGs. This depressurization can be an automatic action, with opening of 8 MSSVs – when some specific conditions are met, or it can be performed by manual opening of MSSVs by the operator. In both cases there is a need only for power supplied by batteries, as the MSSVs are spring and pneumatic actuated and they have independent local tanks with compressed air for their opening. A field operator can block them in open position using a dedicated tool in order to create an open path for steam release from SGs to atmosphere. If it is necessary, the operator can open manually in the field MSSVs, pneumatically or using a dedicated tool.

A large amount of water, around 2,000 m<sup>3</sup>, is available in the dousing tank - located near the top of the containment, to ensure the cooling water for containment spray in a LOCA case and water for the Medium Pressure stage of the ECCS, can be also used in SBO event to recover the SGs inventory, pouring gravitationally through the BMW system piping and open valves.

CANDU-6 reactor shutdown is ensured by the two fast shutdown systems, provided by design, fail safe, acting in less than 2 seconds each on different trip parameters. Containment isolation, even at the loss of power (fail safe feature by design) as well as the dousing spray, local air coolers and Igniters, ensure the containment protection and prevent the radioactive releases into environment in case of an accident. The newer safety improvements after Fukushima Daiichi accident, including the hydrogen management using Passive Autocatalytic Recombiners (PARs) and the Emergency Filtered Containment Ventilation System (EFCVS), different AC power mobile generators and provisions for alternative heat sinks increased the capacity of the CANDU-6 plant to prevent the severe accidents and to mitigate their consequences.

### 3. DESCRIPTION OF SBO EVENT AT CANDU-6 REACTOR

In case of a SBO at a CANDU-6 NPP, the total loss of alternative power will determine the loss of nuclear fuel cooling, as the primary pumps, the main and auxiliary feedwater pumps, the feed pump and the shutdown cooling pumps. The batteries are still available to command the opening of some valves, as MSSV – for steam generators rapid depressurization, or LRVs for PHTS overpressure protection. Both sets of valves have also dedicated tanks with instrument air for valves actuation, so the loss of instrument air will not affect the opening of MSSVs and LWRs, at least for a while (longer than 2 hours).

Loss of nuclear fuel cooling, as a direct consequence of loss of all heat sinks, will conduct also to a possible loss of some barriers (cladding failure, discharge of a mix of fluids from PHTS to DC and the containment atmosphere, through the spring actuated Degasser Condenser Relief Valves (DCRV)). Reactor shutdown and containment isolation safety functions are not affected by the SBO event.

In case of a SBO, after reactor shutdown, the decay heat will be transferred by natural circulation from the reactor core to the SGs. The steam generated will be removed through the open MSSVs. The SGs initial inventory of about 40 t each will ensure the heat removal for about 2 h, when the boilers dry-out. Loss of heat sink after SGs boiling-off will determine primary circuit pressurization and LRVs opening to discharge heavy water into DGC. In turn, DGC tank pressurization will conduct to the spring opening of RVs, which will discharge steam and water into containment atmosphere. For a while, this path LRVs-DGC-RVs-containment atmosphere will ensure the reactor core heat removal but will also conduct to the primary inventory decreasing, which will lead to overheating of the nuclear fuel and to the fuel channel break, at around 13,000s since SBO initiation, according to [7, 8, 9]. Channels break determine a fast pressurization of the moderator and, after the calandria ducts rupture disks break, to the expulsion of a large amount of moderator into containment. The uncovering of some upper fuel channels will conduct to the overheating of the PT/CT and in not a long time to the channel disassembly and beginning of the core damage into severe accident. This scenario of SBO without any measure to protect the reactor core to fail, as it is briefly described above, has been analysed many times, using MAAP4-CANDU, ISAAC or even RELAP/SCDAP computer codes, as it can be seen in [1], too. This SBO scenario was analysed also by the authors of this paper, using the same version of RELAP/SCDAP computer code and the same models [7, 8, 9], in order to have a base for comparison with cases where different accident management measures are considered. It allows also to determine the time windows available to implement accident management measures considered to prevent the core degradation and avoid severe accident.

It was determined, and considered into dedicated EOP for SBO, that the most important measures in case of SBO are to ensure SGs as heat sink, preserving in the same time the primary coolant inventory. In order to keep SGs as a heat sink and remove the heat from the primary coolant, the SGs water inventory recovering has to be ensured. A large amount of water, around 2,000 m<sup>3</sup>, is available in the dousing tank - located near the top of the containment, to ensure the cooling water for containment spray in a LOCA case and water for the Medium Pressure stage of the ECCS. This water from the dousing tank can be also used in SBO event to recover the SGs inventory, pouring gravitationally through the BMW system. The SGs depressurization is mandatory to permit the gravitationally pouring of water, and also the opening of the Boiler Make-up Water system isolation valves to ensure the water path. Once the BMW valves are opened and SGs depressurized, the dousing tank water can ensure the SGs inventory for at least 27 hours, as it resulted from [6], with a maximum water flow of about 43 l/s, for all SGs, according to [6]. This prevents the reactor core conditions degradation and severe accident initiation, as the analysis demonstrated. As long the water is provided to SGs and steam is removed to atmosphere, the thermosyphoning ensures the decay heat removal. On long-term, the Emergency Power Supply system (EPS) or Mobile Diesel Generator (MDG) will supply the necessary electrical power and the EWS will provide water to SGs.

### 4. ANALYSIS METHODOLOGY, MODELS AND INPUT DATA

The analysis presented in this paper has been performed using RELAP/SCDAPSIM/MOD3.6(a) computer code, described in [3], [4], and [5], and also CANDU-6 NPP specific models. A detailed presentation of CANDU-6 NPP models for RELAP/SCDAP code (the PHTS model, the secondary side of SGs model, the CANDU-6 reactor core model - using RELAP5 and SCDAP components), the analysis methodology, assumptions, initial conditions and failure criteria used in the SBO accident analysis are basically the same as those used in [1], section

3.6, where SBO event, without any accident management measure applied, was analysed. The CANDU-6 specific models for RELAP/SCDAP code were developed in time by different Romanian specialists, interested in the study of CANDU-6 reactor in severe accidents and design basis accidents, using a best estimate computer code, an alternative solution to the CANDU specific computer codes. These specialists worked mainly with “Politehnica” University of Bucharest during different studies, including for PhD theses preparation.

The analysis presented in this paper has used a newer version of the REPAL/SDDAP code comparing with [1], and some improvements to models, as a more detailed model for the reactor core and for the LRWs-DGC-RVs path, in order to increase the accuracy of simulation (as the primary inventory discharged into containment from the primary circuit and the reactor core behaviour). The input model is for a generic CANDU-6 NPP. For the simulation of the SGs depressurization and water addition time-dependent conditions were used.

This study considered that the SGs depressurization followed by water addition from the dousing tank, essential in the case of SBO at a CANDU-6 reactor, are applied at different moments from the SBO initiation, in order to determine the time window in which their application conduct to efficient results in removing the reactor decay heat and prevent the core damage. The analysis presented in this paper has used a constant flow of water of 40 l/s of water from the dousing tank to all SGs after SGs depressurization. This flow resulted as optimum (according to [8]), to extract the decay heat from the primary coolant, and it was also confirmed by the tests performed during the stress-tests of Cernavoda NPP, as it is presented in [6]. The following cases have been considered for the analysis presented in this paper:

- SGs depressurization by automatic or operator action, at about 35 minutes after SBO initiation, as it is considered in EOP for SBO. Simulation was performed for SGs depressurization at 2200s, and water injection into SGs 100s later;
- SGs depressurization by operator action at 7200 s, 2h from the event initiation when the boilers dry-out, and water addition from the dousing tank into SGs after 100s;
- SGs depressurization by operator action at 9000 s (2.5 h), when LRWs already opened and discharged some water into DGC and then into containment by RVs, and water addition into SGs after 100s;
- SGs depressurization by operator action at 10800 s (3h), when a large amount of water has been lost from the primary circuit by the cycling opening of LRWs and DGC-RVs and water addition into SGs after 100s.

## 5. ANALYSIS RESULTS

In order to determine the CANDU-6 NPP behaviour in case of a SBO event, when the two important preventive actions (of SGs depressurization and water addition from the dousing tank) were considered in analysis, the evolutions of the following main parameters have been monitored and extracted in graphs:

- PHTS pressure, considering the pressure in ROH (Pa);
- The SGs water level (m from the tube-sheet or water inventory in SGs, - kg);
- Maximum fuel surface temperature (MFST - conservatively the cladding temperature is considered at this value,) – K degrees; this is the most important parameter, showing if the nuclear fuel is adequately cooled or not;
- PHTS coolant inventory, in the two loops, important mainly after LRWs-DGC-RVs path opening (first time at around 9000s, according to [6, 8]) – considered only for the case (d).

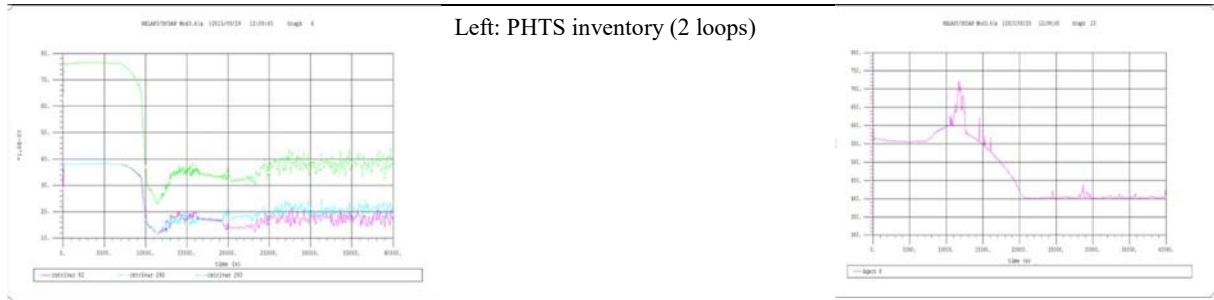
The following results have been obtained, sustained by the graphs presented in TABLE 1:

- a) In the case (a), meaning the actions taken as in the EOP for SBO, the SGs depressurization followed by the water addition in the SGs at a flow rate of 40 l/s determines the PHTS depressurization, with a maximum of 2.4 MPa. SGs inventory starts to recover and arrives at around nominal value at approximately 7 h (25000 s); after this moment, the flow to the SGs can be reduced significantly, as the decay heat decreased, too. As LRVs do not open in this case, the PHTS inventory remains constant and the fuel well cooled (the maximum fuel surface temperature remains less than 500 K).
- b) In case (b), the SGs depressurization and water addition into SGs occur after 2 h since SBO initiation, at this moment SGs being all almost empty (according to [7]). As the LRVs did not open yet, the PHTS inventory is still constant. The maximum fuel surface temperature does not increase over, the fuel remaining well cooled on long term. This case being bounded by the case (c), the PHTS pressure and SGs water level are not presented.

- c) In this case, the LRVs already opened but they didn't reduce the PHTS inventory till the SGs depressurization. Even if water is added 100 s after SGs depressurization, it is not enough to stop the tendency of PHTS pressure increasing, and for a short period of time LRVs and DGC-RVs will open and discharge some heavy water into containment. The heat removed by the water added into SGs will succeed to decrease the PHTS pressure and cool adequately the nuclear fuel. The maximum fuel surface temperature does not increase over 600 K.
- d) The case (d) is the limiting case analysed, in which the SGs depressurization followed by water addition into SGs can be considered still a success from the point of view of the fuel temperature. This can be seen in the graph presenting the maximum fuel surface temperature which indicates that the fuel become still well cooled, as the value of this parameters does not increase over 750 K, meaning less than 500 C (cladding failure is not expected at this temperature). On long term, this temperature remains almost constant, at around 400K. The LRVs-DGC-RVs opening allowed a large amount of heavy water to be discharged from the PHTS, approximately half of each loop inventory being lost. This discharge will probably conduct to the containment pressurization, situation that needs to be analysed.

TABLE 1. COMPARATIVE BEHAVIOUR OF CANDU-6 PHTS AND SGs IN CASE OF SBO WITH SG'S DEPRESSURIZATION AND WATER ADDITION INTO SG'S AT DIFFERENT TIMES

SGs water level (m) – over tube-sheet	ROH pressure (Pa)	Maximum fuel surface temperature (°K)
(a) for SGs depressurization at 2200s, and water injection into SGs 100s later		
(b) SGs depressurization at 7200s, and water injection into SGs 100s later		
(c) SGs depressurization at 9000s, and water injection into SGs 100s later		



(d) SGs depressurization at 10800s, and water injection into SGs 100s later

## 6. CONCLUSIONS

This sensitivity study has indicated that SGs can become and remain an efficient heat sink following a SBO event at a CANDU-6 NPP, when the SGs depressurization is performed before 3 h following the SBO initiation and water is added in less than 100 s, with a minimum flow rate of 40 l/s.

SGs depressurization followed by water addition are able to maintain the efficient core cooling and integrity, preventing the severe core damage.

In case of a very late SGs depressurization followed by water addition (between 9000-10800 s), even if the fuel surface temperature indicates a success regarding the fuel cooling, a significant amount of heavy water can be discharged from the PHTS through LRVs – DGC-RVs open valves and can possibly determine the containment pressurization over the containment spray setpoint. This situation needs to be analysed separately, as well as the configurations in which BMW isolation valves and MSSVs could be. Therefore, it is considered that SGs depressurization and water addition from the dousing tank through the BMW isolation valves after 2.5 hours from the SBO event initiation are risky and not recommended because a containment breach could eventually occur in this case.

## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Benchmarking Severe Accident Computer Codes for Heavy Water Reactor, IAEA-TECDOC-1727, IAEA, Vienna (2013).
- [2] PETOUKHOV, S.M., MAAP4-CANDU simulation results for CANDU 6 accident management measure: steam generator secondary side water make-up from dousing tank for the station blackout scenario, The 19th Pacific Basin Nuclear Conference (PBNC 2014), Vancouver, British Columbia, Canada (2014).
- [3] SCDAP/RELAP5 Development Team, SCDAP/RELAP5/MOD3.2 Code Manual, Vol. 1-5, NUREG/CR-6150, INEL-96/0422, 1998.
- [4] SIEFKEN, L.J., ALLISON, C.M., HOHORST, J.K., RELAP/SCDAPSIM/MOD3.5 – Improvements Resulting from QUENCH and PARAMETER Bundle Heating and Quenching Experiments, ISS, Idaho Falls, USA (2010).
- [5] BONELLI, A., MAZZANTINI, O., DUPLAC, D., DINCA, E., SIEFKEN, L.J., ALLISON, C.M., HOHORST J.K., RELAP/SCDAPSIM/MOD3.6 – Development of Severe Accident Models for Heavy Water Reactors Including CANDU and Atucha-2, Proc. ICAPP 2015, May 03-06, Nice, France, (Paper 15080), 2015.
- [6] NATIONAL COMMISSION FOR NUCLEAR ACTIVITIES CONTROL, “National Report on the Implementation of the Stress Tests”, CNCAN, Bucharest, Romania (2011).
- [7] DINCA, E., DUPLAC, D., PRISECARU, I., Analysis of the CANDU-6 Plant Behavior in Case of Very Late Steam Generators Depressurization and Water Injection Following a Station Black-Out Accident, U.P.B. Scientific Bulletin, Series C, Vol. 78, Issue 4, ISSN 2286-3540, Bucharest (2016).
- [8] DINCA, E., DUPLAC, D., PRISECARU, I., Verification by analytical means of the efficiency of some accident management measures for SBO at CANDU6 NPP, International Nuclear Safety Journal, vol. 4, issue 3, pages 9 – 22, ISSN 2285 – 8717, 2015, <http://nuclearsafety.info/international-nuclear-safety-journal/index.php/INSJ/article/view/125>
- [9] DINCA, E., DUPLAC, D., PRISECARU, I., RELAP/SCDAP Simulation Results for CANDU 6 Accident Management Measure: Primary Heat Transport System Voluntary Depressurization following a Station Blackout, U.P.B. Scientific Bulletin, Series C, Vol. 78, Issue 3, ISSN 2286-3540, Bucharest (2016).

**SYSTEM, STRUCTURE AND COMPONENT (SSC) MODIFICATIONS TO  
COPE WITH SEVERE ACCIDENTS**

**Chairperson**

**D. LOY**  
Switzerland





## SAFETY ENHANCEMENT TECHNOLOGY DEVELOPMENT WITH COLLABORATIVE INTERNATIONAL ACTIVITY

K. ARAI  
Toshiba Corporation  
Yokohama, Japan  
Email: kenji2.arai@toshiba.co.jp

F. ISHIBASHI  
Toshiba Corporation  
Yokohama, Japan  
Email: fumihiko.ishibashi@toshiba.co.jp

### Abstract

IAEA report on reactor safety in the light of Fukushima accident highlighted the lessons learned in the key technical areas important for strengthening safety. These lessons are associated with severe accident management measures and, for the research and development (R&D) required to implement measures, it stresses the importance of an international coordinated approach. Since the accident, Toshiba has conducted R&Ds for the safety enhancement with the support from Japanese Government, which cover the key technical areas in the IAEA report.

Some of the Toshiba R&Ds have been progressed with the international collaboration. For example, the project to develop the accident tolerant fuel (ATF) which is an application of SiC composite to fuel materials has had technical interaction with OECD/NEA expert group on ATF. The passive debris cooling technology development project leverages the expertise and the test facilities in Kazakhstan to obtain the property data of refractory materials and erosion behavior under the core-melt temperature condition. The model enhancements of a severe accident simulation code, MAAP and Fukushima accident progression analysis have been conducted in collaboration with US-EPRI.

Those collaborations are effective to expedite the R&Ds with efficient use of the expertise available worldwide. The paper summarizes the achievements of these R&Ds focusing on the collaborative international activity.

### 1. INTRODUCTION

Fukushima accident identified significance of the measures against the external hazards and highlighted the need to enhance the defence in depth. Since the accident, Toshiba has conducted the technology development for the safety enhancement of nuclear power plants with the support from the Japanese Government. Those technology developments covered a wide range of issues for the prevention and mitigation of severe accidents, which are selected and prioritized based on the Fukushima lessons learned.

IAEA report [1] on reactor safety in the light of Fukushima accident highlighted the lessons learned in the following key technical areas important for strengthening safety:

- Defence in Depth,
- Extreme events/ external events,
- Station blackout and loss of ultimate heat sink,
- Hydrogen management,
- Containment system and venting,
- Severe accident management,
- Instrumentation and control (I&C),
- Spent fuel pools,
- Research and development (R&D).

These lessons are associated with safety measures for the prevention of accidents or the mitigation of accident consequences. For the research and development (R&D) required to implement measures, it stresses the importance of an international coordinated approach.

The above-mentioned Toshiba's R&D activity covers the key technical area identified in the IAEA report. Some of the Toshiba R&Ds have been progressed with the international collaborations which are effective to expedite the R&Ds with efficient use of the expertise, facilities and experiences available worldwide. The paper summarizes the overview and achievements of these R&Ds focusing on the collaborative international activity.

## 2. OVERVIEW OF R&amp;D ACTIVITY FOR SAFETY ENHANCEMENT TECHNOLOGY

Fig. 1 illustrates the overview of the R&D activities which Toshiba has conducted with the support from the Japanese Government after the Fukushima accident. The R&Ds covers the technologies regarding core/ debris cooling, containment integrity and hydrogen management in both pre- and post-core damage phases of an accident. Those for improving the severe accident simulation capability, instrumentation during a severe accident, DC batteries and seismic protection technology are included as well. The international collaborations play an important role in the R&Ds for passive debris cooling technology, accident tolerant fuel (ATF) and MAAP model enhancement which are described in the following section.

	Pre-Core Damage	Post-Core Damage (In-Vessel)	Post-Core Damage (Ex-Vessel)
Core / Debris Cooling	ATF (SiC: Enhanced Tolerance to Loss of Core Cooling)	In-Vessel Retention External Cooling	Passive Debris Cooling / MCCI Prevention
Containment Integrity		Passive Decay Heat Removal	Scrubbing/ Filter Venting
Hydrogen Management	ATF (SiC: Less-H <sub>2</sub> Production)	Passive H <sub>2</sub> Removal with Metal Oxides	
SA Simulator	MAAP Model Development/ Improvement		
Instrumentation	SA-Phenomena related Parameter Measurement Technology		
Battery	Large Capacity Li-ion Battery (SCiB™)		
Seismic Protection	Oscillation Damping/ Isolation		

(ATF: Accident tolerant fuel, SiC: Silicon Carbide)

FIG. 1. Overview of Toshiba's R&D Activity for Post-Fukushima Safety Enhancements.

Other major activities listed in the table are briefly summarized below.

(a) In-Vessel Retention for Debris Cooling [2]: In-Vessel retention (IVR) technology has been studied in order to estimate the success probability of IVR for a large PWR with obtaining critical heat flux (CHF) data under a wide variety of the thermal-hydraulic conditions which can be encountered during hypothetical accident scenarios. The CHF enhancement effect of nanoparticles has been also experimentally studied. The Risk-Oriented Accident Analysis Methodology (ROAAM) was applied to estimate the success probability with using the CHF data and confirmed that it is very likely for a 4500MWth-class PWR to maintain the core debris inside of the reactor vessel by the external cooling.

(b) Passive Containment Cooling for Containment Integrity: The passive containment cooling system (PCCS) with horizontal U-tube type condensers has been developed and the feasibility to conventional BWRs has been studied after the Fukushima accident. Thermal-hydraulic experiments have been conducted to clarify the transient behaviours of both PCCS and the containment considering SA scenarios in conventional BWRs by using the large scale containment test facility in Toshiba. The test results clarified the fundamental phenomena which determine the PCCS performance and demonstrated the effectiveness of the PCCS to suppress the containment pressure rise even in the conventional BWRs.

(c) Passive Hydrogen Removal for Hydrogen Management [3]: A massive amount of hydrogen can be generated by the metal-water reaction during a severe accident and becomes a threat of the containment overpressure and the hydrogen combustion in a secondary containment of a BWR. The hydrogen removal

performance of metal oxides has been examined under a typical severe accident condition and the concept of the hydrogen removal system is developed to be used in inerted atmosphere of a BWR primary containment.

(d) Instrumentation for Monitoring Severe Accident Condition [4]: Considering the severe condition during a severe accident, instrumentation has been developed for monitoring the reactor pressure vessel water level, hydrogen concentration and containment water level. The performance of the instrumentation was examined and confirmed under the severe accident condition.

### 3. R&D ACTIVITY WITH INTERNATIONAL COLLABORATION

#### 3.1. Passive Debris Cooling: MCCI Prevention Technology [5-7]

The R&D activity has progressed to develop a measure for conventional BWRs containments in order to prevent the MCCI which becomes a threat to the containment integrity. It has a refractory layer to prevent the direct contact between the core debris and the concrete containment by sustaining the debris on the layer.

Series of experiments were conducted to obtain the thermal properties data of candidate refractory materials ( $\text{Al}_2\text{O}_3$ ,  $\text{MgO}$ ,  $\text{ZrO}_2$ ) under the severe accident temperature condition and to investigate the erosion behaviour of the materials due to the molten debris by using the dedicated test facilities on different scales in Japan and Kazakhstan. A large scale test using 60 kg  $\text{UO}_2$  debris was carried out at the National Nuclear Center (NNC) of the Republic of Kazakhstan for the investigation of the interaction on the refractory material. In addition, a small scale apparatus was used as well for thermal erosion tests at NNC (Fig. 2). These test results will contribute to establishing the evaluation model for the thermal and chemical interaction between the debris and refractory materials. NNC has accumulated a lot of experience and expertise for the high temperature debris experiment using  $\text{UO}_2$  with the dedicated test facilities. These are essential to obtain the data in an efficient and expedited manner. The collaboration was reported in the country report of the Republic of Kazakhstan at Forum for Nuclear Cooperation in Asia (FNCA) in 2016 [5].

One of major achievements was the establishment of the phase diagram for the composite of debris and refractory materials with different  $\text{UO}_2$ - $\text{ZrO}_2$  ratio. Figure 3 is an example in which the eutectic tests results, liquidus and solidus temperatures for  $(\text{UO}_2)_{0.42}$ - $(\text{ZrO}_2)_{0.58}$ - $\text{Al}_2\text{O}_3$  composite are compared with the phase diagram analysis results which was obtained by using FactSage, showing that the analysis result agrees well with the test data. Liquidus and solidus temperature data were obtained for several  $\text{UO}_2$ - $\text{ZrO}_2$  ratios in Japan and Kazakhstan which confirmed the validity of the phase diagram analysis. By leveraging these results, the refractory material will be selected for the MCCI prevention measure and the design will be established considering a wide range of accident scenarios.



FIG. 2. Erosion Test Vessel at NNC [6].

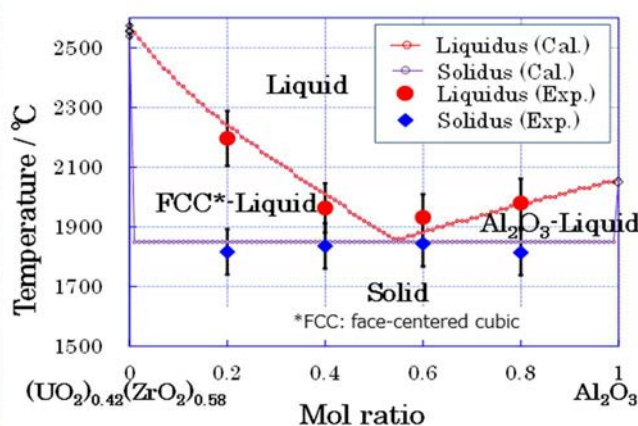


FIG. 3. Comparison between Phase Diagram Analysis and Eutectic Test data [7].

### 3.2. Accident Tolerant Fuel: SiC Application [8,9]

Fukushima accident highlighted the significance of the hydrogen management during severe accidents. The measures have been developed in two ways: One is to enhance the high temperature resistance of fuel material and suppress the hydrogen production caused by the metal-water reaction, that is the development of accident tolerant fuel (ATF). The other is to remove the excessive hydrogen passively in the inerted containment, which is briefly described in Section 2.

For the ATF development, Toshiba identified a silicon carbide (SiC) ceramic as the most promising ATF material since it has less chemically active characteristics under the high-temperature-water steam environment and a smaller neutron absorption cross-section. Toshiba has been participating in two joint teams, involving Ibiden Co., Ltd, Nuclear Fuel Industries Ltd., the University of Tokyo, Tohoku University, Kyoto University and Hokkaido University, and continued the development. Figure 4 shows the roadmap for SiC/SiC composite application to BWR channel box and fuel cladding.

One of the major challenges is to establish the fabrication technology. Toshiba and Ibiden have succeeded in the trial fabrication of the reduced-length channel box and cladding tube with SiC/SiC composite using CVD (Chemical Vapour Deposition) process (Fig. 5); the length of the channel box is 1000mm and the tube length is 800mm. R&D works are continued to achieve the full scale fabrication in parallel with the preparation for the irradiation tests.

ATF development activities are progressing at international level. Multidisciplinary and long-term research works are needed before ATF is put into practical use, which are related to but not limited to fabrication, normal reactor operations, safety, fuel cycle and economy. It is therefore indispensable to pursue efficient and effective research approach by leveraging international collaborations, expertise and facilities. Toshiba has shared the major progress of the development activity with the OECD/NEA Expert Group on ATF (EGATFL) and is participating in the development of the state-of-the-art report on ATF which summarizes the state of development, testing and/or development needs, and associated development risks in the NEA member countries. The report is expected to be a guide for efficient approaches for the development roadmap.

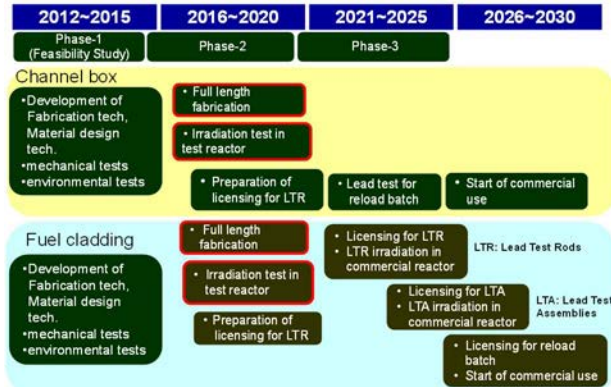


FIG. 4. Roadmap for Toshiba SiC Deployment [8].



FIG. 5. Trial of Channel Box and Cladding Tube [9].

### 3.3. SA Simulation Technology: MAAP Model Enhancement [10]

The Modular Accident Analysis Program (MAAP), which is an Electric Power Research Institute (EPRI) owned and licensed computer software, has been extensively used to analyse the progression of severe accidents. MAAP version 4 analysis results for accidents at Fukushima NPPs reasonably explained the plant parameters measured at the NPPs before the core melts occurred, and however, the agreements were not satisfactory for the post-core-melt consequences. In order to identify the analysis models of MAAP which should be enhanced especially for analysing the molten-core and debris behaviour, sensitivity study on uncertain boundary conditions in the Fukushima accident analyses, e.g. fire engine injection rate, was conducted. Based on the study results, following physical models are extracted as significant models for molten core and debris behaviour analysis:

- Core melt progression model; modelling of additional relocation paths including fuel support piece and shroud wall failure.
- Lower plenum (LP) model; increased nodalization of LP, CRD tubes and stratified debris bed in LP.

- Melt spreading and MCCI model; modelling of melt spreading, convective heat transfer in debris, and ablation front evolution, and update of corium-concrete properties.

These model enhancements have been implemented into MAAP in collaboration with EPRI. The updated MAAP, MAAP 5.03, has been applied to Fukushima accident analyses to support the decommissioning of Fukushima NPPs and has been benchmarked in the OECD/NEA/BSAF project (Benchmark Study of the Accident at the Fukushima Daiichi Nuclear Power Plant). Member countries and organizations in the MAAP Users Group can access the MAAP with the model enhancements. In Japan, MAAP 5.03 is implemented into the SA simulator for the Nuclear Regulatory Authority.

From the viewpoints of dissemination of the achievements in severe accident simulator model enhancements, the MAAP Users Group organized by EPRI is effective. OECD/BSAF is an excellent opportunity to share the state-of-the-art severe accident modelling and obtain experts' feedback on the further model improvements. The collaborative network plays an important role for advancing the severe accident modelling capability.

#### 4. SUMMARY

A wide range of the Post-Fukushima R&D activities has been conducted for the safety enhancement technology. The overview of the activities which Toshiba is leading is provided in the paper.

Some of the Toshiba R&Ds have been progressed with the collaborative international activities which play important role from following viewpoints:

- Efficient use of the expertise, facilities and experiences available worldwide.
- Pursuing efficient approach for multidisciplinary and long-term research works.
- Dissemination of R&D achievements to the international community.

#### ACKNOWLEDGMENTS

The R&D activities mentioned in the paper were financially supported by Ministry of Economy, Trade and Industry (METI) of Japan.

#### REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA report on reactor and spent fuel safety in the light of the accident at the Fukushima Daiichi nuclear power plant, IAEA, Vienna (2012), <https://www.iaea.org/sites/default/files/spentfuelsafety2012.pdf>
- [2] TSUDA, S., et al., "Study on In-Vessel Retention – Analysis of In-Vessel Retention using Risk Oriented Accident Analysis Methodology", Proc. ICAPP 2017, Fukui and Kyoto.
- [3] IWAKI, C., et al., "Development of Hydrogen Treatment System in Severe Accident (2) Study on Reaction Characteristic of a hydrogen proceeding unit", Proc. ICONE24-60917, 2016.
- [4] TAKEMURA, M., et al., "Development of Instrumentation Systems for Severe Accidents", Proc. ICONE23-1179, 2015.
- [5] Forum for Nuclear Cooperation in Asia (FNCA) 2016, Country Report of the Republic of Kazakhstan, [http://www.fnca.mext.go.jp/english/mini/report/17/Country\\_Report\\_Kazakhstan.pdf](http://www.fnca.mext.go.jp/english/mini/report/17/Country_Report_Kazakhstan.pdf).
- [6] KURITA, T., et al., "Evaluation Plan for Passive Debris Cooling System and Refractory Layer", Proc. ICAPP, Paper 14179, 2014.
- [7] TAKAHASHI, Y., et al., "Development of Passive Debris Cooling System", Fall Meeting of Atomic Energy Society of Japan, I12, 2014 (in Japanese).
- [8] KAKIUCHI, K., et al., "Progress on ATF Development of SiC for LWR", Proc. Topfuel 2016.
- [9] UCHIHASHI, M., et al., "Development of SiC/SiC Composite for Nuclear Reactor Core with Enhanced Safety", Proc. ICONE23-1387, 2015.
- [10] KOJIMA, Y., et al., "MAAP Enhancements for Ascertaining and Analyzing Reactor Core Status in Fukushima Daiichi NPP", Proc. ICAPP 2014.

## BRINGING SAFETY PERFORMANCE OF OLDER PLANTS ON PAR WITH ADVANCED REACTOR DESIGNS

A. VIKTOROV

Canadian Nuclear Safety Commission  
280 Slater St, K1P 5S9, Ottawa, ON, Canada  
Email: alexandre.viktorov@canada.ca

G. FRAPPIER

Canadian Nuclear Safety Commission  
280 Slater St, K1P 5S9, Ottawa, ON, Canada

### Abstract

The Canadian regulatory philosophy calls for continuous improvement in safety, to meet the changing expectations of the society. It is acknowledged that there are economic and physical limits to such improvements for existing facilities. Nevertheless, the advances in science, accumulation of experimental evidence, more powerful computational methods, proven design features of advanced reactor designs and better understanding of key risks arising from nuclear facilities - all this allow enhancing safety of facilities built to earlier standards.

The paper elaborates on recent developments influencing safety performance of Canadian nuclear power plants.

### 1. INTRODUCTION

Ours is a fast-paced world with every aspect of life incessantly changing, sometimes at a neck-breaking speed. The nuclear industry is not immune to this. The technology of safety, the societal expectations towards demonstration of safety and regulatory frameworks are different today from what they used to be thirty, twenty and even ten years ago.

In Canada, continuous improvement in safety performance is an accepted paradigm, in fact, a recognized strength of the regulatory and operational practices. Let us dwell first on the cornerstones of the Canadian regulatory philosophy prior to diving into the question how the continuous improvement is pursued and attained.

Under the *Nuclear Safety and Control Act* licensees are directly responsible for managing the regulated activities in a manner that protects health, safety, and the environment, while respecting Canada's international obligations. In other words, an organization operating a nuclear power plant bears primary responsibility for its safety. The regulator, Canadian Nuclear Safety Commission or CNSC, regulates the development, production and use of nuclear energy in order to prevent unreasonable risk to the environment, to the health and safety of persons, and to national security. The CNSC is answerable to Canadians for ensuring that the licensees properly discharge their responsibilities. This is achieved through [1]

- a) Setting regulatory requirements and assuring compliance
- b) Basing regulatory requirements and actions on the level of risk
- c) Making independent, objective and informed decisions, and
- d) Serving the public interest.

The very high level regulatory requirements are set in the law (*the Nuclear Safety and Control Act*), and Regulations under it and are relatively stable. Such, *the Nuclear Safety and Control Act* stipulates the following:

- §24 (4). Conditions for Licence issuance

No licence shall be issued, renewed, amended or replaced unless, in the opinion of the Commission, the applicant

- a) is qualified ...; and
- b) will make adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed.

The specific oversight requirements are spelled in regulatory documents and national standards which are significantly more agile. These documents can be and are periodically revised to reflect the best modern practices and in order to serve the public interest. The regulatory documents spell out attributes of a qualified applicant for a licence, and what constitutes adequate provisions for assuring nuclear safety. The development and update of



regulatory documents is under the control of the CNSC and is flexible enough to respond to the changing realities and expectations. We, the Canadian regulator, have also arrived at what we believe is a balanced approach for incorporation of new or revised regulatory documents into the compliance oversight (or, in other words, making them requirements) while recognizing the benefits of regulatory stability.

## 2. SAFETY AND CONTROL AREA FRAMEWORK

To promote consistency in compliance oversight across all regulated activities, CNSC staff developed a set of Safety and Control Areas (SCA) consisting of 14 subjects or themes. These Safety and Control Areas are used in planning and conduct of inspections, technical reviews, regulatory research and public reporting. They are also used to lend a structure to the regulatory framework across all types of nuclear facilities and activities. These 14 Safety and Control Areas are listed in Table 1; the corresponding regulatory documents can be found at <http://nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/index.cfm>

TABLE 1. CNSC SAFETY AND CONTROL AREAS

Management system	Conventional health and safety
Human performance management	Environmental protection
Operating performance	Emergency management and fire protection
Safety analysis	Waste management
Physical design	Security
Fitness for service	Safeguards and non-proliferation
Radiation protection	Packaging and transport

In the last decade, CNSC has been formalizing regulatory expectations (simultaneously bringing them in closer alignment with the IAEA guidance) as regulatory documents at a relatively fast pace adding several new or revised documents every year. We found however, that making all these new documents part of the compliance activities in an ad-hoc, piece-wise manner is burdensome for both the regulator and the regulated organizations. The preferred approach is to add the new requirements at the time of Periodic Safety Review (PSR) or relicensing<sup>1</sup> (nevertheless, when justified, new requirements can be implemented faster). The PSR itself is a relatively new practice in Canada but which has now become a formal requirement. Objectives of a PSR are seen as helping determine [2]:

- The extent to which the facility conforms to modern codes, standards and practices
- The extent to which the licensing basis remains valid for the next licensing period
- The adequacy and effectiveness of the programs and the structures, systems and components (SSCs) in place to ensure plant safety until the next PSR or, where appropriate, until the end of commercial operation
- The improvements to be implemented to resolve any gaps identified in the review and timelines for their implementation. Such improvements then become part of the licensing requirements.

The Periodic Safety Review offers a systematic and comprehensive approach for identifying safety improvements, in many cases bringing the facility in compliance with the letter or at least the intent of the modern requirements, standards and codes. Identified gaps are assessed to find a practicable resolution which may be either through design changes or modification of operational practices. Not every gap against the current requirements may be bridged in a cost-effective manner. Nevertheless, the advances in science, accumulation of experimental evidence, sharing of best practices among peers, more powerful computational methods, proven design features of advanced reactor designs and better understanding of key risks arising from nuclear facilities – all these are used to find ways for improving safety of the facilities build to the earlier standards. At the completion of a PSR, a licensee operating a NPP identifies a set of concrete and practicable safety improvements, often in response to gaps against the up-to-date safety requirements.

<sup>1</sup> In Canada, the nuclear power plants are relicensed at relatively short intervals, usually every five or ten years.



These two fundamental attributes of the Canadian regulatory regime, namely, a flexible regulatory framework and the periodic safety review process, allow implementation of safety enhancements in response to evolving societal expectations, regulatory priorities and technological progress.

### 3. SAFETY IMPROVEMENTS OF OPERATING NPP

Now, let's have a look at the operating nuclear power plants in Canada. All of the NPP are at least 24 years old; all of them either have undertaken a Periodic Safety Review or are in the process of completing one. The older units have all gone through a refurbishment. Refurbishment involves replacement of components that have reached the end of their operational life (major components may include pressure tubes of a CANDU reactor, steam generators, etc) and overhaul or upgrade of other systems where justified. Refurbishment of a reactor is undertaken during an extended outage and allows prolonging its operating life while at the same time implementing safety enhancements.

TABLE 2. OPERATING NPP IN CANADA

Reactor	MWe net	First power	Refurbishment	Periodic Safety Review
Pickering A1	515	1971	2005	PSR#2 in progress
Pickering A4	515	1972	2003	PSR#2 in progress
Pickering B5	516	1982		PSR#2 in progress
Pickering B6	516	1983		PSR#2 in progress
Pickering B7	516	1984		PSR#2 in progress
Pickering B8	516	1986		PSR#2 in progress
Bruce A1	750	1977	2012	Completed
Bruce A2	750	1976	2012	Completed
Bruce A3	750	1977	2004	Completed
Bruce A4	750	1978	2004	Completed
Bruce B5	825	1984	Planned	In progress
Bruce B6	825	1984	Planned	In progress
Bruce B7	825	1986	Planned	In progress
Bruce B8	825	1987	Planned	In progress
Darlington 1	881	1990	Planned	Completed
Darlington 2	881	1990	In progress	Completed
Darlington 3	881	1992	Planned	Completed
Darlington 4	881	1993	Planned	Completed
Point Lepreau	635	1982	2012	Completed

The list of operational and safety improvements generated by a PSR usually includes scores of items. Only a few of those may involve substantial design modifications. The significant design changes within the scope of PSR/refurbishment activities that were implemented in Canada include:

- installation of dedicated containment filtered venting system dedicated to design extension conditions
- provision of passive hydrogen recombiners inside the reactor building
- modifications to improve fire design
- installation of additional standby or emergency generators with increased seismic robustness
- replacement of computerized systems with modern digital assets
- installation of a post accident monitoring and sampling capabilities
- modification of instrumentation with increased measurement ranges and improved survivability
- implementation of additional systems to monitor and protect environment

In addition to design improvements, many other, programmatic, measures have been brought into the operational practices of the Canadian NPP as result of recent periodic safety reviews. No name just a few:

- incorporation of severe accident management guidelines
- verifying environmental qualification of equipment to the extended operational life duration
- verifying robustness against physical and cyber security threats, etc.

Of course, the other powerful impetus for safety improvements is arising from the operational experience, most visible recent examples of which are the Fukushima Daiichi accident in 2011, and the terrorist attacks in 2001. As a consequence of the latter, the physical security of nuclear facilities has been transformed in a very substantial way. Defining and assimilating lessons arising from the Fukushima event is still ongoing, but nowadays we pay much more attention and implement provisions to respond to the external hazards, multi-unit events, challenges to spent fuel safety, in particular to the events exceeding the original design basis.

In the aftermath of the Fukushima accident, operating Canadian nuclear power plants have implemented various physical and procedural enhancements, to meet the regulatory requirements and following the best peer examples. Such, the Canadian utilities added:

- capabilities to supply power to key safety systems in case of major accidents, including portable sources,
- capability to add coolant to plant primary and secondary circuits and the irradiated fuel bays, and
- provisions to support containment integrity through hydrogen (passive autocatalytic recombiners) and energy (air coolers and venting systems) managements equipment

These physical modifications were supplemented by procedural improvements (for example, updated accident management guidelines) and research results (such as support for demonstration on in-vessel corium retention). Results of updated Probabilistic Safety Assessments, which take credit of some but not all of the recent enhancements, indicate that

- Core Damage Frequency is reduced by a factor from 1.8 to 5.7,
- Large Release Frequency is reduced by a factor from 1.8 to 13.

The specific risk reduction value depends on the nature of hazard (fire, seismic events, high wind, etc) as well as particular set of safety improvements for a specific NPP. PSA methodology for such aspects as improved accident management guidance and training, or deployment of portable equipment, is not yet fully mature and these enhancements are not included in the quantitative risk evaluations.

It is necessary to acknowledge that there are economic and physical limits to the improvements for existing facilities that were designed to earlier standards and have a limited remaining operational life. Overall, it is easier to make changes to procedural / administrative elements, such as improved operational processes and personnel training. On the other hand, design modifications are costlier, require more time, and may be occasionally counterproductive, by introducing different vulnerabilities or complexities.

We also must take into consideration that there may be negative consequences to safety if the new requirements take away the resources from the safety sensitive activities. Generally, introduction of new, incremental requirements, detracts resources from other activities (which could be more safety significant) and introduce new administrative and operational burden, which may lead to errors, in particular during the transitional period. Application of cost-benefit and risk-informed arguments is seen as a useful tool for evaluation of the possible impacts and making informed decisions.

To summarize, in the recent years the operating Canadian nuclear power plants have implemented various physical and procedural enhancements, to meet the regulatory requirements and to follow the best peer examples. Some of these enhancements are expected to be standard features in operation of Generation III reactors. In particular, design extension conditions have been evaluated using systematic approaches and, where feasible, backfitting measures have been put in place. These measures have predominantly strengthened the fourth and fifth levels of defence in depth. Among other recent developments, the Canadian utilities added capabilities to supply power key safety systems in case of major accidents, and to add coolant to plant circuits and support containment integrity using both fixed and portable sources. At the same time, the regulatory framework has been reinforced to expand requirements for accident management, safety analysis (including a whole-site risk assessment), plant design, safety culture, management systems and periodic safety reviews.

## REFERENCES

- [1] CANADIAN NUCLEAR SAFETY COMMISSION, Regulatory Fundamentals. P-299, CNSC, Ottawa (2005).
- [2] CANADIAN NUCLEAR SAFETY COMMISSION, REGDOC-2.3.3: Periodic Safety Reviews. CNSC, Ottawa (2015).

## THE NITROGEN INJECTION THREAT IN PWR REACTORS

### *Weakness of current strategies & ASVAD, the new passive solution*

A. RAMI

ASVAD INTL. SL (Spain)

Tarragona (Spain)

Email: alaborda@asvad-nuclear.com Web: www.asvad-nuclear.com

#### Abstract

The Extended Loss of Ac Power accident (ELAP) is one of the worst accidents that a Pressurized Water Reactor (PWR) plant could face. The plant control is lost for a long time, but it also implies an additional Loss of Coolant Accident (LOCA). The Reactor Cooling System (RCS) depressurization is the next step and the subsequent injection from the safety accumulators. This injection recovers the inventory during some time, but when the water ends, the accumulator shows its ugliest side: Its propellant gas (nitrogen) is injected inside the RCS. This nitrogen can reach the Steam Generators (SG's) tubes. Here, it can interrupt the "natural circulation" which is the main way to cool the core. And it will remain here during all the recovery time, making the SG's unavailable.

Current strategies to deal with this issue are the accumulator isolation or venting. Pressurized Water Reactor Owners Group (PWROG) wrote the Flex Support Guidelines (particularly the FSG-10) to give directions to perform it, and nuclear industry has adapted it into their emergency procedures. Doing this, plants have closed (and forget) this issue. But the sad news is that these current strategies are too weak to be success. It relies on the proper work of a chain of active elements (FLEX generator, cabling and valves) and the operator's effort to deploy it. But this strategy has Time Critical actions which have to be done at the correct moment and simultaneously over all the accumulators. Just one failure in the chain means nitrogen injection.

Fortunately, now we have a great alternative to avoid the nitrogen injection: The Automatic Safety Valve for accumulator Depressurization (ASVAD) which has the following advantages:

The valve is permanently installed in the accumulator and available all the time.

It can avoid completely the nitrogen injection without any human assistance.

It's a PASSIVE element and doesn't require any external energy for their main operation.

Automatically performs its action at the right time. Just when all the borated water ends.

It can be easily installed in the existing facilities.

In the author's opinion, Nuclear Industry has to reevaluate again the nitrogen injection issue, because this risk is underestimated and the current strategies can't assure its success avoiding it. Just applying the Defense in Depth concept, all PWR plants with pressurized accumulators should install this valve as the MAIN BARRIER to avoid this risky complication.

#### 1. INTRODUCTION: THE NITROGEN INJECTION THREAT IN PWR REACTORS

Fukushima accident shows us the disastrous consequences of the Extended Loss of Ac Power accident (ELAP). During this accident, the plant power -and its control- is fully lost. Then, the plant evolves following its own physical processes. Only the passive protections are available, as the "natural circulation" or the accumulator's injection. Natural circulation is a physical process that creates flows in the cooling system pipes by the effect of the temperature difference, and is the main way to cool the core in these circumstances.

Furthermore, the ELAP accident directly induces other risky accident: the Loss of Coolant Accident (LOCA) starts due the loss of cooling in the Reactor Cooling Pumps (RCP) seals. From here, the system depressurization is the natural process.

All PWR reactors usually include a passive system to inject borated water to recover the coolant inventory in the Reactor Coolant System (RCS). They are usually called Accumulators, Safety Injection Tank (SIT), or Core Flood Tank (CFT).

This safety system consists in several accumulators containing borated water, pressurized with nitrogen at high pressure. These accumulators are connected to the RCS through an isolation valve and at least one non-return valve. When the RCS pressure falls under certain level, the accumulator starts injecting their water to the RCS during some time. But when it becomes empty of water, their cover gas begins to be injected into the RCS.

This nitrogen is a non-condensable gas, which finally goes to the higher parts of the RCS, first it goes to the top side of the reactor vessel, and finally it reaches the top of the Steam Generators tubes (SG). At this point,

-like a bubble in a vein-, the gas can cause the disruption of the natural recirculation flow, which is the best available way to extract the heat outward. This situation greatly complicates the subsequent cooling of the core and substantially increases the chances of core melting, because the gas will remain inside during all the recovery process making the SG's unavailable to cool the core. Many studies have been done about this, but some good ones can be the references [1-3, 4].

All these studies have considered relatively low quantities of uncondensables inside the system, mainly from the dissolved gasses in the liquid phase from the accumulators or even the Hydrogen production from the zircaloy oxidation. Just these small quantities are enough to disturb the proper work of the heat exchangers.

But inside the accumulators there are big quantities of nitrogen at high pressure. In one standard accumulator can be around 640 Kg of Nitrogen (@45 Bar @35°C). After its depressurization to lower pressures this nitrogen can fill the whole volume of the RCS. It's really very important to avoid its injection to the RCS.

## 2. CURRENT STRATEGIES TO AVOID THE NITROGEN INJECTION

The Pressurized Water Reactor Owners Group (PWROG) wrote a group of guidelines to cope with severe accidents. These guides are known as "Flex Support Guidelines" (FSG's). These guides describe the strategies to recover and mitigate such accidents. The PWROG plants used these guides to write their own procedures. The PWROG FSG-10 guide [5] specifically describes the strategy to avoid the nitrogen injection.

Currently there are three strategies to prevent this threat:

- a) The first strategy is to close the accumulator output isolation valve before the water injection ends.
- b) The second strategy is to vent the residual nitrogen to the atmosphere by means of relief valves.
- c) The last strategy is to keep the RCS pressure over the nitrogen pressure.

But the worst news is that ALL these strategies have important drawbacks and weakness:

Isolating or venting it's a TIME CRITICAL action. If it's done too soon, part of the water will be wasted. If it's done too late, nitrogen will be injected. And all the actions have to be done at the same time over ALL the accumulators, because all are injecting in parallel to the same RCS pressure.

To know the correct moment is not easy. It mainly depends on the leak rate, and it is nonlinear.

ALL the equipment needed ARE ACTIVE ELEMENTS and needs to be powered from a FLEX generator. This generator must be deployed and connected to the valve's circuitry to allow their closure, and valve by valve. This can take a lot of time and organization efforts during the accident. It can spend resources which other important recuperation tasks may need... or even rest unperformed.

Even when its closure is achieved, these isolation valves ARE NOT LEAK-PROOF. The valves aren't able to keep the gas isolated due their internal leaks (these valves never are leak-tested). Sooner or later this nitrogen will reach the RCS and the SG tubes, despite its rate can be slower. If the gas reaches the SG's tubes, it will remain inside during ALL the recovery process making the SG's unavailable to cool the core.

Operators will be heavily burdened doing all these actions, and with no guarantee of success. Just one failure in the chain of actions, means nitrogen injection to RCS.

Keeping high the RCS pressure also needs the emergency equipment work, and it also implies higher RCS leak rates and hard work to the emergency organization. But this is only a TEMPORAL STRATEGY to get more time. Sooner or later, the RCS will be further depressurized, and then the nitrogen injection will happen if no other actions are taken.

Therefore, it is evident the need for some automatic (and passive) system, which prevents the injection of this residual nitrogen to the reactor, without requiring any external energy for its operation. Furthermore, the system should automatically recognize the appropriate moment for its actuation. This will allow their unattended operation maximizing the cooling water injection, and avoiding the nitrogen injection into RCS.

## 3. ASVAD, THE NEWSOLUTION

We were not satisfied with the simple complaint of these weaknesses. We have done a step forward to find an alternative way that can avoid the nitrogen threat, without the previous strategies weaknesses and shortcomings.

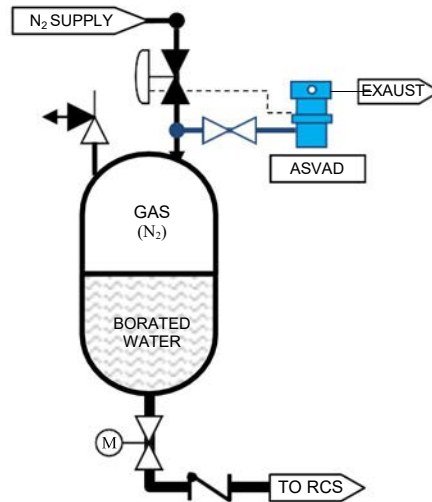


FIG. 1. ASVAD valve installation.

The result of this effort has been the design of a new passive element (ASVAD) which is very similar to a safety valve, but with a reverse operation. This new element does not vent the pressure when a high pressure is exceeded. It does just when the pressure drops under a desired setpoint.

Fig. 1 shows where the ASVAD valve is installed. The valve is installed with an isolation valve in the accumulator's nitrogen side. This isolation valve simply allows servicing the ASVAD valve without disturbing the accumulator system.

As it is bearing the internal accumulator pressure, it can detect the end of the water injection and is able to exhaust the residual nitrogen into the atmosphere before it can reach the RCS pipes.

Basically, the ASVAD valve remains closed while the pressure in the accumulator is normal. After the injection starts, nitrogen will expand inside the tank as the water goes out. This implies a continuous drop in the pressure.

Once all the borated water has been injected, it only remains the residual gas pressure. When this pressure drops below the valve setpoint, the ASVAD valve suddenly opens and remains opened. This allows the complete accumulator depressurization, and thus the complete avoidance of the nitrogen injection. As a secondary consequence, this vented nitrogen will help to cool and inertize the containment building.

Fig. 2 shows the simplified diagram of the ASVAD operation. Its principle of work is the difference between the force made by the inner accumulator pressure (the big red arrow), and the force made by an adjustable spring (the narrow red arrow). While the force done by the pressure inside the accumulator is higher than the opening spring force, the valve remains fully closed. Usually the pressure force is three times the spring force. This is its normal steady state.

During the water injection, the gas expands and the pressure decreases inside the accumulator. When the pressure drops below the spring mechanical force, the shut-off obturator is displaced from its seal and then, the valve suddenly opens and the gas escapes through its holes and central cavity, and finally through the outlet ports. The valve will remain in this state allowing the accumulator fully emptying.

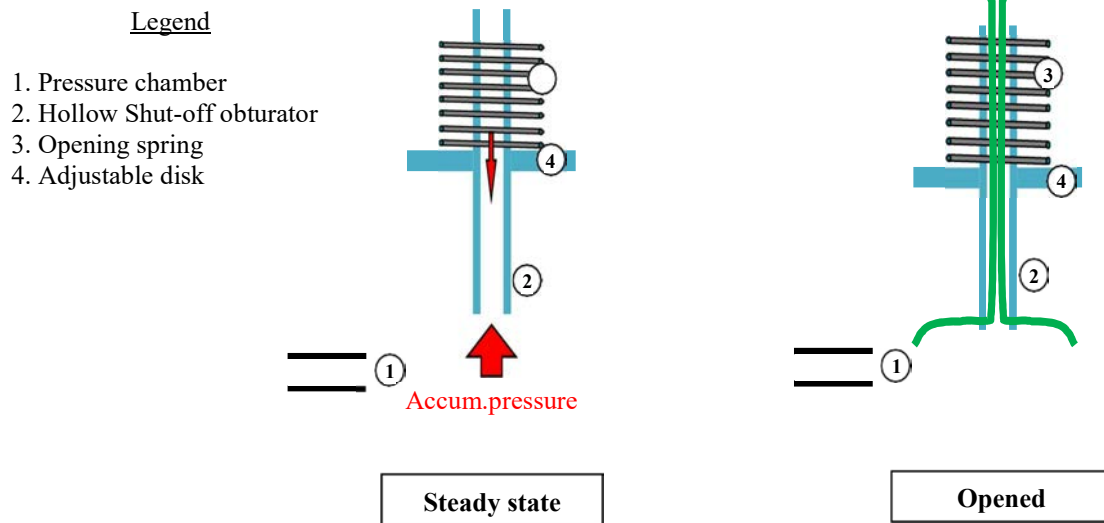


FIG. 2. ASVAD simplified operation diagram.

The ASVAD valve has the following advantages:

- After its installation, the valve IS AVAILABLE ALL THE TIME. It will remain closed until its action will be required. Once tripped, it will remain open allowing the fully accumulator depressurization, FULLY AVOIDING THE NITROGEN INJECTION.
- It's a PASSIVE ELEMENT and doesn't require any external energy for its main operation.
- Automatically performs its action AT THE RIGHT MOMENT, when all the borated water ends, and just before the gas injection. It performs its action WITHOUT ANY HUMAN ASSISTANCE.
- Its use can SAVE organization efforts that can be invested in other recuperation tasks.
- Its simplicity and robust design, makes the valve immune to harsh accident scenarios. Also its qualified life can be very long.
- Its installation in existing facilities is very easy. The ASVAD valve is a relatively small valve. The required modification can be minimal.
- Its simple design also facilitates the maintenance of the valve. You can “install and forget it” until the next outage. It only needs to be tested from time to time in the same way as a normal safety valve.
- The valve installation does not induce any new risk to the accumulator system operability, because the normal accumulator pressure always tends to keep closed the valve during all the time.

#### 4. CONCLUSIONS

- a) After an ELAP, a subsequent LOCA will take place. This RCS depressurization can easily lead to the accumulator injection. But when its water ends, the accumulator's nitrogen injection to RCS can be a risky complication to the core cooling due to its adverse effects to the natural circulation process and even to the reflux cooling mode also.
- b) The current strategies to avoid it are based on the concurrent work of multiple active elements and the (well-trained) organization efforts. These strategies have significant drawbacks and weakness to fully rely on its proper success:
  - Too much human efforts in a bad environment.
  - Time critical actions over many elements.
  - Difficulties to find the correct moment to act.
  - A long chain of active element's operations. Just one failure can compromise its success.
  - The valves weakness to isolate or vent the residual nitrogen.

- c) Now there is available a different solution to these problems. There is a safety valve specifically designed to avoid this risky complication. It has significant advantages over the current strategies. Could the most important one is that it's available from the first moment and it automatically perform its action at the right time. It is a fully passive and doesn't need any operator assistance. With this valve installed, the operators will not be burdened by the nitrogen injection issue and they can remains focused on the core cooling and other recuperation tasks.
- d) Nuclear community must know and re-evaluate the consequences of the nitrogen injection from the accumulators. A common assumption in the mentioned studies is that no accumulator nitrogen injection is done, assuming the correct valve isolation before its water ends. But what happen if this assumption is not true? What if the closed valve leaks continuously nitrogen to RCS?

Nuclear Operators must also re-evaluate their current strategies weakness. Nowadays it seems a “closed item” with little or no attention on it. It seems that having procedure and trained personnel can be enough to solve this problem and to relegate these strategies into the second order priorities during the accident.

Nuclear community must take the appropriate actions to solve this threat definitively.

## REFERENCES

- [1] Various Authors, WCAP-17601-P Rev.1, Reactor Coolant System Response to the Extended Loss of AC Power Event for Westinghouse, Combustion Engineering and Babcock & Wilcox NSSS Designs, Westinghouse Proprietary Class 2, January 2013.
- [2] SARRETTE, C., Effect of Noncondensable Gases on Circulation of Primary Coolant in Nuclear Power Plants in Abnormal Situations (Thesis for the degree of Doctor of Science (Technology), Lappeenranta University of Technology (Finland), February 2003.
- [3] NAGAE, T., CHIKUSA, T., MURASE, M., MINAMI, N., Analysis of Non-condensable Gas Recirculation Flow in Steam Generator U-Tubes during Reflux Condensation Using RELAP5, Journal of Nuclear Science and Technology, **44** 11 (2007) 1395-1406.
- [4] NOEL, B., DERUAZ, R., Reflux condenser mode with non-condensable gas: assessment of CATHARE against BETHSY Test 7.2C. Nuclear Engineering and Design **149** (1994) 291-298.
- [5] Various Authors, FSG-10 Rev.1, Passive RCS injection isolation. Background information for Westinghouse Owners Group Emergency Response Guidelines, PWROG, December 2014.

## CONTRIBUTION OF THE OECD/NEA WORKING GROUP ON THE ANALYSIS AND MANAGEMENT OF ACCIDENTS (WGAMA) IN THE SEVERE ACCIDENT FIELD

D. JACQUEMAIN  
Institut de Radioprotection et de Sûreté Nucléaire  
Saint Paul Lez Durance, France  
Email: didier.jacquemain@irsn.fr

L. HERRANZ  
CIEMAT  
Madrid, Spain  
Email: luisen.herranz@ciemat.es

N. SANDBERG  
OECD/NEA  
Boulogne Billancourt, France  
Email: nils.sandberg@oecd.org

### Abstract

The Committee on the Safety of Nuclear Installations (CSNI) aims to assist OECD Nuclear Energy Agency (NEA) member countries in maintaining and further developing the scientific and technical knowledge base required to assess and improve the safety of nuclear reactors and fuel cycle facilities. As one of the CSNI working groups, the Working Group on the Analysis and Management of Accidents (WGAMA) is committed to advancing the understanding of the physico-chemical processes of accident phenomenology in current and advanced reactors. As a result, it addresses a broad spectrum of safety issues related to the reactor coolant system and the containment including safety and auxiliary systems for management of design-basis and severe accidents. The paper describes some of the major outcomes concerning Severe Accidents WGAMA activities. In total, over 60 reports have been issued since the group creation in the early 2000s, amongst them State-of-the-Art Reports, International Standard Problems and benchmarks. In addition, Workshops have been arranged and also databases have been created. Then, it outlines meaningful contributions that were conducted in response to issues identified after the Fukushima-Daiichi accident. Finally, some information is provided concerning the progress achieved in ongoing activities, like the phenomena identification ranking table on spent fuel pools during LOCAs, informing SAM guidance via simulation, reviewing the major conclusions related to ex-vessel steam explosions in the light of new data and improving long term management of severe accidents in the light of passed major accidents.

### 1. INTRODUCTION

The Working Group on Analysis and Management of Accidents (WGAMA) is one of eight working groups under the Committee on the Safety of Nuclear Installations (CSNI) of the OECD/NEA (Nuclear Energy Agency). Fig. 1 shows the link of the WGAMA in the CSNI framework. The overall WGAMA objectives are: to assess and strengthen the technical basis needed for the prevention, mitigation and management of potential accidents in nuclear power plants; and to facilitate international convergence on safety issues and accident management analyses and strategies. To fulfil this objective, the Working Group exchanges technical experience and information relevant for resolving current or emerging safety issues, promotes the development of phenomena-based models and codes used for the safety analysis, assesses the state of knowledge in areas relevant for the accident analysis and, where needed, promotes research activities aimed to improve such understanding, while supporting the maintenance of expertise and infrastructure in nuclear safety research. Regardless the activity, the intention is always to make significant contributions to the regulatory decision-making concerning prevention and management of accidents, understanding of specific events and identification of possible preventive measures, and to the state of knowledge and knowhow.

Through its activities the Working Group provides answers to CSNI on posed questions and/or challenges on existing reactors, as requested, in the form of state-of-the-art and other types of technical reports, workshops and related proceedings, benchmarking exercises and joint research proposals. Each specific activity is usually undertaken by what is called a task group, which usually consists of a small number of national experts on the



task to be addressed. Priorities are given based on criteria of safety significance and risk and uncertainty considerations.

Given the above objective, there are a number of technical areas that are within the scope of WGAMA. Just to give a few examples: reactor coolant system thermal-hydraulics; scaling of thermal hydraulics systems; best estimate and uncertainty analysis methods, design-basis accident; pre-core melt conditions and progression of accident and in-vessel phenomena; coolability of over-heated cores; ex-vessel corium interaction with concrete and coolant; in-containment combustible gas control; physical-chemical behavior of radioactive species in damaged plants; combustion phenomena; spent fuel pool accidents; informing severe accident management actions through analysis.

WGAMA has about 100 national delegates ensuring the efficient implementation of its broad work programme. The group has a Chair, a Vice-Chair, a Secretary, a Bureau and Task Leaders. The Bureau members play a key role providing technical and strategic advice to the Chair and Vice-Chair while the NEA Secretariat (through NEA's Nuclear Safety Technology and Regulation Division) provides support on organizational, logistic and, sometimes, strategic matters with respect to all WGAMA activities. The Chair and Vice-Chair take over the chairing of WGAMA meetings and monitor the progress of the activities, which they report on annually to CSNI. Specialists other than the WGAMA delegates can work on WGAMA activities; in recent years, more than 250 specialists have been actively contributing to WGAMA's work.

The paper outlines the activities within the WGAMA in the severe accident field. An overview is provided so that this article becomes a sort of directory of current WGAMA activities, including brief introductions and current status of the running activities.

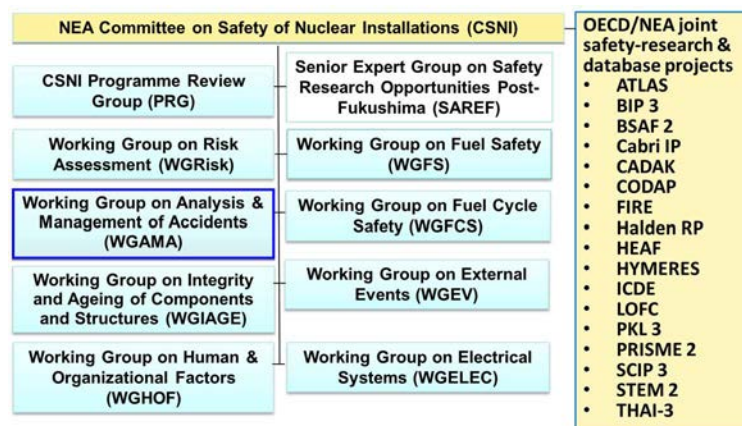


FIG. 1. Working Groups and Project under the NEA/CSNI framework.

## 2. BRIEF OVERVIEW OF RECENTLY FINISHED ACTIVITIES IN THE SEVERE ACCIDENT FIELD

In the follow-up of the Fukushima Daiichi NPP accident (FDNPs), WGAMA conducted for the CSNI several high priority activities and established status reports on spent fuel pool (SFP) accidents [1], hydrogen management [2], filtered containment venting systems (FCVS) [3] and achieved a benchmark exercise on fast running methods and tools for predicting radioactive releases [4].

The status report on SFP produced a summary of the status on SFP accidents and mitigation strategies to contribute to the post-FDNPs decision making process, provided an assessment of current experimental and analytical knowledge about loss of cooling and LOCA in SFPs and their mitigation strategies, briefly discussed strengths and weaknesses of analytical tools to predict SFP accident evolution and assess the efficiency of cooling mechanisms for mitigation and identified research activities to address gaps in the understanding of relevant phenomenological processes to reduce uncertainties in the analysis of such accidents. It was in particular concluded that more specific modelling for SFPs is desired where current codes are intended mainly for SA analysis (source-term estimation being a challenge) and that it would be valuable to produce specific user guidelines for code applications to SFP accidents. It was also concluded that important uncertainties should be ranked via a PIRT exercise; such an exercise is currently being conducted through a WGAMA/WGFS (Working Group on Fuel Safety) joint action.

The status report on hydrogen risk management reviewed the various approaches in member countries (approaches in DBAs and SAs including national requirements, mitigation, measurement strategies, engineered systems (sprays, air cooler, blow-out panels, etc.) and potential impact, advantages and consequences of different options) for all water-cooled reactors (PWRs, VVERs, BWRs & PHWRs). The report also addressed capabilities and validation status of dedicated codes. It was identified that further efforts are needed to close research gaps, enhance code capabilities and reduce code uncertainties. Assessment is needed of how knowledge gained from research has been implemented in NPP safety analysis and how it is considered in SAMG. In particular, pressure loads due to H<sub>2</sub> and/or CO combustion on containment and equipment (especially where this is safety related) need to be further assessed particularly for ex-vessel conditions where this may be plant specific.

The status report on FCVS compiled the status of implementation of FCVS in reactors in OECD countries, the national requirements for systems designs and filter performance, the various venting strategies as well as advantages and disadvantages of containment venting. It also described briefly installed systems and their demonstrated and expected performances. Further, possible improvements for hardware (particularly filtration) and qualification of the systems were identified from an accident management perspective. The report was produced as a guide for decision makers in regulatory authorities, technical support organizations, research institutes and utilities which consider FCVS implementation.

The benchmark on fast running methods and tools for predicting the accident source term of radioactive releases and resulting public doses has demonstrated that the know-how for performing such fast, inevitably approximate accident modelling is quite advanced, benefitting from the mature understanding of the accident phenomenology, software and hardware advances as well as previous development effort in several organizations. Nevertheless, it evidenced that setting up even a relatively simple model to perform accident progression assessment may be a complicated task, especially if dealing with not-so-familiar reactor technology. The spread in predictions was shown to be substantial, explained by the varying capabilities of the tools, as well as by the assumptions made by the project participant regarding the possible accident progression. Based on the project results, several recommendations for future studies have been offered for promoting international cooperation in future development of such tools. These recommendations helped in elaborating the European FASTNET project which is currently under way and aims at improving diagnosis and prognosis methods and tools for emergency response.

An international Iodine workshop was organized in March 2015 in Marseille jointly by OECD/NEA, the NUGENIA association, the European Commission and IRSN. Generally speaking the workshop intended to assess the recent progress made on Source Term research and their application in accident management. The essence of the conclusions and recommendations of the workshop regarding source term research and its implementation in tools supporting accident analysis and management including emergency response are detailed in [5]. They mostly concern the necessity to:

- perform additional research focused on reactor applications to progress in the assessment of the potential effects of “delayed” FP re-emission in SA from deposits on RCS, containment and solid filters surfaces and from pools (sumps, suppression pools, liquid pools in filters) on source term evaluations;
- deepen the assessment of the validity of source term related models implemented in SA system codes and of methods for source term evaluations and quantification of associated uncertainties.

Full proceedings and a summary report of the workshop have been released as an OECD/NEA report [5].

A State-Of-the-Art Report (SOAR) on molten corium concrete interaction (MCCI) and coolability was completed and will be released in 2017 [9]. In the SOAR, the working group concerted vision of the phenomenology of core-concrete interactions and melt coolability is summarized together with a global overview of simulation codes capabilities and validation status. This concerted vision demonstrates the significant progress made on the level of understanding regarding MCCI behaviour under both wet and dry cavity conditions but also led the working group to identify a few issues (particularly based on lessons learned from Fukushima Daiichi situations) that may warrant further investigation to reduce residual uncertainties. These issues include specific realistic reactor configurations (as illustrated in Fig. 2) from the short to the long term and proposition to improve top flooding melt coolability. Further relevant experimental investigations will require technological updates of existing facilities.

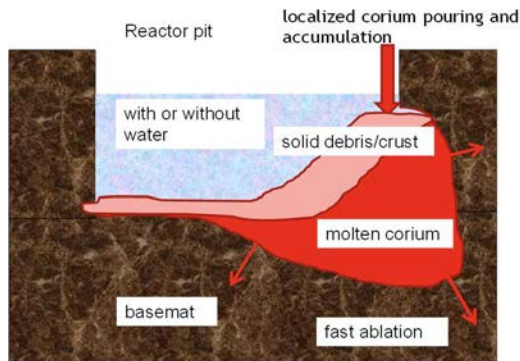


FIG. 2. Schematic representation of a realistic reactor configuration during MCCI.

### 3. ON-GOING ACTIVITIES IN THE SEVERE ACCIDENT FIELD

A Phenomena Identification Ranking Table (PIRT) on spent-fuel pool LOCAs is underway. Earlier work on a NEA joint experimental project on spent-fuel pool (SFP) accidents [7] and review of information and code-analysis capabilities in this area [1] has already been published and it was recognized that a need existed to review the SFP accident phenomenology to evaluate the importance of particular phenomena with respect to the overall influence on the consequences of SFP accidents. The phenomena identification and ranking table (PIRT) approach has been adopted aiming to identify the most influential phenomena for which the level of knowledge is poor, i.e., in need of research and hence a priority for investigation. To do so both loss of cooling and loss of coolant accidents are being addressed and three phases have been set in the accident unfolding (phase 1 up to start of fuel assembly de-watering, phase 2 up to cladding rupture, phase 3 addressing fuel degradation). This work should be published in 2018 and lead to international consensus on prioritization of research needs with respect to this kind of accident. The SFP accident scenarios have been observed to be extremely complex and despite the more than 100 phenomena of potential influence in accident evolution, PIRT contributors have found the way to boil down this list to less than 10 phenomena.

A Technical Opinion Paper (TOP) on ex-vessel steam explosions is being written in the context of previous conclusions from the OECD SERENA project [8] and more recent results that showed melts to have a propensity to produce steam explosions when falling into shallow layers of water [9]. At the same time, WGAMA recognized that changes in national regulatory requirements post-FDNPs in some countries and a desire to have better precision in steam explosion risk assessment led to both additional experiments in some countries and the need to review new information in order to make a judgment on whether the current approaches to steam explosion risk management remain valid. This work is near completion and should be published early 2018. It demonstrates that significant progress was made in the understanding of phenomena involved in steam explosion but that further investigations are still needed to adequately appreciate the risk of safety components and structures failure due to steam explosion. It was thus recommended to perform further experimental investigations of specific realistic reactor configurations and more fundamental investigations of the fragmentation, oxidation, solidification and pressurisation processes to improve the corresponding modelling in dedicated codes.

Following the accident at the Fukushima Daiichi NPP, one of the imperatives for the nuclear science and industry communities is to reassess the safety of existing NPPs, notably to evaluate the sufficiency of technical means and administrative measures addressing the management of an accident for the design basis, the beyond design basis, the emergency response and the long term post-emergency phases. Up to now, international actions primarily addressed lessons learnt from the Fukushima-Daiichi accident for the management of short-term phases (EOP and SAMG domains) and for emergency preparedness but the long term accident management and actions (LTMA) were not examined in detail. Therefore, OECD/NEA decided to launch in 2014 an action to (1) review the experience gained for LTMA from the TMI-2, Chernobyl and Fukushima-Daiichi accidents (2) review envisaged, planned or existing regulations, guidance and practices in OECD countries for LTMA for a SA in a NPP (3) describe possible approaches for LTMA (4) identify main risks and issues to be tackled for LTMA and related knowledge gaps (5) provide guidance for enhancing LTMA for a severe accident and (6) make recommendations for future studies and research, including the development or improvement of methods to assess

LTMA. Among the technical issues presently being covered one may mention: management of damaged fuel on the long term (inside the reactor vessel and containment as well as in SFP) up to its disposal; strategies for liquid and atmospheric releases mitigation on the long term; treatment and management of liquid, gases and solid wastes; management of the hydrogen risk on the long term; survivability and failure risks of equipment, systems and structures required for maintaining the plant in a safe stable state on the long term; instrumentation required for monitoring LTMA; effect of short-term actions undertaken for the crisis management on the LTMA. Guidance for enhancing LTMA and recommendations for future studies and research are expected to be delivered through a status report on LTMA in 2018. The main pillars of this status report will be the information gathered from TMI-2, Chernobyl-4 and Fukushima (as illustrated in Figure 3) as well as alternative approaches, from identifying Plant Damage States (PDS) to using risk-based methods, and MART building (Management Action Ranking Table). At the time this article is being written, there are a number of issues that have been already highlighted as key for the LTMA, among them: water waste management, decontamination of large areas of site's buildings, reactor and spent fuel pools defueling, etc.



FIG. 3. Insights from TMI-2 and Chernobyl accidents for LTMA.

Through the activity on informing Severe Accident Management Guidance and Actions, WGAMA aimed to provide a basis for consistent definitions of concepts of “verification” and “validation” of severe-accident management (SAM) actions and provide examples of several existing practices aiming at ensuring the correctness, usability and efficiency of SAM (e.g., so-called desk-top exercises, analytical simulations, use of simulators, etc.). The result of analytical simulation of SAM actions may help identify gaps or potential weaknesses in the existing SAM guidance and thus help improve or refine it. The status report will present the best and recommended practices regarding the use of analytical simulations as one of the means to validate SAM. Among the upper level conclusions one might include the suitability of the symptom-based approach to severe accident mitigation and the capability of the current tools to help in the definition of accident management; nonetheless, through the discussions held the groups has concluded that a good implementation of any SAM requires a severe accident knowledge level and specific training on the actions to be taken. This work will be published in 2017.

Additionally, there are some activities that have been compiled as potential future activities but have not been even developed to the first step needed, the preparation of a “CSNI Activity Proposal Sheet” (CAPS). Some of them might concern: a workshop on instrument performance in severe-accident conditions; an assessment of

by-pass accident source-term; an analysis of plant ageing influence on severe-accident progression/understanding/mitigation and updates of state of the art reports on FP release and transport.

#### 4. CONCLUDING REMARKS

In the sections above, the current status of the WGAMA group of NEA has been outlined by briefly summarizing what has recently finished, what is presently ongoing and what could be launched in the near future. In short, all this highlights that WGAMA is a very active group of NEA who in the very last years has demonstrated an outstanding capability of response, being capable of shaping their activities to the prompt and demanding needs that stem from the FDNPs analysis without neglecting its own idiosyncrasy and way of doing. Beyond how prolific the Group is in terms of Status Report and Status Of the Art Reports (SOAR), the diversity of the Group activities is outstanding, encompassing a broad spectrum from education to code benchmarking. The WGAMA commitment to produce technical support to regulatory decision-making process has resulted in a number of ideas that are being presently conceived and will streamline the coming activity of the group in those areas in which WGAMA develops their activities: Thermal-hydraulics, Computational Fluid-Dynamics and Severe Accidents.

#### ACKNOWLEDGEMENTS

The authors are indebted to CSNI for their support and NEA for articulating all the necessary means to conduct the WGAMA activities in the best conditions possible. Likewise, thanks all the members of the WGAMA bureau for the technical discussions shaping up and pushing forward the WGAMA work. Last but not least, the authors show their deepest appreciation to all those who actively contribute to the WGAMA activities.

#### REFERENCES

- [1] ADORNI, M., ESMAILI, H., GRANT, W., HOLLANDS, T., HÓZER, Z., JACKEL, B., MUÑOZ, M., HAKAJIMA, T., ROCCHI, F., STRUCIC, M., TRÉGOURÈS, N., VOKAC, P., Status Report of Spent Fuel Pools under Loss-Of-Coolant and Loss-of-Cooling Accident Conditions, OECD/NEA/CSNI Report NEA/CSNI/R(2015) **2** (2015).
- [2] LIANG, Z., SONNENKALB, M., BENTAÏB, A., SANGIORGI, M., Status Report on Hydrogen Management and Related Computer Codes, OECD/NEA/CSNI Report NEA/CSNI/R(2014) **8** (2014).
- [3] JACQUEMAIN, S., GUENTAY, S., BASU, S., SONNENKALB, M., LEBEL, L., ALLELEIN, H.-J., LIEBANA-MARTINEZ, B., ECKARDT, B., AMMIRABILE, L., "Status Report on Filtered Containment Venting", OECD/NEA/CSNI Report NEA/CSNI/R(2014) **7** (2014).
- [4] VIKTOROV, A., DEWITT, P., Benchmark of Fast-Running Software Tools used to Model Releases during Nuclear Accidents Final Summary Report, OECD/NEA/CSNI report, NEA/CSNI/R(2015) **19** (2015).
- [5] JACQUEMAIN, D., ALBIOL, T., DICKINSON, S., HERRANZ, L.-E., FUNKE, F., GLOWA, G., GUPTA, S., HOSHI, H., HOTTA, A., KÄRKELÄ, T., KISSANE, M., LIND, T., SALAY, M., SONG, J.-H., VAN DORSSELAERE, J.-P., Summary Report and Full Proceedings of the International OECD/NEA-NUGENIA Iodine Workshop, OECD/NEA/CSNI report, NEA/CSNI/R(2016) **5** (2016).
- [6] BASU, S., BONNET, J.-M., CRANGA, M., VOLA, D., FARMER, M.T., ROBLEDO, F., SPENGLER, C., State-of-the-Art Report on Molten-Corium-Concrete interaction and Ex-Vessel Molten-Core Coolability, OECD/NEA/CSNI Report NEA/CSNI/R(2016) **15** (2016).
- [7] Proceeding of the SFP Project Concluding Seminar, OECD/NEA/CSNI Report NEA/CSNI/R(2013) **13** (2013).
- [8] OECD/NEA Research Programme on Fuel-coolant Interaction - SERENA Steam Explosion Resolution for Nuclear Applications: Final Report, OECD/NEA/CSNI report, NEA/CSNI/R(2007) **11** (2007).
- [9] KUDINOV, P., GRISHCHENKO, D., KONOVALENKO, A., KARBODJIAN, A., Nuclear Engineering and Design, **314** (2017) 182-197.



# IAEA

International Atomic Energy Agency

No. 25

## ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

### CANADA

#### ***Renouf Publishing Co. Ltd***

22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA

Telephone: +1 613 745 2665 • Fax: +1 643 745 7660

Email: [order@renoufbooks.com](mailto:order@renoufbooks.com) • Web site: [www.renoufbooks.com](http://www.renoufbooks.com)

#### ***Bernan / Rowman & Littlefield***

15200 NBN Way, Blue Ridge Summit, PA 17214, USA

Tel: +1 800 462 6420 • Fax: +1 800 338 4550

Email: [orders@rowman.com](mailto:orders@rowman.com) Web site: [www.rowman.com/bernan](http://www.rowman.com/bernan)

### CZECH REPUBLIC

#### ***Suweco CZ, s.r.o.***

Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC

Telephone: +420 242 459 205 • Fax: +420 284 821 646

Email: [nakup@suweco.cz](mailto:nakup@suweco.cz) • Web site: [www.suweco.cz](http://www.suweco.cz)

### FRANCE

#### ***Form-Edit***

5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE

Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90

Email: [formedit@formedit.fr](mailto:formedit@formedit.fr) • Web site: [www.form-edit.com](http://www.form-edit.com)

### GERMANY

#### ***Goethe Buchhandlung Teubig GmbH***

Schweitzer Fachinformationen

Willstätterstrasse 15, 40549 Düsseldorf, GERMANY

Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28

Email: [kundenbetreuung.goethe@schweitzer-online.de](mailto:kundenbetreuung.goethe@schweitzer-online.de) • Web site: [www.goethebuch.de](http://www.goethebuch.de)

### INDIA

#### ***Allied Publishers***

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA

Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928

Email: [alliedpl@vsnl.com](mailto:alliedpl@vsnl.com) • Web site: [www.alliedpublishers.com](http://www.alliedpublishers.com)

#### ***Bookwell***

3/79 Nirankari, Delhi 110009, INDIA

Telephone: +91 11 2760 1283/4536

Email: [bkwell@nde.vsnl.net.in](mailto:bkwell@nde.vsnl.net.in) • Web site: [www.bookwellindia.com](http://www.bookwellindia.com)



## **ITALY**

### ***Libreria Scientifica "AEIOU"***

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY

Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48

Email: [info@libreriaaeiou.eu](mailto:info@libreriaaeiou.eu) • Web site: [www.libreriaaeiou.eu](http://www.libreriaaeiou.eu)

## **JAPAN**

### ***Maruzen-Yushodo Co., Ltd***

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN

Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364

Email: [bookimport@maruzen.co.jp](mailto:bookimport@maruzen.co.jp) • Web site: [www.maruzen.co.jp](http://www.maruzen.co.jp)

## **RUSSIAN FEDERATION**

### ***Scientific and Engineering Centre for Nuclear and Radiation Safety***

107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION

Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59

Email: [secnrs@secnrs.ru](mailto:secnrs@secnrs.ru) • Web site: [www.secnrs.ru](http://www.secnrs.ru)

## **UNITED STATES OF AMERICA**

### ***Bernan / Rowman & Littlefield***

15200 NBN Way, Blue Ridge Summit, PA 17214, USA

Tel: +1 800 462 6420 • Fax: +1 800 338 4550

Email: [orders@rowman.com](mailto:orders@rowman.com) • Web site: [www.rowman.com/bernan](http://www.rowman.com/bernan)

### ***Renouf Publishing Co. Ltd***

812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA

Telephone: +1 888 551 7470 • Fax: +1 888 551 7471

Email: [orders@renoufbooks.com](mailto:orders@renoufbooks.com) • Web site: [www.renoufbooks.com](http://www.renoufbooks.com)

## **Orders for both priced and unpriced publications may be addressed directly to:**

Marketing and Sales Unit

International Atomic Energy Agency

Vienna International Centre, PO Box 100, 1400 Vienna, Austria

Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302 or +43 1 26007 22529

Email: [sales.publications@iaea.org](mailto:sales.publications@iaea.org) • Web site: [www.iaea.org/books](http://www.iaea.org/books)

INTERNATIONAL ATOMIC ENERGY AGENCY  
VIENNA  
ISBN 978-92-0-104618-5  
ISSN 0074-1884