IAEA TECDOC SERIES

IAEA-TECDOC-1982

IAEA-TECDOC-1982

Current Approaches to the Analysis of Design Extension Conditions with Core Melting for New Nuclear Power Plants

IAEA
International Atomic Energy Agency

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available at the IAEA Internet site

www.iaea.org/resources/safety-standards

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

CURRENT APPROACHES TO THE ANALYSIS OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING FOR NEW NUCLEAR POWER PLANTS

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

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

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

IAEA-TECDOC-1982

CURRENT APPROACHES TO THE ANALYSIS OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING FOR NEW NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2021

COPYRIGHT NOTICE

For further information on this publication, please contact:

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

Printed by the IAEA in Austria
October 2021

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agencyt.
Title: Current approaches to the analysis of design extension conditions with core melting for new nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2021. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1982 | Includes bibliographical references.
Identifiers: IAEAL 21-01456 | ISBN 978-92-0-133921-8 (paperback : alk. paper) | ISBN 978-92-0-133821-1 (pdf)
Subjects: LCSH: Nuclear power plants — Design and construction. | Nuclear power plants — Safety measures. | Nuclear reactors — Cores.

FOREWORD

Since the introduction of the term ‘design extension conditions’ in IAEA Safety Standards Series No. SSR-2/1, Safety of Nuclear Power Plants: Design, Member States have expressed interest in obtaining further guidance on how to address the deterministic analysis for these accident conditions. This publication focuses on collecting current practices in Member States related to design extension conditions with core melting.

This publication was developed with input from technical experts from Canada, Finland, France, India, the Islamic Republic of Iran, the Russian Federation and the United States of America. To address the needs of Member States, the IAEA collected current practices in the form of a questionnaire. A draft questionnaire was discussed and revised in December 2016. The final questionnaire generated responses from technical experts from Canada, Finland, France and the Russian Federation. The responses formed the basis of a draft publication, which was then further consolidated by incorporating information from participants to the Technical Meeting on Current Approaches in Member States to the Analysis of Design Extension Conditions for New Nuclear Power Plants, organized by the IAEA between 19 and 23 March 2018. Following the technical meeting, additional responses from technical experts from India, the Islamic Republic of Iran and the United States of America were also incorporated. Technical experts from Belgium, Bulgaria, Japan, the Republic of Korea, Romania and Sweden also contributed during the technical meeting.

The IAEA is grateful to all the technical experts who contributed to the drafting and review of this publication. The IAEA officers responsible for this publication were A. Amri and J. Luis Hernandez of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

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

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

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

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

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

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

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The requirement of deriving design extension conditions (DEC), which are understood to comprise both conditions in events without significant fuel degradation and conditions in events with core melting, were introduced in IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [1]. In SSR-2/1 (Rev. 1) [1], DEC were introduced for the purpose of further improving the safety of nuclear power plants (NPPs) by enhancing their capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents (DBAs) or that involve additional failures.

The consideration of DEC leads to the introduction, in the design, of safety features for DEC to prevent or mitigate DEC consequences. SSR-2/1 (Rev. 1) [1], states in paragraph 5.27 that "an analysis of design extension conditions for the plant shall be performed" with a footnote stating that "the analysis of design extension conditions for the plant could be performed by means of a best estimate approach (more stringent approaches may be used according to States' requirements)".

Although the term 'design extension conditions' was first introduced in the IAEA safety standards in 2012, some IAEA Member States with active nuclear power programmes had already considered multiple failures of safety systems (e.g. anticipated transient without scram and station blackout) in the design of new NPPs, as well as in the safety assessment of operating plants, in particular within the context of the periodic safety review.

There is, however, still no common understanding of DEC and there is a variety of approaches in IAEA Member States with active nuclear power programmes for the analysis of DEC, in particular of DEC involving core melting. This is due, for in large part, but not only, to the complexity of phenomena in such DEC and insufficient experimental data.

The technical experts participating to this review, who responded to the questionnaire and/or provided inputs during the IAEA technical meeting of March 2018, were from Bulgaria, Canada, France, Finland, Germany, India, the Islamic Republic of Iran, Japan, Romania, the Russian Federation, Sweden and the United States of America (hereafter referred as participating technical experts).

1.2. OBJECTIVE

The objective of this TECDOC is to identify current approaches of different IAEA Member States with active nuclear power programmes regarding the analysis of DEC with core melting, to discuss the regulatory perspective and technical rationale. In addition, this TECDOC attempts to find common practices and possible areas for harmonization of the main rules related to the analysis of DEC with core melting for new water cooled reactors, including their selection for the safety demonstration.

1.3. SCOPE

The scope of this TECDOC applies to the design of new water cooled reactors based on SSR-2/1 (Rev. 1) [1] and mainly addresses the methods used by the participating technical experts to define and select DEC with core melting in their countries, as well as the types of analysis methodologies (probabilistic, deterministic or combination of both) relevant to, and

computer codes applicable to those DEC. However, DEC without significant fuel degradation are sometimes mentioned in this TECDOC as necessary.

Particular attention is paid to the rules and assumptions (e.g. initial and boundary conditions, considerations on uncertainty and sensitivity, availability of systems, operator actions, equipment qualification and analysis end-state[1]) as well as to the acceptance criteria used in DEC with core melting analysis.

1.4. STRUCTURE

This TECDOC consists of nine main sections and a set of annexes. Section 1 describes the background, the objective, the scope and structure of the TECDOC. Sections 2 to 8 provide IAEA considerations and approaches and practices considered by the participating technical experts of those countries regarding definition of DEC, objectives of DEC analysis, end states of DEC, type of analysis methodology relevant to DEC, tools and computer codes applicable to DEC, application of rules and assumptions for DEC analysis, acceptance criteria in DEC analysis performance and documentation of DEC analysis, respectively. Section 9 is an important part of the TECDOC that provides a summary of the current status of DEC analysis as considered by the participating technical experts of those countries. The annexes constitute another important part of the TECDOC as they illustrate to the best knowledge of the participating technical experts the approaches in their individual Member States, and case studies.

2. OBJECTIVES OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING ANALYSIS

2.1. IAEA REFERENCES

IAEA references include safety standards, safety reports and TECDOCs. For each topic, the list is not intended to be comprehensive but can help to estimate how close to or how far from these references the individual participating technical expert's approach is.

In SSR-2/1 (Rev. 1) [1], design extension conditions are defined as "postulated conditions that are not considered for design basis accidents, but that are considered in the design process for the installation or associated facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within the acceptable limits. DEC comprise conditions both in events without significant fuel degradation and conditions in events with core melting".

In addition, SSR-2/1 (Rev. 1) [1] states at the end of Requirement 20 that "these design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or the mitigation of their consequences".

[1] SSR-2/1 (Rev.1), paragraph 5.27, requires that in case of a DEC, "the plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'". Controlled state is defined as plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to effect provisions to reach a safe state.

Paragraphs 2.1 and 2.2 of IAEA Safety Standards Series No. SSG-2 (Rev. 1), Deterministic Safety Analysis for Nuclear Power Plants [2] specify the objectives of deterministic safety analysis of nuclear power plants for all plant states, including DEC with core melting.

In a nuclear power plant, DEC could be defined for the reactor and for the spent fuel pool and are design dependent. In the IAEA approach (see IAEA-TECDOC-1791, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, [3]), only DEC without significant fuel degradation are considered for spent fuel pools while those with significant fuel degradation are considered to be practically eliminated for this type of installation.

DEC with core melting analysis generally aim at:

(a) Selecting the additional scenarios to be considered in the design;
(b) Defining and designing the features credited for DEC with core melting so that these features have the requested performance to meet the relevant safety requirements;
(c) Assisting in establishing and validating severe accident management guidelines;
(d) Providing information on the environmental conditions in which systems required to cope with DEC need to be capable of performing their intended functions;
(e) Helping in safety classification of structures, systems and components (SSCs) as appropriate;
(f) Providing input for emergency preparedness and response.

2.2. PARTICIPATING TECHNICAL EXPERTS' CONSIDERATIONS

For most of the participating technical experts, the analysis of DEC with core melting aims at confirming that the safety features, credited in the safety demonstration for the considered DEC, have the necessary performance to meet the relevant safety requirements or safety goals. For example, participating technical experts from France reported the passive autocatalytic recombiner (PAR) design assessment is performed based on deterministic studies using lumped and computerized fluid dynamics (CFD) tools. For this purpose, representative scenarios are associated to sensitivity studies that permit to demonstrate their robustness and the absence of cliff edge effect.

Additionally, there is a common understanding among the participating technical experts that one of the outcomes of the deterministic safety analysis for DEC with core melting could support the PSA, which demonstrates whether or not the probabilistic safety goals are met. For example, participating technical experts from Finland stated, the radioactive releases for DEC with core melting are required not to necessitate large scale protective measures for the population or long term restrictions on the use of extensive areas of land and water. In order to restrict the radioactive releases, the mean value of the frequency of an atmospheric Cs-137 release in excess of 100 TBq is less than 5×10^{-7}/year and the accident sequences in which the containment function fails or is lost in the early phase of DEC with core melting have only a small contribution (appreciated by expert judgement) to the reactor core damage frequency.

Participating technical experts from Canada, Finland, France, India, the Islamic Republic of Iran, Romania, the Russian Federation and the United States of America reported, DEC analysis provides an estimate of source terms arising from different DEC with core melting scenarios

and assists in defining emergency arrangements[2]. For example, participating technical experts from Canada stated, emergency preparedness is under the responsibility of the provincial authorities and the source term, as a result of the safety analysis, is an important component of the planning basis. For instance, the provincial nuclear emergency plan, based on the international best practices and lessons learned from past events, considers both DBAs and DEC including severe accidents and multi-unit scenarios where applicable. It is important to highlight that when interpreting the source term results, there is a need to acknowledge that the scenarios are hypothetical and that there are still inherent uncertainties associated with DEC with core melting analysis. While these results might provide some useful information, they do not serve as the sole source of information for nuclear emergency preparedness activities.

Additionally, participating technical experts from Canada, Finland, France, India, the Russian Federation, and the United States of America reported, DEC analysis provides inputs to establish and validate emergency operating procedures (for DEC without significant fuel degradation) and severe accident management guidelines (for DEC with core melting). Some urgent actions dedicated to severe accident management can be anticipated in the emergency operating procedures in order to be sure that they are performed in a timely manner in case of further degradation progresses towards core melting.

Participating technical experts confirmed they use insights from DEC with core melting analysis to support the development of equipment safety requirements (e.g. safety classification, operational limits and conditions). For instance, participating technical experts from the United States of America uses DEC analysis to identify which, if any, of safety features for DEC require additional regulatory consideration. More specifically, for plants where only passive systems are used to cope with DBAs, safety features necessary to meet large release frequency or containment performance goals may be subject to augmented design standards and additional availability and reliability controls.

Some participating technical experts stated they use DEC with core melting analysis as input for the qualification (those from Bulgaria, Finland, France and the Islamic Republic of Iran) or the survivability[3] (those from Canada and the United States of America) or similar concept[4] (those from the Russian Federation) of the equipment necessary to cope with those DEC, for the resulting environmental conditions such as temperature, pressure, humidity and radiation levels. Participating technical experts from Finland stated the environmental conditions anticipated during DEC with core melting need to be analysed. The analysis is prepared for containment, but also for all other areas where safety features for DEC with core melting are located. The analysis needs to provide the (maximum) temperature, pressure, humidity and radiation level results from which the environmental qualification requirements for safety features are derived. These safety features are required to fulfil the environmental qualification requirements of the location in which they are installed. The qualification process, that demonstrates that the SSCs are suitable for their intended use and includes the environmental qualification, is done according to the ISO 9000 standard. The licensee needs to have a

---

[2] According to the IAEA Safety Glossary [4], emergency arrangements are "the integrated set of infrastructural elements, put in place at the preparedness stage that are necessary to provide the capability for performing a specified function or task required in response to a nuclear or radiological emergency".

[3] Some Member States' policy is that a full qualification to environmental conditions related to DEC with core melting is unnecessary due to the low likelihood of DEC with core melting. In this case, some Member States prefer speaking about 'equipment survivability'.

[4] The concept of survivability is presented in NP-001-15 General safety provisions for nuclear power plants as "*Survivability - the property of systems and components particularly control rooms to perform their functions in spite of any sustained damage"*.

qualification plan for the process that, for example, identifies the external assessments, tests and analyses to be used for the purpose of qualification, including the methods to be used, their relevance and the individual performing them. The Finnish Guide YVL B.1, chapter 3.9 Qualification [9], establishes requirements related to environmental qualification of SSCs (see Annex III, Answer 7). Participating technical experts from the United States of America reported, the licensee is required to demonstrate with reasonable assurance through testing, analysis, or some combination thereof, that the equipment credited in DEC with core melting will survive, i.e. will operate in the environment for which it is intended and over the time span for which it is needed. Participating technical experts from the Russian Federation stated, safety features designed for DEC (i.e. named as special technical means), need to be able to fulfil their functions taking into account the impacts arising from those DEC (such impacts might include high temperature, humidity, high radiation levels, loss of coolant accident (LOCA) effects and chemical reactions, such as hydrogen recombination, and other effects).

3. SELECTION OF REPRESENTATIVE SETS OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING

3.1. IAEA REFERENCES

Requirement 20 of SSR-2/1 (Rev. 1) [1] states:

> "A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures".

Focusing on DEC with core melting for which maintaining the containment integrity is the main objective, SSG-2 (Rev. 1) [2] provides recommendations on that aspect and Ref. [3] provides insights on how a list of representative groups of severe accident conditions (i.e. DEC with core melting) could be derived for a given nuclear power plant design in order to define the design basis of the safety features for these conditions. Those safety features are such to prevent that severe accident phenomena (e.g. hydrogen detonation, direct containment heating, basemat melt-through due to melt core–concrete interaction, steam explosions) lead to the loss of containment integrity, and to ensure that releases of radioactive material are kept within acceptable limits and as low as reasonably achievable. Paragraph 5.31 of SSR-2/1 (Rev. 1) [1] states that "the design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'". This paragraph means that, it has to be shown physically impossible of those conditions to arise or could be considered with a high level of confidence to be extremely unlikely of those conditions to arise. Paragraphs 3.56 and 3.57 of SSG-2 (Rev. 1) [2] provide recommendations on the categorization of the event sequences that could lead to an early radioactive release or a large radioactive release and for which specific demonstration of their 'practical elimination' is required. Paragraphs 7.68 to 7.72 of SSG-2 (Rev. 1) [2] provide recommendations on deterministic safety analysis in support of that 'practical elimination'.

3.2. PARTICIPATING TECHNICAL EXPERTS' CONSIDERATIONS

There is a variety of approaches among the participating technical experts regarding the development of representative sets of DEC with core melting ranging from a simple postulated

DEC list to a systematic approach. The main elements considered by the participating technical experts when forming sets of DEC with core melting are the following:

(a) National and international operating experience feedback (considering lessons learned from previous severe accidents and/or other accidents which could result into a core melting stage but were prevented in time owing to operator intervention);
(b) Engineering judgement (identification of all the threats to the integrity of the remaining physical barriers that need to be considered);
(c) Results of the deterministic analyses (identification of the penalizing scenarios regarding the phenomena considered);
(d) Results of Level 1 PSA and Level 2 PSA (identification of the main contributors to core damage and to large releases).

Development of the sets of DEC with core melting could be based on the consideration of a combination of the aspects mentioned above or could rely just on a few of these aspects as applicable. For example, participating technical experts from Romania, Bulgaria and the Islamic Republic of Iran reported, the sets of DEC with core melting are mostly defined on the basis of physical phenomena to be addressed. Participating technical experts from Germany and Japan stated PSA is the main basis to define the scope of DEC with core melting. Participating technical experts from Canada, Finland, France[5], the Russian Federation and the United States of America reported, most of the aspects mentioned above are considered in the definition of the sets of DEC with core melting.

Some participating technical experts, such as those from Canada, India, Japan and the Russian Federation reported using the generic list of DEC with core melting (developed by the vendor or established in the regulations) as a basis for plant specific list of DEC with core melting. In general, engineering judgment and operating experience feedback are used to justify the completeness and representativeness of DEC with core melting.

Participating technical experts from Canada reported, PSA allows systematic identification of event sequences leading to challenges with the fundamental safety functions. Representative event sequences are then analysed using deterministic safety analysis techniques to assess the extent of fuel failures, damage to the reactor core, primary heat transport system and containment, and releases of radionuclides. In the use of any cut-off limit for the frequency of occurrence of analysed DEC, the safety goals established for the plant need to be considered and to be consistent with the safety analysis objectives.

Participating technical experts from Finland and France stated (for the European Pressurized Reactor under construction), a list of DEC with core melting phenomena that can affect the containment is established first. Then, for each phenomenon, a set of scenarios is chosen to define the dispositions that will mitigate their consequences. For the European Pressurized Reactor, the following DECs with core melting sets are defined:

(a) ‘Representative’ scenarios against which the design features (severe accident management (SAM) systems) are defined. Participating technical experts from Finland stated these analyses are conducted with the assumption that systems function as designed with the assumed most penalizing single failure;

[5] In France, the approach is primarily deterministic; PSA studies allow to complete, if necessary, and validate the list of DEC with core melting.

(b) ‘Extreme’ scenarios against which the robustness of SAM systems and severe accident measures are studied. With these analyses, absence of cliff edge effects is investigated and confirmed. Analyses are done with the assumption of failures or delays in performing safety functions (e.g. primary circuit depressurization), excluding the loss of the confinement function.

Participating technical experts from the Russian Federation reported, the list of DEC with core melting is based on a list of scenarios. The representativeness of the scenarios is ensured by taking into account the severity levels of the plant states together with states of operability and inoperability of safety systems and safety features, dedicated for severe accident management. A special procedure on how to elaborate the representative list of scenarios without significant fuel degradation and with core melting is recommended in the regulatory guide RB-150-18 [14]. According to this guide, the main goal of developing the representative DEC list is to create the basis for the development of severe accident management guidelines (SAMGs). In order to fulfil the representativeness requirement, the list of DEC is expected to cover all levels of severity, arising from a severe accident which differ among themselves in relation to the severe accident management strategy considered to cope with each of them in the list of DEC.

Further categorization of DEC with core melting could be done in different ways, according to the following:

(a) Plant operational modes (e.g. power operation, shutdown, refuelling);
(b) Initiating events (e.g. primary leaks, primary to secondary leaks, loss of power);
(c) Location of the fuel (reactor, spent fuel pool, dry storage casks);
(d) Objectives of analyses (to confirm the robustness of systems, dedicated in the design for SAM, or to confirm the limitations of the radiological consequences);
(e) The studied phenomena (e.g. molten corium–concrete interaction, recriticality, hydrogen combustion risk);
(f) External events that can affect several units at the same site.

4. CONTROLLED AND SAFE STATES OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING

4.1. IAEA REFERENCES

Paragraph 5.27 of SSR-2/1 (Rev. 1) [1], states:

> “The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is practically eliminated.”

A ‘*controlled state’* is defined in the IAEA Safety Glossary [4], as a “plant state following an anticipated operational occurrence or accident conditions, in which fulfilment of the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state.”

A ‘*safe state’* is defined in Ref. [4] as a “plant state following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.”

The concept of safe state appears in SSR-2/1 (Rev. 1) [1], in paragraphs 2.13 and 2.13 related to level 2 and level 3 defence in depth respectively, in para. 5.24 under Requirement 19: Design basis accidents and in footnote 15 related to para. 5.29 under Requirement 20: Design extension conditions. The concept of safe state is also mentioned in para. 5.53 of SSR-2/1 (Rev. 1) [1] related to the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state.

Requirement 65: Control room in SSR-2/1 (Rev. 1) [1] states:

> "A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions."

It is understood that accident conditions mentioned in this requirement include also DEC with core melting.

The concept of safe state or safe and stable state is also reflected in the recommendations in paras 3.23, 7.27 and 8.9 of SSG-2 (Rev. 1) [2]. In particular, para. 8.9 states that "The time span covered by any scenario analysed and presented should extend up to the moment when the plant reaches a safe and stable end state (although not all sensitivity calculations need necessarily be presented over the full timescale)".

The items used in DEC to bring the plant in a controlled state are the safety features, although footnote 15 of SSR-2/1 (Rev. 1) [1], mentioned above, allows the temporary use of additional systems in complement to the full design capabilities of the plant for returning the plant to a safe state or for mitigating the consequences of an accident. According to paras 4.13A and 5.29 of SSR-2/1 (Rev. 1) [1], the safety features for DEC are required to be designed in such a way that they are independent, as far as practicable, from safety systems used in more frequent accidents.

4.2. PARTICIPATING TECHNICAL EXPERTS' CONSIDERATIONS

In general, participating technical experts from Canada, Finland, France, the Russian Federation, the United States of America reported they have established requirements stating that in DEC with core melting analysis, it has to be shown that a safe state is reached and maintained for a long time[6].

Participating technical experts use different wording such as 'safe state', 'safe shutdown state', 'controlled safe state', 'severe accident safe state' or 'long term safe stable state' to describe the ultimate acceptable condition of a nuclear power plant following DEC with core melting. For simplicity, from this point onwards in this section the term 'safe state' will be used.

Generally, this definition is derived from the IAEA safe state definition then adapted to the particular situation of a severe accident where the instrumentation needed to characterize a safe

[6] There is no precise duration for maintaining the safe state in case of DEC with core melting. In practice, this duration goes up to the removal of the damaged fuel from the plant. However, in the safety demonstration, a shorter duration is considered and that it is sufficient to implement countermeasures if necessary.

state can be lost or does not exist. In this case, indirect measurements or analysis could be accepted to justify that a controlled state or a safe state has been reached.

Besides the safe state, an intermediate 'controlled' state following a severe reactor accident is considered, which was confirmed by some participating technical experts such as those from France, Finland and the Russian Federation. For example, participating technical experts from Finland reported, a controlled state following DEC with core melting is defined as the state where the removal of decay heat from the reactor core debris and the containment has been secured, the temperature of the reactor core debris is stable or decreasing, the reactor core debris is in a form that poses no risk of recriticality, and no significant volumes of fission products are any longer being released from the reactor core debris.

Consistent with the IAEA definition, some participating technical experts reported they define the acceptable safe state as the plant state in which the fundamental safety functions are ensured for a long time. Those participating technical experts from Canada, Finland, France, the Russian Federation, India, and the United States of America reported they prefer to define the safety functions as being reactivity control ensuring subcriticality, cooling and confinement in order to limit radioactive releases. Participating technical experts from France reported they further define the safe state as stabilized and cooled core melt, removal of heat outside of the containment, confinement of radioactive material, but practically the studies aim at demonstrating more specific technical acceptance criteria such as the containment pressure and temperature rather than focusing on the safe state. Participating technical experts from Finland reported they also require that the safe state following a severe reactor accident meets the criteria listed above for the controlled state following a severe reactor accident. In addition, participating technical experts from Finland reported they require the pressure inside the containment is low enough such that leaks from the containment are minor, even if the containment is not leaktight. Participating technical experts from the Russian Federation reported, a safe state is a state of the power unit maintained for an unlimited time, during which the basic safety functions established in federal norms and rules are fulfilled. Some participating technical experts such as those from Canada and France reported they specify that the safe state is not reached until there are means to maintain these safety functions for a long term, but most of them are silent on the expected future performance of the safety functions. Participating technical experts from France reported, Électricité de France (EDF) does not consider the safe state to be reached until critical parameters have remained in the stabilized zone for at least 24 hours as per the severe management guidelines. Participating technical experts from the United States of America reported, a safe state for more likely severe accident challenges is that the reactor containment function is expected to provide a leak-tight barrier for 24 hours. After 24 hours, the reactor containment function continues to provide a barrier against uncontrolled release of radionuclides.

Because it is difficult to monitor or assess the local corium subcriticality during the degradation of corium in the reactor vessel or when relocating outside of the vessel, it would be difficult to demonstrate that subcriticality of the corium is ensured. Therefore, some participating technical experts confirmed it is assumed that the subcriticality may be temporarily lost, provided that this does not jeopardize residual heat removal. Similarly, the residual heat may temporarily not be removed if this does not jeopardize the control of the confinement of radiological substances.

No participating technical expert makes a distinction between a safe state with the melt retained in the reactor vessel and a safe state in which the melt is stabilized and cooled in the containment outside the reactor vessel.

For instance, participating technical experts from Canada stated, the analysis covers the event from the initial steady state up to a predefined long term stable state. The duration of the transients considered in the analysis needs to be sufficient to determine the event consequences. Therefore, the calculations for plant transients are extended beyond the point where the NPP has been brought to shutdown and stable core cooling, as established by some identified means (i.e. to the point where a long term stable state has been reached and is expected to remain as long as required). The analysis is expected to take into account the capacity and limitations of long term makeup water and electrical power supplies.

Some participating technical experts, such as those from Canada, Finland and France, note that because fuel melting in the spent fuel pool has to be 'practically eliminated', there is no need to define a safe state for DEC with fuel melting in the spent fuel pool. Participating technical experts from the United States of America stated, licensees need to demonstrate capability to prevent and mitigate spent fuel pool severe accidents. Participating technical experts from the Russian Federation stated, licensees need to demonstrate capability to prevent or to mitigate spent fuel pool severe accidents in case they happen, and to assess their radiological consequences. The DEC representative list includes the relevant scenarios.

5. TYPE OF ANALYSIS METHODOLOGIES RELEVANT TO DESIGN EXTENSION CONDITIONS WITH CORE MELTING

5.1. IAEA REFERENCES

In SSR-2/1 (Rev. 1) [1], footnote 13 states that DEC analysis "could be performed by means of the best estimate approach". This means that the analysis could be performed as "realistically as possible" according to the state of the art knowledge; this applies to the computer codes used, initial and boundary conditions, and to the availability of the systems and operator actions. In particular, redundancies necessary to comply with the single failure criterion are not required, provided the reliability of the function to be accomplished is adequate. Insights on the best estimate approach that could be applied to the analysis of DEC with core melting are included in SSG-2 (Rev. 1) [2].

Requirement 17 of IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities [5] states that: "Uncertainty and sensitivity analysis shall be performed and taken into account in the results of the safety analysis and the conclusions drawn from it".

Paragraph 4.59 of GSR Part 4 (Rev. 1) [5] states:

> "Uncertainties in the safety analysis shall be characterized with respect to their source, nature and degree, using quantitative methods, professional judgement or both. Uncertainties that may have implications for the outcome of the safety analysis and for decisions made on that basis shall be addressed in uncertainty and sensitivity analyses. Uncertainty analysis refers mainly to the statistical combination and propagation of uncertainties in data, whereas sensitivity analysis refers to the sensitivity of results to major assumptions about parameters, scenarios or modelling."

Paragraph 5.73 of SSR-2/1 (Rev. 1) [1], states that: "The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in

particular that adequate margins are available to avoid cliff edge effects[7] and early radioactive releases or large radioactive releases."

Paragraphs 7.1-7.72 of SSG-2 (Rev. 1) [2] provide recommendations on deterministic safety analysis of plants states of nuclear power plants, by addressing, for each type of plant state, specific objectives of the analysis, the acceptance criteria, the availability of features and systems, operator actions, and analysis assumptions and treatment of uncertainties.

In particular, para. 7.63 of SSG-2 (Rev. 1) [2] states that: "For design extension conditions with core melting, the single failure criterion does not need to be applied. Furthermore, unavailability of a system or a component due to maintenance does not need to be considered in the deterministic analysis. Appropriate rules should be defined for testing and maintenance of systems or components necessary for design extension conditions to ensure their availability".

Moreover, para. 7.67 of SSG-2 (Rev. 1) [2] states that: "Analysis of severe accidents should be performed using a realistic approach (Option 4 in Table 1, Section 2) to the extent practicable. Since explicit quantification of uncertainties may be impracticable due to the complexity of phenomena and insufficient experimental data, sensitivity analyses should be performed to demonstrate the robustness of the results and the conclusions of the severe accident analyses".

5.2. PARTICIPATING TECHNICAL EXPERTS' CONSIDERATIONS

5.2.1. Best estimate analysis approach (methodology)

Both deterministic safety analysis (DSA) and probabilistic safety assessment (PSA), complement each other for the assessment of DEC with core melting. There is a general agreement among all participating technical experts for using a best estimate analysis methodology according to the state of the art knowledge, although those participating technical experts reported they use assumptions that might be more conservative when it is justified, e.g. to perform bounding analysis[8].

It is commonly recognized that a severe accident best estimate analysis methodology is performed as 'realistically as possible' according to the state of the art knowledge; this applies to aspects such as facility representation, initial and boundary conditions, operator actions, the availability of the safety features as well as to the computer codes used.

Facility representation

Most participating technical experts reported, a realistic representation of the facility is defined and applied when performing the numerical simulation of DEC with a core melting scenario. The representation of the facility is as close to the actual plant as practical to ensure correct accident progression, enable correct modelling of the expected physical phenomena, and achieve accurate results of the accident analysis.

[7] A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input [4].

[8] In France, in practice, the parameters chosen need to be such as to reasonably cover the physical modelling uncertainties if they are proven.

Initial and boundary conditions

The initial conditions of the facility in the analysis are modelled by choosing input parameters for the calculation model. Bases for numerical values used in accident analysis have to be specified and justified.

Initial conditions can be chosen with a realistic or a conservative manner. Best estimate methods for determining initial conditions are applied as reported by participating technical experts from Bulgaria, Canada, France, Germany, India, Japan, the Russian Federation and the United States of America. Conservative methods for initial conditions, for parameters of major influence (95%/95%), are applied the Islamic Republic of Iran, Romania and Sweden.

The boundary conditions for the analysis can be modelled through system performance, e.g. the assumption of how the credited safety features operate in the analysed scenario. This performance is modelled realistically, according to the design parameters as reported by participating technical experts from countries, such as Bulgaria, Canada, France, Germany, India, Japan, the Russian Federation, and the United States of America. The assumption in these analyses is that the system capability is as designed (nominal) and no variation in the parameter's value is applied in the analysis. When considering assessing the variation of the feature or system capability or its momentary performance in a conservative manner, the minimum or maximum design capability can be applied as a boundary condition, as reported by participating technical experts from the Islamic Republic of Iran. Participating technical experts from Romania reported, the feature or system performance is assumed to be as designed, but with added conservatism to cover possible uncertainties.

There is also a common understanding among participating technical experts that using best estimate methods in DEC with core melting analysis make it possible to ensure consistency with the SAM of which the development and/or the validation are supported by DEC with core melting analysis. As the accident progresses to core melting, severe accident management actions become an important part of defence in depth. It is desired that the consequences of DEC with core melting are estimated so that the analysis results reflect a realistic plant response and provide best estimate information for accident management. The management of severe accidents is generally a challenging arbitration between the various risks incurred. A conservative approach may skew this arbitrage and lead to deviation from optimal severe accident management strategies; therefore, DEC with core melting analysis, performed for the safety demonstration where conservative assumptions have been made, are not recommended to be used for the development and/or the validation of SAM.

In addition to best estimate studies, sensitivity analyses need to be performed to demonstrate the avoidance of cliff edge effects or challenges (e.g. the largest hydrogen concentration or generation rate) to ensure that the required additional safety features considered in the design of the plant are capable of coping with the DEC with core melting. As for the production of hydrogen, it has to be demonstrated that the hydrogen mitigation measures (e.g. passive autocatalytic recombiners and/or igniters, mixing in the containment airspace) are capable to operate under DEC with core melting to prevent any challenge to the integrity of the containment. Besides, as reported by participating technical experts from Finland coping with the highest challenge is a way to achieve the defined requirement that such events have to be practically eliminated. The deterministic analyses complemented by probabilistic risk assessments and expert judgement are required to justify that a load jeopardising the integrity of the containment during a severe reactor accident is practically eliminated. This includes events such as reactor pressure vessel breach at high pressure, hydrogen explosion, steam

explosions, direct impact of molten reactor core on containment basemat or wall and uncontrolled containment pressure increase.

Operator actions

Most participating technical experts, such as those from Canada, the Russian Federation, France, Finland, and the United States of America reported, the operator actions are considered on a best estimate basis consistent with the SAM guidelines. Action times may account for harsh environmental conditions (e.g. radiation levels, temperature) and possible delays due to infrastructure damage.

For example, participating technical experts from France stated, DEC with core melting analysis include sensitivity studies such as a delay of immediate actions performed from the main control room up to one hour from the beginning of core melting. These studies help to ensure margins with respect to possible cliff edge effect.

Equipment credited in DEC with core melting

All participating technical experts confirmed the availability of equipment, including instrumentation and control, credited in the safety demonstration of DEC with core melting has to be justified. Many participating technical experts, such as those from Canada, France, Germany, India, the Russian Federation and the United States of America, reported the availability of systems and components is assumed if their failure is not postulated as part of the accident sequence or consequently to it and their operation under severe accident environment is demonstrated.

While using dedicated additional safety features for DEC with core melting is recognized to provide more robustness in the safety demonstration as it does not depend on the accident path that leads to core melting, participating technical experts' positions differ on the systems that can be used to bring the plant to a safe state. Many participating technical experts reported, additional safety features credited in DEC with core melting are required to be independent (physically and functionally separate) from all other safety systems as far as practicable. Among all participating technical experts, those from Finland confirmed they are the only one country to require the active parts of the additional safety features credited in DEC with core melting and of their support systems (e.g. power supply, cooling chain, instrumentation and control) to be single failure tolerant. Participating technical experts from France reported, the independence of the additional safety features for DEC without significant fuel degradation and the additional safety features for DEC with core melting needs also to be sought as far as possible, but no redundancy is required for additional safety features for DEC with core melting. However, it is required that the failures considered in the sequences before reaching DEC with core melting, such as failures in DEC without significant fuel degradation situations, do not jeopardize the operation of additional safety features for DEC with core melting, recognising that a total independence is a challenge, for some systems (e.g. containment isolation). Several participating technical experts, such as those from Canada, the Russian Federation, and the United States of America, reported they consider that deterministic analysis of DEC with core melting may use applicable[9] inputs from PSAs and may credit all the available SSCs, as long as it has been demonstrated (with reasonable confidence) that they are able to perform their

[9] Applicability is shown by demonstrating that the assumptions, models and rules used for generation of the information in the PSA are compatible with the use of that data.

intended function in DEC with core melting. However, some participating technical experts such as those from Finland and France stated they require that only those additional safety features designed and qualified for DEC with core melting can be credited in the safety demonstration.

For the context of DEC analysis, only participating technical experts from Canada reported they introduced the reasonable confidence concept which is defined as a better than average expectation that the SSCs or actions will achieve the minimum safety functionality required for success.

Participating technical experts from Canada, Finland, France, the Russian Federation and the United States of America reported they generally require functional capability, during postulated severe accident conditions, of additional safety features to cope with DEC with core melting. As reported by the participating technical experts, that functional capability is substantiated differently. For example, in Finland and France through qualification, in Canada and the United State of America through survivability proofness and in the Russian Federation through a similar concept for qualification of survivability. Additionally, participating technical experts from Finland, France, and the Russian Federation reported they require the additional safety features to be safety class 3. It is noted that participating technical experts from the Russian Federation reported functionality and safety class requirements only apply to systems to be used in DEC management within the first three days following the accident initiation (it is assumed that recovery of the failed NPP equipment and external support provision are limited during this period, but after the 72 hour period the accident response tools are prepared and deployed and the failed equipment for DEC management means can be replaced or repaired). As reported by the participating technical experts from the United States of America, "additional safety features" (as stated in Requirement 20 of SSR-2/1 (Rev. 1) [1]) to cope with DEC with core melting, determined to be risk-significant[10], may be subject to augmented design standards. Participating technical experts from France, Finland, Romania, the Russian Federation, and the United States of America stated they generally require that the containment include measurement and monitoring systems to follow the progress of the accident and confirm a safe state is reached. Most participating technical experts reported they require each unit to have its own additional safety features for DEC.

The answers presented by the participating technical experts confirmed the systems credited in the DEC analysis depend on each Member States' regulations and approaches. Participating technical experts reported that to the extent practicable, safety systems credited for DBA are not used for DEC with core melting in many Member States the participating technical experts represented. This is to comply with the national requirements for independence between level of defence in depth, as far as practicable. All participating technical experts reported they consider the environmental conditions of the accident as limiting the ability to credit a system: if a system cannot withstand the environmental conditions of a core melting scenario, it cannot be credited in the scenario analysis.

Among the participating technical experts, two different approaches are applied:

(1) All available systems are credited;

[10] In the United States Nuclear Regulatory Commission terminology, 'risk-significant' can refer to a facility's system, structure, component, or accident sequence that exceeds a predetermined limit for contributing to the risk associated with the facility. The term also describes a level of risk exceeding a predetermined 'significance' level. https://www.nrc.gov/reading-rm/basic-ref/glossary/risk-significant.html.

(2) Only systems designed for DEC with core melting scenario are credited.

The first approach was reported that is applied in Bulgaria, Germany, India, the Russian Federation, the United States of America and Canada, where any systems not affected by the progression of the accident sequence can be credited in DEC with core melting analysis.

Participating technical experts from Finland reported they apply the second approach, where the requirements call for the independent set of additional safety features, designed only for severe accident management purpose; in DEC with core melting analysis only those additional safety features are credited. Participating technical experts from France, the Islamic Republic of Iran, Japan, Romania and Sweden reported they follow a similar approach, but systems or features not dedicated to DEC with core melting may be used provided a case by case justification.

5.2.2. Use of non-permanent equipment

Some participating technical experts reported they credit non-permanent equipment in DEC with core melting. However, this has to be realistically justified in terms of bringing the equipment to the site (including assessment of the availability of necessary transport routes, their protection from external and internal event impacts) and the time needed to connect them to the facility and supporting systems, with consideration of possible harsh conditions. Also, there is a need to consider and justify that the non-permanent equipment can be connected in time to avoid any cliff edge effect and large radioactive releases. Emergency drills could be a way to confirm these justifications. When the demonstration is not achieved, the use of the non-permanent equipment needs to be revisited; this might necessitate to permanently install them on site.

Participating technical experts from Germany, India, the Islamic Republic of Iran and Japan reported they credit on-site non-permanent equipment, but not off-site non-permanent equipment. Participating technical experts from Bulgaria, Canada, France, Romania, the Russian Federation, Sweden and the United States of America reported, all non-permanent equipment can be used to manage DEC with core melting. Participating technical experts from France stated, however, such equipment cannot be credited as part of the formal severe accident safety demonstration. They are only introduced in robustness studies for extremely unlikely events such as extended loss of all AC power. Participating technical experts from Finland stated the practice is that non-permanent equipment is not credited in the DEC with core melting analysis or as a mean of severe accident management.

All participating technical experts reported that credit non-permanent equipment in DEC with core melting analysis declared having the means of connecting the non-permanent equipment included in the design of the facility (e.g. permanent connections to pipelines or to power supply).

When considering the usage of non-permanent equipment, many participating technical experts reported they have specific time requirements for their deployment; the achievement of such requirements needs to be demonstrated. For on-site non-permanent equipment, a minimal deployment time of 8-24 hours is applied (Canada (8 hours), Germany (10 hours), India (24 hours), Japan (12 hours), Sweden (8 hours)) and for off-site non-permanent equipment, this minimal time is 24 hours (Sweden) or 72 hours (Canada, Romania). Participating technical experts from France reported the deployment time of off-site non-permanent equipment depends on the environmental conditions and the size or weight of the equipment (from 24

hours for ‘light equipment’ up to 100 hours for heavy equipment in case of extreme earthquake or flood with limited access to the plant, for instance).

5.2.3. Application of the single failure criterion

It is worth noting that most participating technical experts reported, the single-failure criterion, which does apply to all safety groups credited in DBAs, does not have to apply to DEC with core melting analysis. However, the application of the single failure criterion to active components in safety features for DEC with core melting appears to be required only in Finland.

5.2.4. Accounting for uncertainties and performing uncertainty evaluation

It is commonly recognized that there are two types of uncertainty: aleatory (or stochastic) uncertainty and epistemic uncertainty. Aleatory uncertainty is related to events or phenomena that occur in a random manner, such as random failures of equipment, or to the performance of an operator action. These aspects of uncertainty are inherent in the logical structure of the probabilistic model. Epistemic uncertainty is associated with the state of knowledge relating to a given situation under consideration. In any analysis or analytical model of a physical phenomenon, simplifications and assumptions are made. Even for a relatively simple situation, a model may omit some aspects that are considered as not significant or as being of secondary importance with respect to the solution. Additionally, the state of knowledge within the relevant scientific and engineering disciplines might be incomplete. Simplifications and incompleteness of knowledge give rise to some uncertainties in the prediction of the outcomes for a specific situation.

There is a common understanding among participating technical experts that epistemic uncertainties in the analytical prediction of challenges to fission product barriers are to be taken into account, as practicable, if the level of knowledge of important severe accident phenomena and physical processes is low or if the associated supporting experimental data are insufficient.

There is a common agreement among many participating technical experts, that the uncertainties in the phenomena involved in DEC with core melting, particularly in their late phase, are so large that fully implementing a best estimate plus uncertainty method is difficult to achieve and is not formally required. It is not achievable to perform uncertainty analyses in a reliable manner considering the lack of knowledge, e.g. of the distribution of the uncertainty of the relevant parameters. Rather than uncertainty analyses, sensitivity studies are deemed to be more appropriate to demonstrate the robustness of the results and the conclusions of DEC with core melting analysis.

However, quantification of uncertainties is required, as reported by participating technical experts from Japan and in the Russian Federation and soon to be, as reported by participating technical experts from the United States of America. Participating technical experts from the Russian Federation reported, the uncertainties’ studies of the phenomena involved in DEC with core melting are a mandatory part of code certification (uncertainties of a physical phenomenon, simplifications and assumptions). Uncertainties encountered during validation need to be considered in the DEC with core melting safety analysis. Uncertainty studies, with uncertainty propagation, as reported by participating technical experts from the United States of America were performed to determine the likelihood that the molten core remains in-vessel, and the likelihood of in-vessel steam explosions. Moreover, as reported by participating technical experts from the United States of America, applicants are expected to follow the ‘Probabilistic

Risk Assessment standard', which requires that DEC with core melting analysis supporting the Level 2 PSA discuss the treatment of uncertainties.

It is important however, to highlight that a number of initiatives, at the IAEA and the European Commission (EC) involving a number of Member States are being undertaken to expand the best estimate and uncertainty evaluation methodologies to the DEC with core melting.

5.2.5. Performing sensitivity analyses

Sensitivity analyses for DEC with core melting need to be performed to identify and rank important phenomena and parameters and to assess their impact on the analysis results. The results of sensitivity analyses provide additional insights to evaluate grace times, to optimize SAM and to investigate cliff edge effects, as well as to verify complex design features and modelling aspects. Sensitivity analyses for DEC with core melting analysis are performed as reported by participating technical experts from Bulgaria, Canada, France, India, Japan, Romania, the Russian Federation, Sweden and the United States of America.

5.2.6. Considering cliff edge effects and safety margins

All participating technical experts reported they share the same understanding that margins to cliff edge effects are assessed by means of sensitivity calculations. Expert judgement is used to determine if the safety margins are sufficient. For DEC with core melting, the principle is that there is a 'reasonable confidence'[11] that the acceptance criteria are met.

6. APPLICABILITY OF COMPUTATIONAL TOOLS AND COMPUTER CODES

6.1. IAEA REFERENCES

Paragraph 4.60 of GSR Part 4 [5] states:

> "Any calculational methods and computer codes used in the safety analysis shall undergo verification and validation to a sufficient degree. Model verification is the process of determining that a computational model correctly implements the intended conceptual model or mathematical model; that is, whether the controlling physical equations and data have been correctly translated into the computer codes. System code verification is the review of source coding in relation to its description in the system code documentation. Model validation is the process of determining whether a mathematical model is an adequate representation of the real system being modelled, by comparing the predictions of the model with observations of the real system or with experimental data. System code validation is the assessment of the accuracy of values predicted by the system code against relevant experimental data for the important phenomena expected to occur. The uncertainties, approximations made in the models, and shortcomings in the models and the underlying basis of data, and how these are to be taken into account in the safety analysis, shall all be identified and specified in the validation process. In addition, it shall be ensured that users of the code have sufficient experience in the application of the code to the type of facility or activity to be analysed."

[11] In Canada, 'reasonable confidence' means a higher than average expectation (the confidence level is higher than 50%) that acceptance criteria are met. The United States of America use the term 'reasonable assurance', which is determined by expert judgement.

Paragraphs 5.1–5.43 of SSG-2 (Rev. 1) [2] provide recommendations on the use of computer codes for deterministic safety analysis that address the rules for selecting and using computer codes, for the process management in connection with the use of computer codes, for verification of computer codes, for validation of computer codes, for qualification of input data and documentation of computer codes. In particular, para. 5.22 of SSG-2 (Rev. 1) [2] states that: "Validation of the computer code should provide confidence in the ability of a code to predict, realistically or conservatively as required, the values of the safety parameter or parameters of interest. The level of confidence provided by the validation should be appropriate to the type of analysis. For example, the scope of validation may be relaxed for codes used in severe accident analysis, in view of the limited experimental data available, in which case additional reliance should be placed on verification (see paras 5.14–5.20)".

The following list identifies what a well validated tool means, recognizing it is not fully applicable to severe accident codes (see Ref. [6]):

(a) Each phenomenon needs to be addressed in test facilities of different scales;
(b) Each single model within the code is expected to be validated in separate effects tests, if possible, on different scales;
(c) The models need to be validated in coupled effects tests with regard to their complex interactions and scaling aspects;
(d) The overall capability of the code is to be demonstrated by means of numerous 'blind' pre-test calculations for different types of experiments.

6.2. PARTICIPATING TECHNICAL EXPERTS' CONSIDERATIONS

6.2.1. General computational tool and computer code applicability

There is a general understanding among the participating technical experts that there are no additional code applicability requirements on computational tools or computer code used for DEC with core melting, compared to those used for DBA. In addition, there is a shared understanding that the extent of the verification and validation necessary and the means of achieving it depend on the specific applications. The shared key message is that in both deterministic and probabilistic safety analyses for DEC with core melting, the computational tool and computer code applicability needs to be appropriate and adequate for the purpose of the analyses.

Participating technical experts from Canada reported, the principle is that there need to be a 'reasonable confidence' in the analysis results. This implies that the application of the requirements for verification and validation are not as rigorous as for the verification and validation of the tools used for DBA analysis and that the use of the common CSA standard N286.7-16, Quality assurance of analytical, scientific, and design computer programs [7], is adapted to the analysis under consideration.

In France, Article 3.8 of the Order of 7 February 2012 [8], states that:

"I – The demonstration of nuclear safety is based on:

— up to date and referenced data; it takes into account the available information mentioned in the Article 2.7.2[12];

— appropriate, clearly explained and validated methods, integrating assumptions and rules adapted to the uncertainties and limits of knowledge of the phenomena in play;

— calculation and modelling tools qualified for the areas in which they are used.

II – The licensee specifies and justifies its criteria for validating the methods, for qualifying the calculation and modelling tools, and for assessing the results of the studies carried out to demonstrate nuclear safety."

In general, participating technical experts reported they consider that some established severe accident computer codes, such as ASTEC, MAAP, MELCOR, SAMPSON and SOCRAT may be applied for DEC with core melting analysis within their domain of validity defined as part of the verification and validation process, but engineering judgement is still necessary to assess the results. Hence, the user needs to be qualified for using the computer codes. The qualification of the user includes the following:

(a) The user has adequate training on the use of the computer code(s);
(b) The user has good understanding of the models and methods used in the code(s);
(c) The user has sufficient understanding of the code limitations for a specific application;
(d) Adequate guidance is available to the user;
(e) The user rigorously follows the recommendations, in particular those relevant to the specific application in the frame of the analysis;
(f) The output of the code(s) is evaluated and understood adequately and used correctly by the user.

6.2.2. Certification of computer codes

Participating technical experts from Canada, Finland, France, and the United States of America reported they do not certify or require the certification of computer codes used for the assessment of DEC with core melting. It appears that only the Russian Federation certifies them. Therefore, code certification, as reported by participating technical experts from the Russian Federation, is a procedure whereby a group of authorized experts evaluates the results of code validation and verification presented in a special report prepared by the code developer in accordance with the requirements established by the regulatory body. The result of this procedure is the preparation of a certificate, which provides a brief description of the purpose of the code and confirms the area of applicability of the code, errors of calculation and restrictions on the application, including the duration of the certification.

Participating technical experts generally agree that whether the codes are certified or not, they need to be verified and validated.

[12] Article 2.7.2 requires the operator to take all necessary steps to collect information likely to reduce the risks or drawbacks of nuclear power plants with respect to public safety, health and public safety or the protection of the nature and the environment [8].

6.2.3. Verification of computer codes

For the verification of the tools used for analysis of DEC with core melting, as a part of quality assurance, there is a coherent view among most participating technical experts that the tools need to undergo an extensive review by the tool developer or user and that this review is equivalent to the verification of the tools used for DBA analysis. As reported by participating technical experts from the Russian Federation, verification of the codes used for analysis of DEC with core melting is part of an obligatory procedure of certification of the code (see 6.2.2).

6.2.4. Validation of computer codes

Participating technical experts stated they generally agree that the use and selection of analytical tools is done on the basis of limits of applicability, suitability for purpose and adequacy of validation and verification.

The validation of computer tools is a continuous process, and significant progress in this area can be expected in the future. The validation process would follow the same process as for the validation of the tools used for DBA. Still, for some participating technical experts, the application of the validation process of computer tools used for DECs with core melting may be relaxed in view of the experimental data available. To overcome limited availability of experimental data, some participating technical experts, such as those from Canada and France are conducting R&D severe accident programmes to improve severe accident phenomena modelling and to upgrade the validation level and application domain of their tools. As reported by participating technical experts from France, comparisons of MAAP code (used by EDF) and ASTEC code (used by IRSN) contribute to their mutual validation.

In addition, code-to-code comparison and crosswalk analysis are performed to help understand the analysis of the Three Mile Island accident and the Fukushima Daiichi nuclear accident.

Nevertheless, some participating technical experts, such as those from the United States of America, do not formally require validation, but it is expected that the applicant will use well-established and validated codes, such as MAAP or MELCOR codes.

6.2.5. Independent analyses by the regulatory body

The regulatory bodies, as reported by some participating technical experts, such as those from Canada, Finland, France, the United States of America, and the Russian Federation, conduct, as deemed necessary, independent confirmatory analyses for selected specific accident sequences to evaluate safety analysis results for the specific applications and/or confirm the validation of the tools.

For example, as reported by participating technical experts from the United States of America, according to the Nuclear Regulatory Commission Standard Review Plan (NUREG-0800, Ch. 19.0 [11]), the regulatory body of the United States of America runs independent confirmatory analysis with MELCOR, a fully integrated computer code that they developed and continue to sponsor. This well-established code has been validated against a broad set of experiments and the regulatory body is confident in its ability to predict severe accident progression and source terms. For some issues, the United States of America regulatory body runs independent uncertainty analysis and sensitivity analysis to determine the likelihood of phenomena. For example, NUREG/CR-6849 [12] assesses the likelihood of the molten core failing the reactor vessel lower head and subsequent potential for ex-vessel fuel coolant interaction in the AP1000 design.

6.2.6. Assessment of accuracy of the computer tools

Most participating technical experts reported, there is no indication that an assessment of the accuracy is required or even necessary since there is a general agreement among the scientific community that the level of uncertainty is still high and the level of knowledge in the severe accident progression and in the severe accident phenomena still needs more improvement.

7. ACCEPTANCE CRITERIA FOR DESIGN EXTENSION CONDITIONS WITH CORE MELTING ANALYSIS

7.1. IAEA REFERENCES

In accordance with Requirement 20 of SSR-2/1 (Rev. 1) [1], a set of applicable acceptance criteria for DEC with core melting analysis have to be identified, including any regulatory requirements. Indeed, paragraph 5.31A of SSR-2/1 (Rev. 1) [1] states that: "The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures." More specific technical criteria can be derived from this high level requirement and expressed as qualitative or quantitative acceptance criteria.

Recommendations on acceptance criteria for deterministic safety analysis are provided in paras 4.1–4.18 of SSG-2 (Rev. 1) [2]. More specifically, recommendations for acceptance criteria for DEC with core melting are provided in paras 7.58–7.60 that address radiological acceptance criteria (doses to the public or releases to environment), technical acceptance criteria (e.g. limitation of the containment pressure, containment water level, temperature and flammable gas concentrations, stabilization of molten corium), and on-site radiological acceptance criteria.

7.2. PARTICIPATING TECHNICAL EXPERTS' CONSIDERATIONS

Generally, participating technical experts reported they require accident conditions that could lead to early or large radioactive releases are practically eliminated, i.e. they are physically impossible or extremely unlikely to occur. For the accident conditions involving core melting that are not practically eliminated, there is a general agreement among participating technical experts from Bulgaria, Canada, Finland, France, Germany, India, Romania, the Russian Federation, Sweden, and the United States of America that they need to be studied as part of DEC with core melting to demonstrate that there is only a limited impact on people and environment. The exception from the participating technical experts contributing to the questionnaire were those from the Islamic Republic of Iran, which stated they require no impact on the population.

Participating technical experts reported they require differently the population protective measures in case of DEC with core melting, such as:

(a) limited impact on the population allows for evacuation (no evacuation before 24 hours, then no evacuation beyond 3 km in France[13], and beyond 5 km in Finland);
(b) no protection actions beyond the boundary of the Emergency Planning Zone (with the boundary set at 5 km in France, 20 km in Finland and not more than 25 km in the Russian Federation) and;

[13] In France a release is considered small if it does not require any protection countermeasures.

(c) no permanent relocation (Canada, Bulgaria, Finland France, India) or;
(d) long-term restrictions on the use of extensive areas of water and land (Finland, France).

As reported by participating technical experts from Canada and France, they allow the use of protective measures that are of limited scope in terms of area and time, provided sufficient time is available to implement these measures. Participating technical experts from India explicitly states these protective measures can include off-site interventions.

Many participating technical experts stated they further quantify the requirement for practical elimination of accident conditions that could lead to early or large radioactive releases using numerical safety criteria for small and/or large release frequency. For example, safety goals for large release frequency (for internal events and external hazards) are specified as less than 10^{-6} per reactor year (/r.y) in Canada and the United States of America, as less than 5.10^{-7}/r.y in Finland or as less than 10^{-7}/r.y in Romania and the Russian Federation. Canada has a safety goal for small release frequency of less than 10^{-5} /r.y. Small release is defined in Canada as less than 10^{15} Bq of iodine-131. Large release is defined in Canada, Finland and by the Tokyo Electric Power Company (TEPCO) as greater than 10^{14}Bq of caesium-137, in France as effective doses higher than 50mSv over 7 days and beyond 3 km (or higher than 10mSv beyond 5 km) or thyroid doses higher than 50mSv over 7 days beyond 5 km, in Germany as low as reasonably achievable, and in the United States of America it is defined by individual reactor vendors to be consistent with the Safety Goal Policy Statement[14].

As reported by participating technical experts, performance goals for containment include a conditional containment failure probability (given core damage) of less than 0.1 in the United States of America or a requirement that loss of containment function in the early phase of the severe accident is only a small contributor to the reactor core damage frequency in Finland. Participating technical experts from India stated they specify that containment be leaktight for a time sufficient to implement off-site emergency procedures and prevent uncontrolled release after this period. Participating technical experts from the Russian Federation reported they require the containment to perform its function and that there is no expected detonation of flammable gases.

8. DOCUMENTATION OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING ANALYSIS

8.1. IAEA REFERENCES

GSR Part 4 (Rev. 1) [5], states:

> "The results and findings of the safety assessment shall be documented, as appropriate, in the form of a safety report that reflects the complexity of the facility or activity and the radiation risks associated with it. The safety report presents the assessments and the analyses that have been carried out for the purposes of demonstrating that the facility or activity is in compliance with the fundamental safety principles and the requirements established in this Safety Requirements publication, and with any other safety requirements as established in national laws and regulations."

[14] SECY-13-0029, "History of the Use and Consideration of the Large Release Frequency Metric by the U.S. Nuclear Regulatory Commission," March 22, 2013

Chapter 8 of SSG-2 (Rev. 1) [2] describes the documentation of deterministic safety analyses and their results. The results and findings of a safety analysis are generally documented in some form of safety assessment report, with possibly separate supporting documentation (e.g. the model description, code validation, assumptions for plant state).

8.2. PARTICIPATING TECHNICAL EXPERTS' CONSIDERATIONS

Participating technical experts reported they identified in which documentation the DEC with core melting analysis is presented and that the analysis description and results are part of the power plants' safety analysis report (SAR) or of a similar safety document.

Standard formats of the IAEA and the Nuclear Regulatory Commission are widely applied in the structure of safety analysis reports as reported by participating technical experts . In the standard format of that IAEA for the SAR, the core melting analysis is part of chapter 7. In the standard format of the Nuclear Regulatory Commission for the SAR, deterministic core melting analysis is presented in chapter 19 with the PSA results and other DEC analysis. Participating technical experts from Finland, France, the Russian Federation and the United States of America reported, more detailed supporting documentation (e.g. topical reports) can be submitted as an addition or attachment to the SAR. Participating technical experts from the Russian Federation stated, according to the national standard format for the SAR (NP-006-16 [13]), the results of DEC with core melting analysis are presented in chapter 15 of the SAR.

Some participating technical experts reported, DEC with core melting analysis is not part of the SAR. For example, as reported by participating technical experts from India, DEC with core melting analysis which are relevant to the SAMG have been covered in SAMG technical basis documentation.

This documentation describes the accident analysis made for the facility, while the content depends on the Member States' requirements. It includes calculation methods for the transients and accidents, applied approaches and justification of the assumptions. At a minimum, references to the computer codes used are presented, as well as a description of the code models used.

Most importantly, the analysis results are described in the documentation where the safety of the plant, management of the core melt scenario and minimization of the consequences are presented. Accident analysis results are also provided as an accident progression specification and the transient state of the unit. Analyses are also used to assess the technical solutions in the design of DEC with core melting safety features and to confirm that they are operating as expected, so documentation of the analysis can include descriptions of the systems relating to the accident scenario.

As reported by participating technical experts the detail of the SAR is country-specific and follows national regulations. Many Member States (e.g. Finland, France, and the Russian Federation) have established a requirement that the analyses of the safety analysis report describe the plant to a level of detail such as it is possible to facilitate independent confirmatory analyses or verify the analyses by other means.

Many participating technical experts reported, SAR or similar documentation include the source term or dose rate analysis of DEC with core melting accident. Many participating technical experts stated the evaluation of radiological consequences of DEC with core melting accident is required for the assessment of the regulatory body.

9. CONCLUSIONS AND SUMMARY

Based on the responses of the participating technical experts and the presentations made by them during the technical meeting, summarized in Sections 2–8 and detailed in the annexes, it can be concluded that DEC with core melting are postulated for defence in depth purposes and that their analysis is required as part of the safety demonstration, generally following a best estimate approach in analysing DEC with core melting. This important conclusion holds in spite of differences in the terminology (e.g. design extension conditions vs. beyond design basis accidents) and details of the approaches.

However, more or less significant differences, presented in Sections 28, can be noted and are summarized in this section.

9.1. OBJECTIVES OF DEC WITH CORE MELTING ANALYSIS

Most participating technical experts reported, DEC with core melting are postulated for defence in depth purposes and dedicated safety features are designed to meet the associated safety criteria. The analysis of DEC with core melting aims at confirming that the safety features, credited in the safety demonstration for the considered DEC scenarios, perform in such a manner as to meet the relevant safety requirements or safety goals.

Additionally, the results of the deterministic safety analysis for DEC with core melting could be used as follows:

(a) To support PSA, demonstrating whether or not the probabilistic safety goals are met;

(b) To provide an estimate of source terms and assist in defining emergency arrangements;

(c) To support the development and validation of SAMG;

(d) To support equipment safety requirements (e.g. safety classification, operational limits and conditions).

Some participating technical experts declared using DEC with core melting analysis as an input to the qualification or the survivability of the equipment necessary to cope with those DEC, for the resulting environmental conditions such as temperature, pressure, humidity and radiation levels.

9.2. IDENTIFICATION AND DEFINITION OF REPRESENTATIVE SETS OF SEQUENCES FOR DEC WITH CORE MELTING

There is a variety of approaches as reported by the participating technical experts to develop representative sets of DEC with core melting from simple postulation of a DEC list to a systematic approach. Participating technical experts reported they consider the following aspects when forming sets of DEC with core melting:

(a) National and international operating experience feedback;

(b) Engineering judgement;

(c) Results of deterministic analyses;

(d) Results of Level 1 PSA and Level 2 PSA.

Development of the sets of DEC with core melting could be based on the consideration of combination of the aspects mentioned in the above list or could rely on a few of them as applicable. Some participating technical experts stated, the generic list of DEC with core melting is developed by the vendor or established in the regulations, and then used as a basis for the development of a plant specific list of DEC with core melting. PSA is often used for systematic identification of event sequences leading to challenges to the fundamental safety functions, while in general engineering judgment and operating experience feedback are used to prove the completeness and representativeness of DEC with core melting.

9.3. REPRESENTATION OF THE PLANT

Most participating technical experts reported, a realistic representation of the plant, which depends on the objectives of the numerical simulation, is defined and applied when analysing DEC with core melting. This representation is as close to the actual plant as practicable to ensure correct accident progression simulation, enable correct modelling of the expected physical phenomena, and achieve accurate results of the accident analysis.

9.4. INITIAL AND BOUNDARY CONDITIONS

The participating technical experts reported, initial conditions are chosen with a realistic or a conservative manner. Many participating technical experts reported, best estimate methods for determining initial conditions are applied, while conservative assumptions for parameters of major influence appear to be applied by others.

The boundary conditions for the analysis can be modelled through system performance, e.g. the assumption of how the credited safety features operate in the analysed scenario. Many participating technical experts reported, system performance is modelled realistically, according to the design parameters (i.e. nominal as designed), while an added conservatism to cover possible uncertainties is considered by others.

9.5. OPERATOR ACTIONS

Most participating technical experts reported, the operator actions are considered on a best estimate basis consistent with SAMG. Action times may account for harsh environmental conditions (e.g. high radiation levels, extreme temperature) and possible delays due to infrastructure damage.

9.6. UNCERTAINTY ANALYSIS AND SENSITIVITY STUDIES

There is a common understanding among participating technical experts that epistemic uncertainties in the analytical prediction of challenges to fission product barriers need to be taken into account if the level of knowledge of important severe accident phenomena and physical processes is limited or if the associated supporting experimental data are insufficient.

Many participating technical experts recognized that the uncertainties in the phenomena involved in DEC with core melting, particularly in their late phase, are so large that fully implementing a best estimate plus uncertainty method (BEPU) is difficult to achieve (e.g. determination of the distribution of the relevant uncertain parameters), although some

initiatives are being undertaken by the IAEA and the European Commission (EC) to explore the extension of these methodologies to DEC with core melting. Sensitivity studies are still deemed to be more appropriate than uncertainty analyses to demonstrate the robustness of the results and the conclusions of DEC with core melting analysis. However, quantification of uncertainties appears to be required or expected in some Member States, as reported by participating technical experts.

9.7. AVAILABILITY OF AND CREDITING EQUIPMENT

Participating technical experts' positions differ, more or less, on the systems that can be used to bring the plant to and maintain it in a safe state in terms of independence, qualification and use of non-permanent equipment.

All participating technical experts reported, the availability of equipment, including I&C, credited in the safety demonstration of DEC with core melting needs to be justified. Availability of systems and components is assumed if their failure is not part of or consequent to the accident sequence and their operation under severe accident environment is demonstrated. Several participating technical experts consider that deterministic analysis of DEC with core melting may use applicable inputs from PSAs and may credit all the available SSCs, provided it has been demonstrated, with reasonable confidence, that they are able to perform their intended function in DEC with core melting. However, some other participating technical experts reported they require that only those safety features designed and qualified for DEC with core melting can be credited in the safety demonstration.

Many participating technical experts reported, systems credited in DEC with core melting are required to be independent (physically and functionally separate) from all other systems as far as practicable; in particular, safety systems credited for DBA are not used for DEC with core melting.

All participating technical experts consider the environmental conditions of the accident as limiting the ability to credit a system: if a system cannot withstand the environmental conditions of a core melting scenario, it cannot be credited in the scenario analysis.

With respect to the use of non-permanent equipment, some participating technical experts reported they credit non-permanent equipment in DEC with core melting. However, this has to be realistically justified in terms of bringing the equipment to the site and the time needed to connect it to the facility and supporting systems, with consideration of possible harsh conditions. Some participating technical experts stated they credit on-site non-permanent equipment, but not off-site non-permanent equipment. Many participating technical experts reported all non-permanent equipment can be used to manage DEC with core melting although in a few of them, such equipment cannot be credited as part of the formal DEC with core melting safety demonstration but is only introduced in robustness studies for extremely unlikely events.

9.8. APPLICATION OF THE SINGLE FAILURE CRITERION

Most participating technical experts reported, the single-failure criterion, which does apply to all safety groups credited in the DBAs, does not have to apply to DEC with core melting analysis. The application of single failure criterion to active components of safety features for DEC with core melting appears to be required only in Finland.

9.9. DEFINITION AND CONSIDERATION OF A SAFE STATE

Participating technical experts use different wordings such as ‘safe state’, ‘safe shutdown state’, ‘controlled safe state’, ‘severe accident safe state’ or ‘long-term safe stable state’ to describe the ultimate acceptable condition of a nuclear power plant following a DEC with core melting situation. In general, participating technical experts reported they require that in DEC with core melting analysis, it has to be shown that a safe state is reached and maintained for a long time. No distinction is made between a safe state with the melt retained in the reactor vessel and a safe state in which the melt is stabilized and cooled outside the reactor vessel.

Consistent with the IAEA safety standards, an acceptable safe state is usually defined as a plant state in which the fundamental safety functions are ensured for a long time. However, most participating technical experts stated they prefer to define the safety functions as being reactivity control to ensure subcriticality, cooling and confinement such that radioactive releases are limited by focusing on practical parameters (e.g. temperature and pressure in the containment). Some participating technical experts specify that the safe state is not reached until there are means to maintain these safety functions for a long time, but most participating technical experts are silent on the expected future performance of the safety functions.

Some participating technical experts note that because fuel melting in the spent fuel pool has to be practically eliminated, there is no need to define a safe state for DEC with fuel melting in the spent fuel pool. However, other participating technical experts reported, licensees need to demonstrate the capability to prevent or to mitigate spent fuel pool severe accidents in case they happen, and to assess their radiological consequences.

As it is difficult to practically monitor or assess the local corium subcriticality during the degradation of corium in the reactor vessel or when relocating outside of the reactor vessel, it would be difficult to demonstrate that subcriticality of the corium is ensured. Therefore, some participating technical experts reported, which deepened the reflection on the safe state following a DEC with core melting, it is assumed that the subcriticality may be temporary lost, provided that this does not jeopardize residual heat removal. Similarly, the residual heat may temporarily not be removed if this does not jeopardize the control of the confinement of radiological substances.

9.10. COMPUTER CODES USED FOR DEC WITH CORE MELTING ANALYSIS

As reported by participating technical experts, computer codes are widely used by the licensees to support the safety assessment of their nuclear power plants; they are also used by some Member States regulatory bodies that run, as deemed necessary, independent confirmatory analyses for selected specific accident sequences to evaluate safety analysis results for the specific applications and/or confirm the validation of the tools.

For both deterministic and probabilistic safety analyses for DEC with core melting, the computer tool applicability needs to be appropriate and adequate for the purpose of the analyses. This includes verification and validation of the tools as well as user qualification to prepare and

run the numerical simulations and correctly interpret their results. In general, participating technical experts reported they consider that well established severe accident computer codes, such as ASTEC, MAAP, MELCOR, SAMPSON and SOCRAT, may be applied for DEC with core melting analysis within their domain of validity defined as part of the verification and validation process, but engineering judgement remains necessary to assess and interpret the results.

With respect to the process of computer code certification and as reported by participating technical experts from the Russian Federation, it appears that only the Russian Federation certifies the computer codes used for DEC with core melting analysis for a given period of time. Whether the codes are certified or not, they need to be verified and validated, although some participating technical experts reported they do not formally require validation, but it is expected that the applicant will use well-established, verified and validated computer codes.

For the verification of the tools used for the analysis of DEC with core melting, as a part of quality assurance, most participating technical experts reported they consider that the tools need to undergo an extensive review by the tool developer or user that is equivalent to the verification of the tools used for DBA analysis.

Validation of computer codes is considered a continuous process and significant progress in this area can be expected in the future. This validation process would follow the same process as for the validation of the tools used for DBA. Yet, for some participating technical experts, the application of the validation process of computer tools used for DEC with core melting may be relaxed in view of the experimental data available. To overcome the limitations of experimental data, some participating technical experts reported they are conducting R&D severe accidents programmes to improve severe accident phenomena modelling and to upgrade the validation level and application domain of their tools. This experimental validation is complemented by code-to-code comparison and crosswalk analyses are performed to help understand the analysis of the Three Mile Island accident and the Fukushima Daiichi nuclear accident.

9.11. ACCEPTANCE CRITERIA

Generally, participating technical experts require that accident conditions that could lead to early or large radioactive releases be practically eliminated although the terminology of practical elimination is not explicitly used. For the accident conditions involving core melting that are not practically eliminated, there is a general agreement that they need to be studied as part of DEC with core melting to demonstrate that there is only a limited impact on people and environment. Similarly to the IAEA safety standards, some participating technical experts reported they allow the use of protective measures that are of limited scope in terms of area and time, provided sufficient time is available to implement these measures.

Many participating technical experts further quantify the requirement for practical elimination of accident conditions that could lead to early or large radioactive releases using numerical safety criteria for small and/or large release frequency. Performance goals for containment include a conditional containment failure probability (given core damage) of less than 0.1 or a requirement that loss of containment function in the early phase of the severe accident is only a small contributor to the reactor core damage frequency. Similarly, other participating technical experts reported they specify that containment leaktightness be ensured for a time period sufficient to implement off-site emergency procedures and prevent uncontrolled releases after this period.

9.12. DOCUMENTATION OF DEC WITH CORE MELTING ANALYSIS

In general, the analysis description and results are part of the nuclear power plants safety analysis report (SAR) or similar safety documentation. As reported by many participating technical experts, SAR or similar documents include also the source term or dose rate analysis of the DEC with core melting accident as the evaluation of radiological consequences is required for regulatory review and assessment.

The level of detail in the SAR is country-specific and follows national regulations. Many participating technical experts stated their country has established a requirement that the analyses of the safety analysis report describe the nuclear power plant to a level of detail such that it is possible to facilitate independent confirmatory analyses or to verify the analyses by other means.

For each of the topics mentioned above, relevant IAEA references, including safety standards, safety reports and TECDOCs have been indicated in this publication. While the list of requirements and recommendations is not intended to be comprehensive, it can however help estimate how close to or how far from these references the approach considered for a specific participating technical experts is.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, VIENNA (2016).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2 (Rev. 1), IAEA, VIENNA (2019).

[3] 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).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: 2018 Edition, IAEA, VIENNA (2019).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR PART 4 (Rev. 1), IAEA, VIENNA (2016).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants, IAEA Safety Reports Series No. 56, IAEA, VIENNA (2008).

[7] CSA GROUP, QUALITY ASSURANCE OF ANALYTICAL, SCIENTIFIC, AND DESIGN COMPUTER PROGRAMS, N286.7-16 (2016).

[8] ORDER OF 7 FEBRUARY 2012 SPECIFYING THE GENERAL RULES RELATED TO THE NUCLEAR INSTALLATIONS AND PUBLISHED IN THE FRENCH OFFICIAL GAZETTE ON 8 FEBRUARY 2012, HTTP://WWW.LEGIFRANCE.GOUV.FR/AFFICHTEXTE.DO?CIDTEXTE=JORFTEXT000025338573&DATETEXTE=20160205

[9] STUK GUIDE YVL B.1 SAFETY DESIGN OF A NUCLEAR POWER PLANT OF 15 NOVEMBER 2013. ISBN 978-952-309-047-7 (PDF), FIRST EDITION, HELSINKI 2014.

[10] RB-180-15 REGULATIONS FOR CONTROL OF METAL OF EQUIPMENT AND PIPELINES OF NUCLEAR POWER INSTALLATIONS AT MANUFACTURE AND ASSEMBLY

[11] NUCLEAR REGULATORY COMMISSION, PROBABILISTIC RISK ASSESSMENT AND SEVERE ACCIDENT EVALUATION FOR NEW REACTORS, NUREG-0800, WASHINGTON DC, USA (2015)

[12] NUCLEAR REGULATORY COMMISSION, ANALYSIS OF IN-VESSEL RETENTION AND EX-VESSEL FUEL COOLANT INTERACTION FOR AP1000, NUREG/CR-6849, WASHINGTON DC, USA (2004).

[13] SCIENTIFIC AND TECHNICAL CENTER FOR NUCLEAR AND RADIATION SAFETY, REQUIREMENTS TO THE CONTENT OF SAFETY ANALYSIS REPORT OF POWER UNIT VVER REACTOR TYPE, NP-006-16, MOSCOW (2017).

[14] SCIENTIFIC AND TECHNICAL CENTER FOR NUCLEAR AND RADIATION SAFETY, RECOMMENDATIONS ON THE DEVELOPMENT OF A FINAL LIST OF BEYOND DESIGN BASIS ACCIDENTS TO BE TAKEN INTO ACCOUNT IN THE DESIGN OF NUCLEAR POWER PLANTS WITH VVER-TYPE REACTORS, RB-150-18, MOSCOW (2018).

ANNEX I. QUESTIONNAIRE

The purpose of the questionnaire presented in this annex was to elicit and characterize the international state of practice with respect to approaches used by Member States with active nuclear power programme to analyse design extension conditions (DEC) or similar conditions[1] taken into account at the design stage for nuclear facility[2] conditions more severe than those considered for design basis accidents. It is expected that the answers to this questionnaire presented in this TECDOC will contribute to an enhanced and common understanding of how DEC are defined, identified and analysed. The responders were requested to provide the technical rationale behind each answer as far as possible.

Annexes II–VII present the answers provided by representatives from Canada, Finland, France, India, the Islamic Republic of Iran, the Russian Federation and the United States of America to the questionnaire that was distributed before and during the Technical Meeting on Current Approaches in Member States for the Analysis of Design Extension Conditions for New Nuclear Power Plants that was organized by the IAEA on 19–23 March 2018. Answers are numbered according to the questions, i.e. answer *n* corresponds to question *n*.

[1] In this questionnaire, the term 'design extension conditions' is used as defined in SSR-2/1 (Rev. 1) (2016) or to describe similar conditions taken into account at the design stage to address facility conditions more severe than those considered for design basis accidents.

[2] In this questionnaire, 'facility' refers to the reactor or the spent fuel pool.

Question 1:

Background

According to IAEA Safety Standards Series No. SSR-2/1 (Rev. 1) [I-1], Safety of Nuclear Power Plants: Design, design extension conditions (DEC) are "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". In addition, SSR-2/1 (Rev. 1) [I-1] requires that: "these design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences". In a nuclear power plant, DEC may be defined for the reactor and for the spent fuel pool and are design dependent. In the IAEA approach, only DEC without significant fuel degradation are considered for spent fuel pools while those with fuel melting are practically eliminated.

Question

How do you define DEC or similar conditions taken into account at the design stage for facility conditions more severe than those considered for design basis accident (DBAs)?

- Elaborate on consideration of conditions generated by internal hazards or external hazards, or their combination, as possible DEC or similar conditions.
- Please refer to the regulatory documents, standards or guidelines you use to define these conditions.

Question 2:

Background

In general, the objectives of DEC analysis are used:

- To confirm that features, credited for the design extension conditions, have the requested performances to meet the relevant safety requirements;
- To assist in establishing and validating emergency operating procedures and accident management guidelines;
- To provide the environmental conditions to which systems called in DEC have to be qualified. The DEC analysis may also help in structures, systems and components (SSCs) safety classification as appropriate, and in providing inputs for off-site emergency planning.

Question

- What are the objectives of DEC analysis?

Question 3:

Background

SSR-2/1 (Rev.1) [I-1] states that: "A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures."

Question

Elaborate on DEC identification and classification.

— Elaborate on the role of PSA & DSA in identification and definition of DEC.
— Elaborate on the criteria taken into account to classify DEC in DEC without significant fuel degradation and DEC with core melting

Question 4:

Background

To describe acceptable facility conditions after a transient or an accident, in the IAEA Safety Glossary (2018 Edition) [I-2], controlled state is defined as "a plant state following an anticipated operational occurrence or accident conditions, in which fulfilment of the main safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state."

And safe state is defined as "a plant state following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the main safety functions can be ensured and maintained stable for a long time."

Question

In your national approach, do you have similar definitions for controlled state and safe state following DEC? If yes, please elaborate on those definitions considering both types of DEC (DEC without significant fuel degradation, and DEC with core melting).

Question 5:

Background

SSR-2/1 (Rev. 1) [I-1] states that DEC analysis "could be performed by means of the best estimate approach". This means that the analysis could be performed as "realistically as possible" according to the state-of-the-art knowledge; this applies to the computer codes used, boundary and initial conditions, and the availability of the systems and operator actions.

Question

Elaborate on the best estimate approach.

— How do you define a best estimate approach and what level of confidence do you

assume in using it?
— Elaborate on the use of the best estimate approach for identification and definition of DEC, and their analysis.
— How uncertainty evaluations and sensitivity evaluations are considered in your approach?
— Elaborate on cliff edge effect assessment and safety margins as considered in your approach for DEC consideration (identification and analysis).

Question 6:

Background

Section 5 of the SSG-2 (Rev. 1) [I-3] describes the use of computer codes for deterministic safety analysis. In summary: for the analysis results to be reliable, the selected code needs to be justified for its intended purpose, code verification needs to be done to ensure the implemented models are done correctly and code validation is to be done to ensure the implemented models accurately describe the real modelled system.

Question

With this in mind, are there any special considerations in your national approach for:

— The analysis tool selection;
— Code applicability;
— Code verification and validation, when the tool is used for design extension conditions without significant fuel degradation and/or with core melting?

Question 7:

Background

SSR-2/1 (Rev. 1) [I-1] requires that "An analysis of design extension conditions for the plant shall be performed" with a footnote clarifying that "This analysis of DECs could be performed by means of a best estimate approach. (Nevertheless, more stringent approaches may be used according to States' requirements)."

So, analysis and assumptions used may be different in different technical experts. The following question concerns the different assumptions used in DEC analysis. Information is needed about rules and assumptions as detailed below. In particular, justification of reaching and maintaining a controlled state or a safe state for a long time is requested.

Question

Elaborate on the assumptions used for DEC analysis, including the following:

- Facility representation and modelling;
- Initial and boundary conditions;
- Considerations on uncertainty and sensitivity as applicable;
- Availability of systems and components;
- Systems credited in the analysis (use of safety features and other systems);
- Operator actions (time and action);
- Equipment qualification;
- Operator action in a harsh environment;
- Analysis of end-state.

Question 8:

Background

A set of applicable criteria need to be identified, including any regulatory requirements. Paragraph 5.31.A of SSR-2/1 (Rev. 1) [I-1] requires that: "The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures." More specific technical criteria may be derived from this high level requirement and expressed as qualitative or quantitative acceptance criteria.

Question

Elaborate on the following acceptance criteria:

- Qualitative or quantitative acceptance criteria for DEC without significant fuel degradation;
- Qualitative or quantitative acceptance criteria for DEC with core melting.

Question 9:

Background

Chapter 8 of SSG-2 (Rev. 1) [I-3] describes the documentation of deterministic safety analyses and their results. The results and findings of a safety analysis are generally documented in some form of safety assessment report, with possibly separate supporting documentation (e.g. the model description, code validation, assumptions for plant state).

Question

With this in mind, are there any special considerations in your national approach for the documentation of the analysis of DEC without significant fuel degradation and of DEC with core melting?

Question 10:

Are there any other considerations relevant to DEC or similar conditions taken into account at the design stage for nuclear facility conditions more severe than those considered for DBAs to be added?

Question 11:

Please provide one detailed example of DEC without significant fuel degradation analysis and one detailed example of DEC with core melting analysis illustrating the previous questions (1 to 8) as applicable.

REFERENCES ANNEX I

[I-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, VIENNA (2016).

[I-2] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA SAFETY GLOSSARY: 2018 EDITION, IAEA, VIENNA (2019).

[I-3] INTERNATIONAL ATOMIC ENERGY AGENCY, DETERMINISTIC SAFETY ANALYSIS FOR NUCLEAR POWER PLANTS, IAEA SAFETY STANDARDS SERIES NO. SSG-2 (REV. 1), IAEA, VIENNA (2019).

ANNEX II. ANSWERS TO THE QUESTIONNAIRE PROVIDED BY PARTICIPATING TECHNICAL EXPERTS FROM CANADA

Answer 1

Definition of DEC

In CNSC REGDOC-3.6, Glossary of CNSC Terminology [II-1], DEC is defined as: "design extension conditions (DEC) (conditions additionnelles de dimensionnement (CAD)), a subset of beyond design basis accidents that are considered in the design process of the facility in accordance with best estimate methodology to keep releases of radioactive material within acceptable limits. Design extension conditions could include severe accident conditions. DEC is a plant state."

The definition used by CNSC is based on, and is compatible with, the definition in IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [II-2]. An effectively identical definition is used in Canadian Standard CSA N290.16-16, Requirements for beyond design basis accidents [II-3]

DEC includes accidents involving the reactor core, spent fuel pools and, where appropriate, multiple units at a site. Such accidents could be triggered by multiple failures of equipment, operator errors, internal or external events and, most probably, by a combination of several events.

In the Canadian approach, frequency ranges for anticipated operational occurrences and design basis accidents (DBAs) are given in CNSC REGDOC-2.4.1, Deterministic Safety Analysis, [II-4]. However, CNSC has not defined a lower frequency boundary for DEC. Implicitly, DEC are a selected subset of beyond design basis accidents (BDBAs), and not necessarily a continuous subset from the border of the DBA to a low frequency in the BDBA domain. In this sense, there is no need to define such a 'cut-off' low frequency for DEC. Obtaining credible frequency values for low frequency events, which might include multiple failures of equipment and human errors, is difficult due to the large inherent ambiguities. The approach for identifying events to be considered as DEC inevitably involves a measure of judgement and is characterized by notable uncertainties. For these reasons, the regulatory body does not impose any lower frequency limit for DEC; however, the designer may select sensible values to the convenience of decision making during the design development.

New NPPs

The design would be required to meet CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants [II-5]. REGDOC-2.5.2 is based on SSR-2/1 (Rev. 1) [II-2] and uses the categorization of plant states described there.

The safety analysis would be required to meet CNSC REGDOC-2.4.1, Deterministic Safety Analysis [II-4] and CNSC REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants [II-10].

The requirements do not differentiate between random failures, failures caused by operator errors or failures caused by internal or external hazards.

Existing NPPs

The CANDU® reactor fleet was already in service when the DEC concept was developed, and hence the challenge was to introduce DEC into the existing design framework for the CANDU® fleet. In parallel, there was a pressing need to address the lessons learned from the Fukushima Daiichi accident.

At the design stage of current nuclear power plants (NPPs) in Canada, the concept of DEC was not in use. At the time of first licensing, the designs considered failure of any process system with coincident failure of a protective system. This included all typical DBA equipment failures (such as loss of forced circulation, loss of normal electrical power, loss of primary or secondary coolant) with coincident failure of a protective system (shutdown system, emergency core cooling or containment). Some of these faults would typically now be classified as DEC. The requirements did not differentiate between random failures, failures caused by operator errors or failures caused by internal or external hazards.

To address these issues, the CANDU® industry prepared design guidance for beyond DBA (and DEC) which was later incorporated in the CSA standard N290.16-16, Requirements for beyond design basis accidents [II-3].

CSA N290.16-16 provides specific guidance related to DEC arising from both internal hazards and external hazards. The reference BDBA/DEC for CANDU® stations is the extended loss of all AC power (ELAP), based on the World Association of Nuclear Operators (WANO) document SOER 2013-2-Rev. 1, Post-Fukushima Daiichi Nuclear Accident Lessons Learned [II-6] and the earlier SOER 2011-3 Fukushima Daiichi Nuclear Station Spent Fuel Pool/Pond Loss of Cooling and Makeup [II-7]. Under the ELAP accident scenario, all engineered electrical power supplies (except for station batteries) are assumed to fail and be unavailable. The ELAP event sequence is the basis for both events without significant fuel degradation and for events with significant fuel degradation.

For CANDU® stations, there are no credible event sequences which lead to fuel degradation in the spent fuel pool.

For a periodic safety review, or an integrated safety review in support of refurbishment for life extension, licensees of existing NPPs are required to perform a review against modern standards and identify practicable safety enhancements to meet the modern standards. See information for new NPPs above for the relevant modern standards. The relevant REGDOCs mentioned above would be among the modern standards used.

Answer 2:

The overall safety objective of safety analysis is to demonstrate the safety of the design. Safety objectives for new reactors are stated in section 4 of CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants [II-5]. General safety objectives, technical safety objectives and qualitative safety objectives are given hierarchically. These safety objectives apply to an NPP during operation or during an accident, and the DEC plant state is included as a subset of BDBA.

Dose limits are set for anticipated operational occurrences and DBA and safety goals for overall nuclear safety (core damage frequency, small release frequency and large release frequency). See response to Question 8 for more detail on safety goals for new reactors.

CNSC REGDOC-2.4.1, Deterministic Safety Analysis [II-4], specifies high level requirements for deterministic safety analysis for anticipated operational occurrences, DBAs and BDBAs. Since DEC is a subset of BDBAs, BDBA analysis requirements given below and taken from CNSC REGDOC-2.4.1 apply to DEC analysis:

> "A safety assessment for BDBAs shall be performed to demonstrate that:
>
> The NPP as designed can meet the requirements for release limits established as the safety goals. A deterministic safety analysis provides consequence data for accident sequences to use in the PSA.
>
> The accident management program and design provisions put in place to handle the accident management needs are effective, taking into account the long-term availability of cooling water, material and power supplies." [II-4].

Clearly, deterministic BDBA analysis is required not only to support the evaluation of safety goals in conjunction with PSA, but also to demonstrate the adequacy of the design provisions and accident management program. Therefore, deterministic safety analysis is also performed to demonstrate that the complementary design features are capable of coping with DEC.

For equipment and instrumentation survivability, CNSC REGDOC-2.5.2 [II-5] requires that equipment and instrumentation credited to operate during DEC be demonstrated, with reasonable confidence, to be capable of performing their intended safety function under the expected environmental conditions.

Answer 3

Identification of postulated initiating events

Quantitative methods are used as well as engineering judgement, as required by Requirement 20 of SSR-2/1 (Rev. 1) [II-2].

Requirements for identification of postulated initiating events are given in CNSC REGDOC-2.4.1 [II-4]. A systematic process of identification is required. The methods need to include quantitative and qualitative methods (e.g. hazard and operability analysis, failure mode and effects analysis, master logic diagrams) and be supported by judgement and cross-checking against postulated initiating events for similar designs.

Identification of DEC may involve a two-step process:

(a) Firstly, the probabilistic safety assessment would help identifying dominant contributors to the overall core damage frequency and large release frequency, as well as event that come close to challenging the core and containment integrity.

(b) Secondly, regardless of the specific scenario, the designer needs to consider the known physical phenomena, which could challenge the fundamental safety functions.

The DEC identified for a plant needs to lead to provisions that not only improve probabilistic safety assessment results, but also tackle plant specific severe accident challenges and strengthen the management of BDBAs including severe accidents.

Categorization of event sequences

Requirements for categorization of events into plant states are given in CNSC REGDOC-2.4.1 [II-4] with the categorization based primarily on frequency of the event sequence. This is compatible with Requirement 13 of SSR-2/1 (Rev. 1) [II-2]:

"Plant states shall be identified and shall be grouped into a limited number of categories primarily on the basis of their frequency of occurrence at the nuclear power plant."

The frequency range for DEC is from below 10^{-5} events per reactor-year to a lower limit that has not been defined numerically (due to the large uncertainties associated with low probability estimates). However, for the DBAs, RECGDOC 2.4.1 [II-4] specifies that this class of events also includes any events that are used as a design basis for a safety system, regardless of whether the estimated frequencies are less than 10^{-5} per reactor year.

There is no requirement for sub-categorization of DEC into DEC without fuel melting and DEC with core melting. Events are categorized primarily by frequency. It is not considered advisable to categorize events on the basis of the event consequences which are an output from analysis, not an input. "Events that do not lead to fuel melting shall not lead to fuel melting" is a circular requirement.

The number of DEC events to be considered in design is expected to be small and to be selected based on judgement, using event frequency, dominant phenomena and event timescales to guide the selection.

As discussed in CSA N290.16-16 [II-3], the CANDU® approach reviewed both DSA and PSA to determine the set of DEC to be considered.

DSA

(a) For the CANDU® reactor designs, it was found that the 'Industry Standard' extended loss of all AC power (ELAP), based on the WANO document SOER 2013-2-Rev. 1 [II-6] and the earlier SOER 2011-3 [II-7], bounded the possible consequences of all DSA event sequences. The ELAP event was used to determine what additional design features would be required. These features address both events without significant fuel degradation and for events with significant fuel degradation.

(b) For the CANDU® fleet's spent fuel pools, there are no credible event sequences which lead to fuel degradation in the spent fuel pool. The additional portable equipment procured for the reactor also provides additional protection for the spent fuel pool.

PSA

The PSA was used to evaluate the station robustness against the full set of internal and external hazards. A subset of review level conditions was identified for further investigation. This resulted in several design modifications to deal with extreme (BDBA) conditions.

Criteria

As far as criteria for differentiating the two event classes (DEC without significant fuel degradation and DEC with core melting), the CANDU® fleet's PSA and DSA evaluate the potential for fuel and core damage and hence are sufficient for this purpose.

Answer 4:

Canadian regulatory documents do not formally define 'safe state' or 'controlled state'. The term 'stable state' is used with an implied meaning like the definition for 'safe state' given above. However, domestic CANDU® fleet complies with the direction of the CNSC in this area, which is aligned with the IAEA direction (above). The recently issued CNSC REGDOC-3.6 Glossary of CNSC Terminology [II-1], defines the safe shutdown state as follows:

"A state in which a facility is not operational and the fundamental safety functions can be ensured and maintained stable for a long time. For nuclear reactors, a safe shutdown state is characterized by reactor subcriticality and the presence of core cooling. For all facilities, radioactive discharges are within limits, and the integrity of the barriers to releases is maintained."

CNSC REGDOC-2.4.1 [II-4] states that: "The duration of the transients considered in the analysis should be sufficient to determine the event consequences. Therefore, the calculations for plant transients are extended beyond the point where the NPP has been brought to shutdown and stable core cooling, as established by some identified means (i.e. to the point where a long-term stable state has been reached and is expected to remain as long as required). The analysis should take into account the capacity and limitations of long-term makeup water and electrical power supplies."

For BDBA, CANDU®'s existing design features and additional complementary design features (referred to as emergency mitigating equipment at CANDU® stations) are sufficient to ensure with high confidence that DEC are terminated and that the safe shutdown state is achieved to avoid fuel damage.

In the event that barriers to release are compromised (i.e. for DEC involving fuel degradation) the potential for, and severity of, releases are minimized through the deployment of emergency mitigating equipment and application of severe accident management (SAM) strategies.

Answer 5:

Definitions (from CNSC REGDOC-3.6, Glossary of CNSC Terminology) [II-1]:

best estimate (meilleure estimation)

With respect to safety analysis, an unbiased estimate obtained by using a mathematical model, calculation method or data to realistically predict behaviour and important parameters.

best estimate method (méthode de la meilleure estimation) A method designed to give realistic results.

Use of Best Estimate Approach

Use of a best estimate approach is specifically allowed for design and analysis of DEC. CNSC REGDOC-2.4.1 [II-4] states that: "For the analysis of a BDBA, it is acceptable to use a more realistic analysis methodology consisting of assumptions that reflect the likely plant configuration, and the expected response of plant systems and operators in the analysed accident." A required confidence level is not specified.

One of the reasons for using best estimate methods and computer codes in DEC analysis is related to accident management. As the accident progresses to the conditions beyond the design basis, accident management actions become an important part of defence in depth. It is desired that the consequences of DEC are estimated so that the analysis results reflect a realistic plant response and provide best estimate information for accident management.

Deterministic analysis needs to be performed for an event leading to the highest challenge (e.g. the largest hydrogen source term) to ensure that the complementary design features are capable of coping with the DEC. In this case, it needs to be demonstrated that the hydrogen mitigation measures (e.g. passive autocatalytic recombiners and/or igniters) are able to function under DEC to prevent the potential challenge to the integrity of the containment due to the most challenging hydrogen burn modes.

Analysis of DEC may use applicable[1] input from PSAs and may credit all the available SSCs, as long as it has been demonstrated with reasonably high confidence that they are able to perform their intended function in DEC. It is worth noting that the single failure criterion, which applies to all safety groups credited in the DBA analysis, does not have to apply in DEC analysis.

Uncertainty and sensitivities

Full uncertainty evaluation is not required for DEC. Sensitivity studies may be used to assess the effects of major uncertainties in the calculations or to search for cliff edge effects.

Cliff edge effects and safety margins

Cliff edge effects are assessed by means of sensitivity calculations.

The term 'safety margin' is not defined numerically. Judgement is used to determine if there is sufficient safety margin. For DEC, the principle is that there need to be 'reasonable confidence' that acceptance criteria are met.

Overview for the existing CANDU® fleet

The CANDU® fleet's guidance to applying the best-estimate approach to BDBA and DEC is described in COG guidance, [II-9]. This is consistent with CSA N290.16-16 [II-3] in this area (and which reflects IAEA publications in this area).

CSA N290.16-16 [II-3] provides general guidance to using best estimate as it relates to the

[1] Applicability is shown by demonstrating that the assumptions, models, rules, etc. used for generation of the information in the PSA are compatible with the use of that data.

modifications for DEC. Application of this guidance to the design of emergency mitigating equipment is given in utility documents.

In terms of the specific application of best estimate to the 'reference BDBA/DEC', the extended loss of all AC power event, the CANDU® fleet adopted the industry guidance provided by WANO in SOER 2013-2 Rev. 1 [II-6] and the earlier SOER 2011-3 [II-7].

The application of uncertainties will depend on the type of equipment being considered: For existing (design basis) equipment, uncertainties will be treated in the normal manner, using the standard DBA approach. For other (BDBA) equipment, the application may be adjusted as described in CSA N290.16-16 [II-3]. However, under no circumstances, BDBA equipment need to compromise normal plant operation or to response to DBA.

Sensitivity assessments are performed as required to ensure the DEC analyses objectives are met (see Question 2).

The CANDU® fleet's analyses looked for indications of cliff edge effects, particularly for severe weather and flooding hazards, and design improvements were implemented as required.

Answer 6:

There are no separate requirements for DEC in these areas. For DEC, the principle is that there need to be 'reasonable confidence' in the analysis results detailed below. This implies that the requirements for verification and validation are not as rigorous as for DBA analysis.

The CANDU® fleet's use and selection of analytical tools already consider limits of applicability, suitability for purpose and the adequacy of verification and validation. These are given in CSA standard N286.7-16, Quality assurance of analytical, scientific, and design computer programs, [II-8] and the corresponding utility documentation in this area.

In the case of DSA for DEC, the existing suite of software tools was found to be adequate for the required analyses of both design extension conditions without significant fuel degradation and/or with core melting.

In the case of PSA studies of BDBA and DEC, the existing suite of software tools was found to be adequate for the required analyses of both design extension conditions without significant fuel degradation and/or with core melting.

DETAILED CONSIDERATIONS ON THE 'REASONABLE CONFIDENCE' CONCEPT

In accordance with Canadian requirements for design and analysis, such as REGDOC-2.5.2, Design of Nuclear Power Plants [II-5], and REGDOC-2.4.1, Deterministic Safety Analysis [II-4], a lower level of confidence is accepted for DEC than for DBA. These Canadian documents are based on SSR-2/1 (Rev. 1) [II-2] and SSG-2 [II-11] respectively which also differentiate between conservative design and analysis rules for DBA and best estimate or realistic assumptions for DEC. Extracts from SSR-2/1 (Rev. 1) [II-2] and SSG-2 [II-11] are given in later answers with examples of application of reasonable confidence highlighted.

Since severe accident management requires a symptom-based approach, to achieve optimal results following actions of the SAM guidelines, it is important to provide the best possible advice to operators who will be managing the accident. A conservative approach is not suitable for SAM since undue conservatism would bias results and could lead to less than optimal advice.

Reasonable confidence is a higher than average expectation (the confidence level is higher than 50%) that SAM action will achieve at least the minimum functionality required for success.

Reasonable confidence can be shown through evaluation of conditions under which the SAM action is to take place and assessing the likelihood of the system or personnel to successfully perform the action while applying a best estimate approach.

CSA N290.16-16, Requirements for beyond design basis accidents, CSA Group, Canada, 2016 defines 'reasonable confidence' as, "In the context of BDBA mitigation, a better than average expectation that the SSC or action will achieve the minimum safety functionality required for success". [II-3]

Note: Reasonable confidence that complementary design features will deliver the required functionality is obtained by the following:

(a) Employing best estimate approach to determine the reactor-specific conditions corresponding to the DEC;

(b) Determining the required functionality for the complementary design features corresponding to the DEC from item a);

(c) Evaluating and confirming the robustness of the complementary design features impact of internal and external hazards and cliff edge effects that could pose functionality challenges for the complementary design features.

In the concept of reasonable confidence the need is recognized for greater reliance on engineering judgement than is usual within the design basis of the NPP. Scientific certainty is hard to achieve and so a much more flexible approach is accepted. This leads inevitably to a lack of clear rules; this can be difficult to interpret. However, given the inherent uncertainties in the DEC domain, particularly for severe accidents, development of rigorous rules is not realistic. With this in mind, safety assessment will be realistic to the extent practicable, rather than conservative.

Several factors are associated with DEC events, such as the following:

(a) Extremely low likelihood of occurrence;

(b) Limited experience base (most reactor designs have never had a severe accident);

(c) Large uncertainties associated with prediction of event progression;

(d) Difficulty obtaining experimental evidence on which to develop and test computer models.

'Reasonable confidence' can be applied in most reactor safety areas, not just design and safety analysis. For example, human factor verification (determination of staff complement or verification of operating procedures) and qualification of equipment for harsh conditions.

EXAMPLES OF APPLICATION OF ‘REASONABLE CONFIDENCE’

General

More use of judgement, less emphasis on rigorous demonstration.

Lower level of conservatism than for DBA.

DEC without significant fuel degradation (DEC-A) may use more conservatism than DEC with core melting (DEC-B) as referred in Canada.

Design and Deterministic Safety Analysis

Use of best estimate safety analysis computer models and assumptions, including reduced requirements for code validation and verification.

Reduced requirements for uncertainty assessment.

Design of DEC equipment does not need to meet single failure criterion and does not need to allow for outage for maintenance and testing.

Use of ‘reasonable confidence’ in determining equipment operability in DEC harsh conditions less rigorous than formal Environmental Qualification.

Emergency Operating Procedures and SAM Guidelines

Use of best estimate analysis results, realistic operator action times and reasonable assumptions on equipment availability.

Human Performance

Use of reasonable confidence in verification of operator procedures.

Answer 7:

The underlying principle is that there need to be ‘reasonable confidence’ in the results of the analysis as summarized in Table II-1.

Table II-1: Summary of the answer related to analysis results

Facility representation and modelling	Best estimate / realistic. The facility representation and modelling assumed in the PSA and in the DSA for DBA are generally best.
Initial and boundary conditions	Best estimate / realistic. Initial plant conditions assumed in the PSA and in the DSA for DBA are modified to be compliant with the best estimate approach. Boundary conditions are not changed significantly.
Considerations on uncertainty and sensitivity as applicable	Sufficient to give reasonable confidence. These best estimate approaches do not always account for modelling uncertainties, but sensitivity assessments are performed as required to ensure the DEC analyses objectives are met (see Question 2).

Availability of systems and components	Best estimate / realistic. For other (BDBA) equipment, the application may be adjusted as discussed in CSA N290.16-16 [II-3]. However, under no circumstances, BDBA equipment need to compromise normal plant operation or to response to DBA.
Systems credited in the analysis (use of safety features and other systems)	Credit for systems is allowed if they are not failed as part of the accident sequence and if there is reasonable confidence that they will function in the accident conditions (equipment survivability, not full equipment qualification)
Operator actions (time and action)	Best estimate / realistic Note that, for DBA, operator actions in the control room are not credited for 30 minutes for new reactors (15 minutes for existing NPPs). The equivalent for field actions is 60 minutes (30 minutes for existing NPPs). There are no equivalent figures defined for DEC. CNSC REGDOC-2.5.2 [II-5] requires that a new NPP need to be capable of meeting safety requirements: a. without the need for operator action to connect temporary onsite services for at least 8 hours; b. without the need for offsite services and support for at least 72 hours. However, these are design requirements. The safety analysis can credit realistic operator action times.
Equipment qualification	Reasonable confidence that equipment will function in the accident conditions (equipment survivability, not full equipment qualification)
Operator action in a harsh environment	Realistic. The timing of required operator actions is determined from the DEC analyses. Important examples include timely load shedding actions (to preserve battery capacity) and restoration of fuel cooling.
Analysis end-state	Up to a predefined long term stable state. CNSC REGDOC-2.4.1 includes, “The duration of the transients considered in the analysis should be sufficient to determine the event consequences. Therefore, the calculations for plant transients are extended beyond the point where the NPP has been brought to shutdown and stable core cooling, as established by some identified means (i.e. to the point where a long-term stable state has been reached and is expected to remain as long as required). The analysis should take into account the

	capacity and limitations of long-term makeup water and electrical power supplies." [II-4]. Note that there is little point continuing detailed thermal-hydraulic analysis for several weeks. Provided subcriticality is ensured and cooling is stable all that is required is to ensure that cooling will not be interrupted. This is not in the scope of safety analysis.

Answer 8:

Canada follows SSR-2/1 (Rev. 1) [II-2] and does not define separate criteria for DEC with significant fuel degradation and DEC with core melting. It is not considered advisable to categorize events based on their calculated consequences. Canada categorizes events based mainly on frequency.

CNSC REGDOC-2.5.2 [II-5] includes: "The design shall be such that plant states that could lead to significant radioactive releases are practically eliminated. For plant states that are not practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures." This is fully compatible with SSR-2/1 (Rev. 1) [II-2].

CNSC REGDOC-2.5.2 [II-5] sets safety goals applicable to events beyond the design basis (including DEC) for new NPPs as follows:

"For practical application, quantitative safety goals have been established, so as to achieve the intent of the qualitative safety goals. The three quantitative safety goals are:

1. core damage frequency
2. small release frequency
3. large release frequency

A core damage accident results from a postulated initiating event (PIE) followed by the failure of one or more safety system(s) or safety support system(s). Core damage frequency is a measure of the plant's accident prevention capabilities.

Small release frequency and large release frequency are measures of the plant's accident mitigation capabilities. They also represent measures of risk to society and to the environment due to the operation of an NPP.

Core damage frequency

The sum of frequencies of all event sequences that can lead to significant core degradation shall be less than 10^{-5} per reactor year.

Small release frequency

The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{15}Bq of iodine-131 shall be less than 10^{-5} per reactor year. A greater release may require temporary evacuation of the local population.

Large release frequency

The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{14}Bq of caesium-137 shall be less than 10^{-6} per reactor year. A greater release may require long-term relocation of the local population."

The additional measures implemented by the CANDU® fleet to address DEC and BDBA are such that the protection of the public is assured.

(a) As an example, a major criterion for successful mitigation of the extended loss of all AC power is deployment of portable pumps and generators to restore fuel cooling and essential electric power within 4-6 hours after the extended loss of all AC power occurs.

(b) In the event that the extended loss of all AC power is not terminated prior to fuel damage occurring, cooling water makeup to the moderator system needs to occur within 12 hours.

Answer 9:

No specific requirements for documentation of DEC analysis have yet been defined in CNSC regulatory documents. The requirements for documentation of DEC analyses are presented in CSA N290.16-16 [II-3]. Station specific documentation provides additional detail. This set of documents (and supporting documents) provides a fulsome description of the safety features required for mitigation of DEC and BDBA.

IAEA SSG-2 [II-11] is, at the time of completion of the questionnaire, undergoing a significant revision and is unlikely to be published before 2018. Following publication, it will take time for the changes to be evaluated and adopted or adapted in Canadian regulatory documents.

Answer 10:

New NPPs

The Canadian regulatory body has not received an application to construct a new NPP since the publication of CNSC REGDOC-2.5.2 [II-5] which includes requirements for DEC. Therefore, these requirements have not yet been fully applied to an NPP at the design stage.

Pre-licensing vendor design reviews have been conducted for modern reactor designs. As part of this process, the design and safety analysis were assessed. However, the analysis submitted by the vendors was not specifically performed to the current requirements of CNSC REGDOCs 2.5.2 [II-5], 2.4.1 [II-4] and 2.4.2 [II-10]. Moreover, the depth of the reviews was significantly less than would be applied to a licence application. However, all designs were found to have no significant impediment to licensing.

Existing NPPs:

The concept of DEC had not been introduced at the time of original licensing of Canadian NPPs. The original licensing included events that would currently be classified as DEC. Additionally, Canadian NPPs have performed integrated safety reviews (similar to periodic safety review) in

support of refurbishment for life extension. This process includes comparison against modern standards.

See response to Q1 for more details.

Canada's responses to questions 1-9 fully describe the current CANDU® fleet's approach to DEC analyses. The main findings of these DEC analyses were that the following:

(a) The provision of temporary and portable equipment (emergency mitigating equipment at CANDU®) is effective and provides the best additional lines of defence for BDBAs and DEC;

(b) Enhanced barriers against external hazards (severe weather, high winds, flooding) are beneficial in reducing public risk and improving overall safety.

Answer 11:

In CANDU® safety analysis, a key measure is to prevent fuel channel failures and thus to maintain a coolable core configuration to remove the decay heat, rather than 'significant fuel degradation'. Events leading to fuel channel failures are referred as to severe core damage, which could include or be equivalent to the 'core melting' concept.

Since the Fukushima Daiichi accident, particular emphasis has been placed on long term failure of all AC power as part of the CNSC Fukushima Action Plan [II-12].

For the CANDU® designs, it has been shown that core melting can be prevented by the action of emergency mitigating equipment (e.g. portable pumps and power supplies). Core melting can be prevented by establishing a heat sink either by providing feed to the boilers or to the calandria vessel. However, if further failures are postulated, then core melting can occur. In-vessel retention can successfully prevent a large release if makeup to the shield tank is established. However, if all attempts to establish a heat sink are assumed to fail, a large release can occur. The release can be mitigated to some extent by emergency filtered containment venting, where installed.

DEC without significant fuel degradation analysis

A typical CANDU® example of DEC leading to fuel damage without channel failure is a loss of coolant accident (LOCA) coincidently combined with a loss of emergency core cooling (LOECC). Such LOCA and/or LOECC events were considered in the original design basis and analysed in the safety report. In terms of frequency of occurrence, these dual-failure events could be classified as BDBAs. Since they were considered in the design, they can be considered as DEC. The LOCA/LOECC scenarios have the following characteristics:

(a) Limited or no water coolant in fuel channels;

(b) Fuel bundles exposed to steam cooling at low pressures;

(c) Significant fuel degradation;

(d) Significant hydrogen production (but within the mitigation capability of passive autocatalytic recombiners);

(e) Core decay heat primarily removed by the moderator water and the moderator cooling system;

(f) Fuel channel integrity remained (no pressure tube and calandria tube failure);

(g) Coolable core geometry remained.

DEC with core melting analysis

In this case, initial attempts to restore fuel cooling to the reactor and essential electric power are assumed to be unsuccessful and some core damage is predicted. In this case, the moderator acts as a heat sink limiting the extent of fuel damage. Containment design features (such as filtered containment venting) and SAM strategies will prevent or limit radiological releases.

An example of DEC leading to severe core damage or core melting is a station blackout leading to loss of all AC powers for an extended period of time. In this case, it is assumed that the multiple provisions (including implementation of emergency mitigating equipment) fail to mitigate the consequences of such an accident. Therefore, station blackout with an unspecified failure of emergency mitigating equipment can be considered as DEC with core melt and has the following characteristics:

(a) Reactor is automatically shut down due to loss of power.

(b) Steam generators are maintained as a heat sink for at least 2 hours (control room operator actions can connect other water sources to steam generators for prolonging this heat sink for another few hours (e.g. 9 hours); this gives sufficient time to deploy emergency mitigating equipment for water makeup to steam generators to maintain the heat sink for a long time).

(c) If steam generators are no long a heat sink, fuel and fuel channel heat up, leading to fuel channel failures and depressurization of the heat transport system and the moderator due to the opening of the calandria pressure relief rupture disks.

(d) Moderator water level starts to drop, leading to further heat up or even melting of the fuel in the uncovered fuel channels (this time, emergency mitigating equipment can be used to add water into the calandria vessel to cool the fuel. If a containment heat sink is available, the accident progress can be stopped).

(e) As noted above, the reference BDBA/DEC for CANDU® stations is the extended loss of all AC power (ELAP), based on the WANO document SOER 2013-2-rev1 [II-6] and the earlier SOER 2011-3 [II-7]. This BDBA/DEC is the basis for both

events without significant fuel degradation and for events with significant fuel degradation. The BDBA/DEC and the mitigating design features are described in CSA N290.16-16 [II-3].

(f) Many BDBA sequences are evaluated in the plant PSAs. These include events that could be considered DEC. For some sequences, mitigation by complementary design features or other emergency mitigating equipment will prevent significant fuel failure. For other sequences, emergency mitigating equipment is assumed to fail, leading to core melting.

(g) Current PSAs show that CANDU® plants can meet safety goals applicable to existing NPPs.

Description of DEC Transients

The examples describe transients at a single CANDU® unit following a total and unrecovered loss of electrical power. The examples cover two end points:

1. Early in-vessel retention, i.e. transient halted just before core collapse (see Part A).
2. Late in-vessel retention, i.e. transient halted just before calandria failure (see Part B).

PART A: SINGLE UNIT BLACKOUT TERMINATED AT EARLY IN-VESSEL RETENTION

Introduction

This example describes the sequence of events following a total loss of AC and DC electrical power at one reactor of a Canadian multi-unit CANDU® nuclear power plant.

The sequence has been halted at early in-vessel retention. That is, it has been assumed that makeup to the calandria tank is initiated just prior to the onset of severe core damage.

Accident description

The postulated accident is initiated by a total and unrecovered loss of AC and DC power at a single reactor. This initiating event results in the immediate failure of key process systems and key mitigating systems in the accident unit. Table A-1 describes the effect of the initiating event upon key systems.

Table A-2 shows key event times in the accident sequence. Sequence details for a range of key systems and parameters are provided in the following sections of this example.

— *Heat Transport System Response and Steam Generator Response*

The initiating event causes the heat transport system (HTS) main circulating pumps and the HTS pressurizing pumps to trip immediately. This results in the automatic trip of the shutdown systems and shutdown of the reactor.

Fuel cooling is initially maintained by forced circulation as the HTS main circulating pumps rundown, and then by thermo-syphoning. Heat is transferred to the steam generators and rejected to the atmosphere through the failed open steam relief valves.

HTS pressure initially falls following the trip of the shutdown systems (Figure A-1).

The initiating event causes the main boiler feedwater system pumps to trip immediately and prevents makeup of the steam generator inventory from either the auxiliary boiler feedwater system or the boiler emergency coolant system. In the absence of makeup, the steam generator level falls as steam is rejected to the atmosphere through the failed open steam relief valves. At about 1.8 hours after accident initiation, the steam generators are empty (Figure A-2).

As the steam generator level falls, the effectiveness of the steam generators as a heat sink degrades. When the steam generators are empty, HTS pressure begins to rise rapidly (Figure A-1). HTS fluid passes through the failed open HTS liquid relief valves to the bleed condenser. At about 3.2 hours after accident initiation, the bleed condenser relief valves open and discharge HTS fluid into the reactor building.

As a result of the loss of HTS inventory through the bleed condenser relief valves, the first fuel channel dries out at about 4.7 hours after accident initiation. Heat-up of the pressure tubes causes them to sag and come into contact with the calandria tubes. Heat is transferred from the fuel through the pressure tubes and calandria tubes into the moderator fluid in the calandria tank.

— *Moderator System Response*

The initiating event causes the main moderator circulating pumps to trip and prevents the auxiliary moderator circulating pumps from starting. This causes the moderator fluid in the calandria tank to swell and pressurize.

When the pressure tubes sag and come into contact with the calandria tubes, heat is transferred from the fuel through the pressure tubes and the calandria tubes into the moderator fluid in the calandria tank. This causes an additional increase in the pressure of the moderator fluid and the calandria tank rupture discs open (Figure A-3).

When the calandria tank rupture discs open, a large mass of moderator fluid is expelled to the reactor building. Channels that are dry on the HTS side and are uncovered in the calandria tank begin to fail.

In early in-vessel retention, it is assumed that makeup to the calandria tank begins just after failure of the first channel and is just sufficient to prevent the failure of additional channels. Makeup is begun at about 5 hours after accident initiation and may be from either permanent systems or from the portable emergency mitigating equipment.

Immediately after initiation of makeup to the calandria tank, the discharge through the calandria tank rupture discs is a two-phase mixture. At about 9 hours after accident initiation, all channels are submerged and the majority of the calandria tank rupture disc flow is in the liquid phase.

— *Containment Response and Fission Product Release*

The initiating event causes the accident unit ventilation system to button-up and the reactor vault air cooling units to trip. Pressure remains slightly above atmospheric until the bleed condenser relief valves open at about 3.2 hours after accident initiation (Figure A-4).

Shortly after the bleed condenser relief valves open, the vacuum building pressure relief valves open, connecting the reactor building to the vacuum building. This draws down reactor building pressure below atmospheric pressure and the vacuum building pressure relief valves reclose.

Shortly after the calandria rupture discs open, at about 4.8 hours after accident initiation, the vacuum building pressure relief valves reopen. This draws down the reactor building pressure below atmospheric pressure and the vacuum building pressure relief valves reclose.

Reactor building pressure slowly rises due to moderator boil-off and containment structural leakage. At about 8.8 hours after accident initiation, the vacuum building pressure relief valves begin to cycle open and closed to maintain reactor building pressure slightly sub-atmospheric. Cycling continues until the vacuum reserve in the vacuum building is exhausted at about 20 hours after accident initiation (Figure A-4).

Following exhaustion of the vacuum reserve in the vacuum building, reactor building pressure rises above atmospheric due to moderator boil-off. Canadian multi-unit nuclear power plants all have a filtered air discharge system. This system can be placed in service when reactor building and vacuum building pressure are close to atmospheric pressure. The filtered air discharge system includes particulate and charcoal filters that remove the majority of the iodine and caesium from airborne releases.

In order to maximize the magnitude of the airborne release, it has been conservatively assumed that the filtered air discharge system is not placed in service.

Airborne releases to the environment occur when the pressure in the reactor building is greater than atmospheric pressure. The majority of the releases occur after the vacuum reserve in the vacuum building is exhausted. Even in the absence of the filtered air discharge system, the magnitude of the activity release is less than the Canadian regulatory threshold for a large release, i.e. 10^{14}Bq of Cs-137.

TABLE A-1 SYSTEM STATUS IN THE ACCIDENT UNIT

System	Status
Primary systems	
Reactor shutdown systems	Successfully trip at the time of the initiating event.
Heat transport system main circulating pumps	Fail at the time of the initiating event.
Heat transport system pressurizing pumps	Fail at the time of the initiating event.
Heat transport system liquid relief valves	Fail open at the time of the initiating event.
Heat transport system loop isolation	Fails open at the time of the initiating event.
Shutdown cooling system	Unavailable from the time of the initiating event.

Emergency coolant injection system	Unavailable from the time of the initiating event.
Moderator circulation and cooling	Fail at the time of the initiating event.
Makeup to the calandria	Initially unavailable. Recovered just after bursting of the calandria rupture discs.
End shield circulation and cooling	Fail at the time of the initiating event.
Secondary systems	
Main boiler feedwater system	Fails at the time of the initiating event.
Auxiliary boiler feedwater system	Unavailable from the time of the initiating event.
Boiler steam relief valves	Instrumented valves fail open at the time of the initiating event.
Boiler emergency cooling system	Unavailable from the time of the initiating event.
Passive Boiler Makeup from the Deaerator Storage Tank	Unavailable from the time of the initiating event.
Support systems	
Instrument air system	Fails at the time of the initiating event.
Low pressure service water system	Fails at the time of the initiating event.
High pressure service water system	Fails at the time of the initiating event.
Emergency service water system	Unavailable from the time of the initiating event.
Containment systems	
Reactor vault air cooling system	Fails in the accident unit at the time of the initiating event.
Ventilation system button-up system	Fails closed at the time of the initiating event.
Vacuum and dousing systems	Available on demand
Emergency filtered air discharge system	Conservatively assumed unavailable.

TABLE A-2 EVENT SEQUENCE TIMING (cont.)

Major events	Timing (hrs)
Shutdown system trip	0.0
Steam generators empty	1.8
Bleed condenser relief valves open	3.2
Vacuum building pressure relief valves open	3.7
First heat transport system channel is dry	4.7
First pressure tube ruptures	4.8
Calandria tank rupture discs open	4.8
Vacuum building pressure relief valves open	4.8
Calandria tank makeup initiated	5.0
Vacuum building pressure relief valves start cycling	8.8
Vacuum building reserve exhausted	20

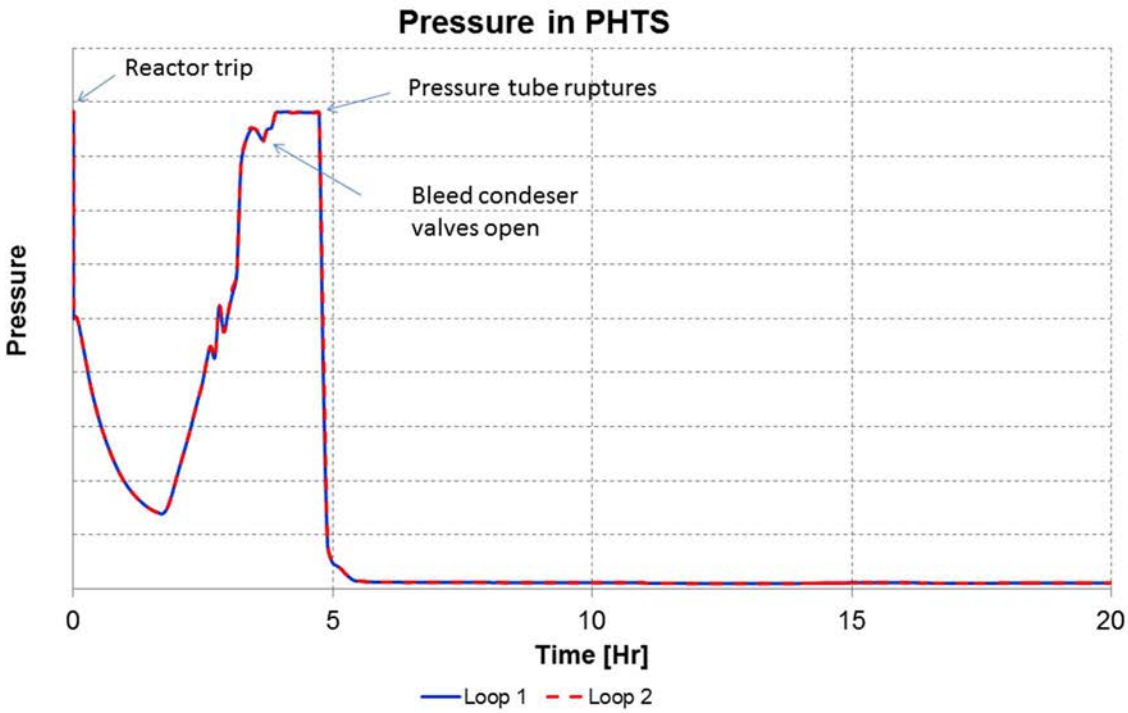

FIG. A-1 Heat transport system pressure response.

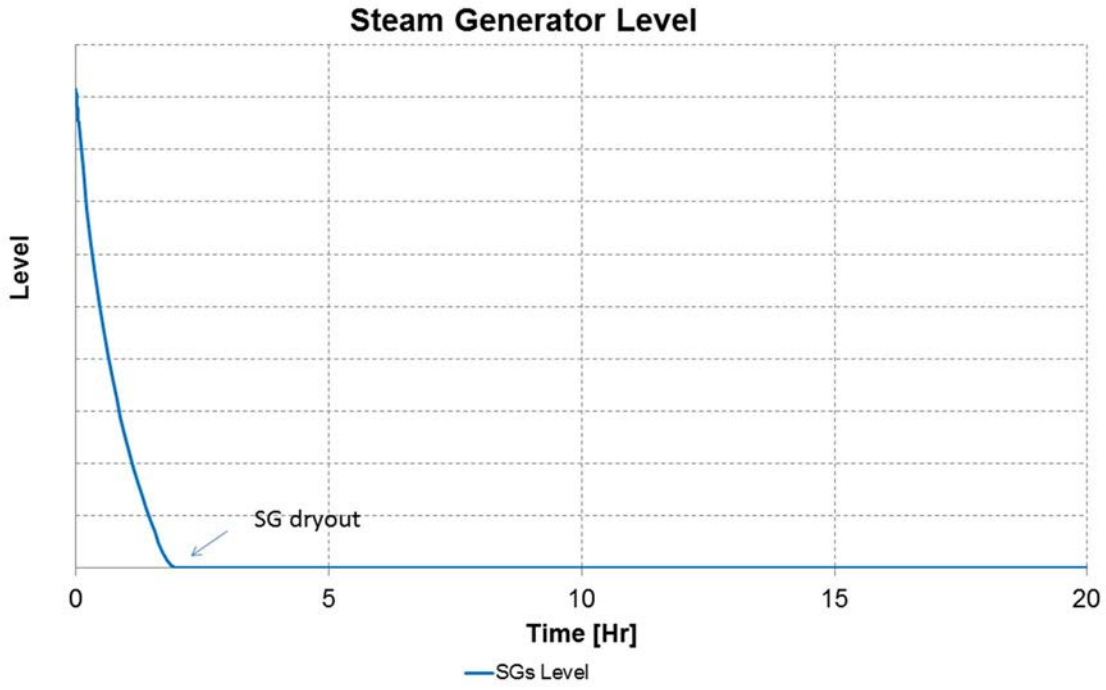

FIG. A-2 Steam Generator Level Response.

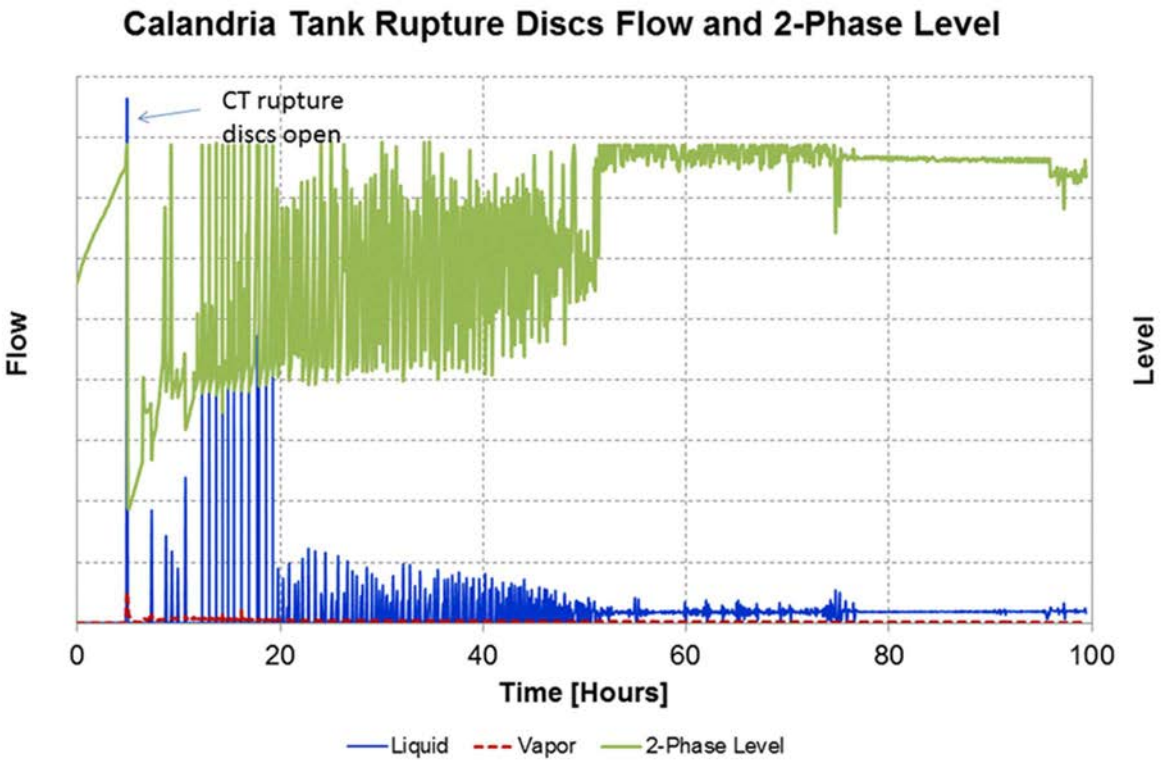

FIG. A-3 Calandria Tank Response.

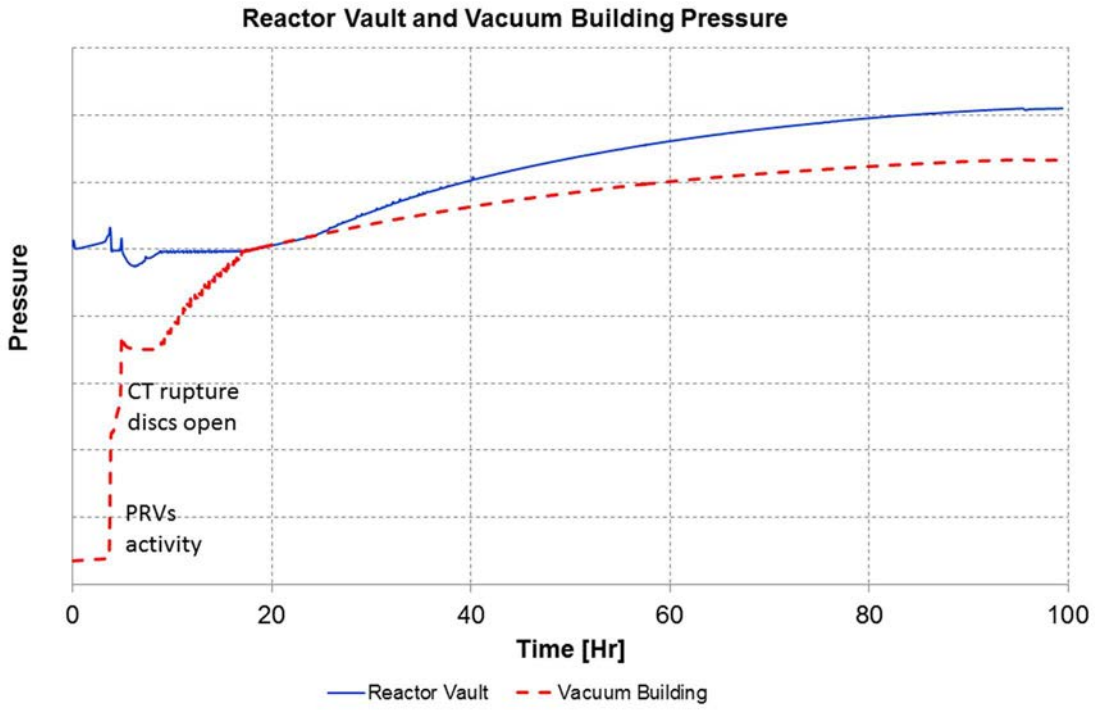

FIG. A-4 Reactor Building and Vacuum Building Pressure Response.

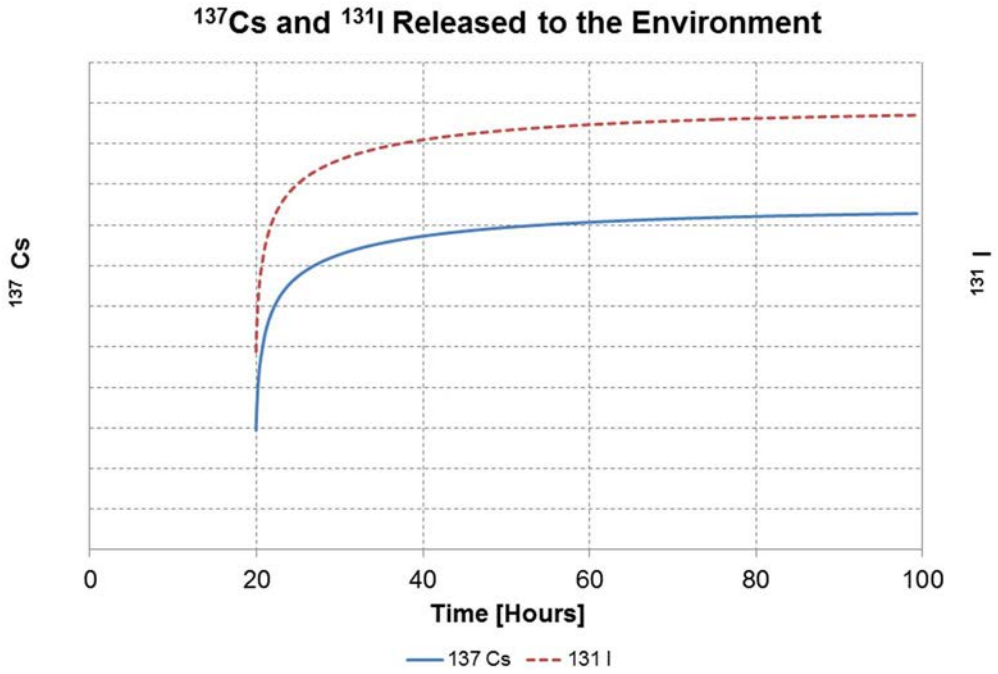

FIG. A-5 Airborne Activity Release to the Environment.

PART B: SINGLE UNIT BLACKOUT TERMINATED AT LATE IN-VESSEL RETENTION

Introduction

This example describes the sequence of events following a total loss of AC and DC electrical power at one reactor of a Canadian multi-unit CANDU® nuclear power plant.

The sequence has been halted at late in-vessel retention. That is, it has been assumed that makeup to the calandria tank is initiated just prior to calandria tank failure.

Accident description

The accident is initiated by a total and unrecovered loss of AC and DC power at a single reactor. This initiating event results in the immediate failure of key process systems and key mitigating systems in the accident unit. Table B-1 describes the effect of the initiating event upon key systems.

Table B-2 shows key event times in the accident sequence. Sequence details for a range of key systems and parameters are provided in the following sections of this example.

— *Heat Transport System Response and Steam Generator Response*

The initiating event causes the heat transport system (HTS) main circulating pumps and the HTS pressurizing pumps to trip immediately. This results in the automatic trip of the shutdown systems and shutdown of the reactor.

Fuel cooling is initially maintained by forced circulation as the HTS main circulating pumps rundown, and then by thermo-syphoning. Heat is transferred to the steam generators and rejected to the atmosphere through the failed open steam relief valves.

Heat transport system pressure initially falls following the trip of the shutdown systems (Figure B-1).

The initiating event causes the main boiler feedwater system pumps to trip immediately and prevents makeup of steam generator inventory from either the auxiliary boiler feedwater system or the boiler emergency coolant system. In the absence of makeup, the steam generator level falls as steam is rejected to atmosphere through the failed open steam relief valves. At about 1.8 hours after accident initiation, the steam generators are empty (Figure B-2).

As the steam generator level falls, the effectiveness of the steam generators as a heat sink degrades. When the steam generators are empty, HTS pressure begins to rise rapidly (Figure B-1). HTS fluid passes through the failed open HTS liquid relief valves to the bleed condenser. At about 3.2 hours after accident initiation, the bleed condenser relief valves open and discharge HTS fluid into the reactor building.

As a result of the loss of HTS inventory through the bleed condenser relief valves, the first channel dries out at about 4.7 hours after accident initiation. Heat-up of the pressure tubes causes them to sag and come into contact with the calandria tubes. Heat is transferred from the fuel through the pressure tubes and calandria tubes into the moderator fluid in the calandria tank.

— *Moderator System Response*

The initiating event causes the main moderator circulating pumps to trip and prevents the auxiliary moderator circulating pumps from starting. This causes the moderator fluid in the calandria tank to swell and pressurize.

When the pressure tubes sag and come into contact with the calandria tubes, heat is transferred from the fuel through the pressure tubes and the calandria tubes into the moderator fluid in the calandria tank. This causes an additional increase in the pressure of the moderator fluid and the calandria tank rupture discs open (see Figure B-3).

When the calandria tank rupture discs open, a large mass of moderator fluid is expelled to the reactor building. Channels that are dry on the HTS side and are uncovered in the calandria tank begin to fail.

As more of the calandria tank inventory boils off, more and more channels heat-up and sag onto the channels below. At about 8 hours after accident initiation, the weight of the suspended debris becomes so large that the core collapses to the bottom of the calandria tank. The core debris is a mixture of solid and molten material.

The remaining inventory in the calandria tank boils off at about 11 hours after accident initiation (Figure B-3). When the calandria inventory is exhausted, the decay heat is transferred through the calandria shell to the end shields and the reactor vault/shield tank.

In late in-vessel retention, it is assumed that makeup to the calandria tank begins after core collapse but just prior to calandria tank failure. Makeup is begun at about 14 hours after accident initiation and may be from permanent systems or from the portable emergency mitigating equipment.

Immediately after initiation of makeup to the calandria tank, the discharge through the calandria tank rupture discs is a two-phase mixture. At about 23 hours after accident initiation, the calandria tank has been refilled and the majority of the calandria tank rupture disc flow is in the liquid phase (Figure B-3).

— *Containment Response and Fission Product Release*

The initiating event causes the accident unit ventilation system to button-up and the reactor vault air cooling units to trip. Pressure remains slightly above atmospheric until the bleed condenser relief valves open at about 3.2 hours after accident initiation (Figure B-4).

Shortly after the bleed condenser relief valves open, the vacuum building pressure relief valves open, connecting the reactor building to the vacuum building. This draws down reactor building pressure below atmospheric pressure and the vacuum building pressure relief valves reclose.

Shortly after the calandria rupture discs open, at about 4.8 hours after accident initiation, the vacuum building pressure relief valves reopen. This draws down reactor building pressure below atmospheric pressure and the vacuum building pressure relief valves reclose.

A third spike in reactor building pressure occurs when the core collapses, at about 8 hours after accident initiation. The vacuum building pressure relief valves reopen, draw down reactor building pressure below atmospheric pressure, and the vacuum building pressure relief valves reclose.

Initiation of makeup the calandria tank at about 14 hours after accident initiation results in a fourth pressure spike in the reactor building. The vacuum building pressure relief valves reopen and draw down reactor building pressure below atmospheric pressure. This fourth pressure spike almost exhausts the vacuum reserve in the vacuum building.

Reactor building pressure slowly rises due to moderator boil-off and containment structural leakage. The vacuum reserve in the vacuum building is exhausted at about 15 hours after accident initiation (Figure B-4).

Following exhaustion of the vacuum reserve in the vacuum building, reactor building pressure rises above atmospheric pressure due to moderator boil-off. Canadian multi-unit nuclear power plants all have a filtered air discharge system. This system can be placed in service when reactor building and vacuum building pressure are close to atmospheric pressure. The filtered air discharge system includes particulate and charcoal filters that remove the majority of the iodine and caesium from airborne releases.

In order to maximize the magnitude of the airborne release, it has been conservatively assumed that the filtered air discharge system is not placed in service.

Airborne releases to the environment occur when the pressure in the reactor building is greater than atmospheric pressure. The majority of the releases occur after the vacuum reserve in the vacuum building is exhausted. Even in the absence of the filtered air discharge system, the magnitude of the activity release is less than the Canadian regulatory threshold for a large release, i.e. 10^{14}Bq of Cs-137.

TABLE B-1 SYSTEM STATUS IN THE ACCIDENT UNIT

System	Status
Primary systems	
Reactor shutdown systems	Successfully trip at the time of the initiating event.
Heat transport system main circulating pumps	Fail at the time of the initiating event.
Heat transport system pressurizing pumps	Fail at the time of the initiating event.
Heat transport system liquid relief valves	Fail open at the time of the initiating event.
Heat transport system loop isolation	Fails open at the time of the initiating event.
Shutdown cooling system	Unavailable from the time of the initiating event.
Emergency coolant injection system	Unavailable from the time of the initiating event.
Moderator circulation and cooling	Fail at the time of the initiating event.
Makeup to the calandria	Initially unavailable. Recovered just prior to calandria tank failure.
End shield circulation and cooling	Fail at the time of the initiating event.
Secondary systems	
Main boiler feedwater system	Fails at the time of the initiating event.
Auxiliary boiler feedwater system	Unavailable from the time of the initiating event.
Boiler steam relief valves	Instrumented valves fail open at the time of the initiating event.
Boiler emergency cooling system	Unavailable from the time of the initiating event.
Passive boiler makeup from the deaerator storage tank	Unavailable from the time of the initiating event.
Support systems	
Instrument air system	Fails at the time of the initiating event.
Low pressure service water system	Fails at the time of the initiating event.
High pressure service water system	Fails at the time of the initiating event.
Emergency service water system	Unavailable from the time of the initiating event.
Containment systems	
Reactor vault air cooling system	Fails in the accident unit at the time of the initiating event.
Ventilation system button-up system	Fails closed at the time of the initiating event.
Vacuum and dousing systems	Available on demand.
Emergency filtered air discharge system	Conservatively assumed unavailable.

TABLE B-2 EVENT SEQUENCE TIMING

Major events	Timing (hrs)
Shutdown system trip	0.0
Steam generators empty	1.8
Bleed condenser relief valves open	3.2
Vacuum building pressure relief valves open	3.7
First heat transport system channel is dry	4.7
First pressure tube ruptures	4.8
Calandria tank rupture discs open	4.8
Vacuum building pressure relief valves open	4.8
Core collapse	8.0
Makeup to calandria tank initiated	14
Vacuum building reserve exhausted	15
Calandria tank refilled	23

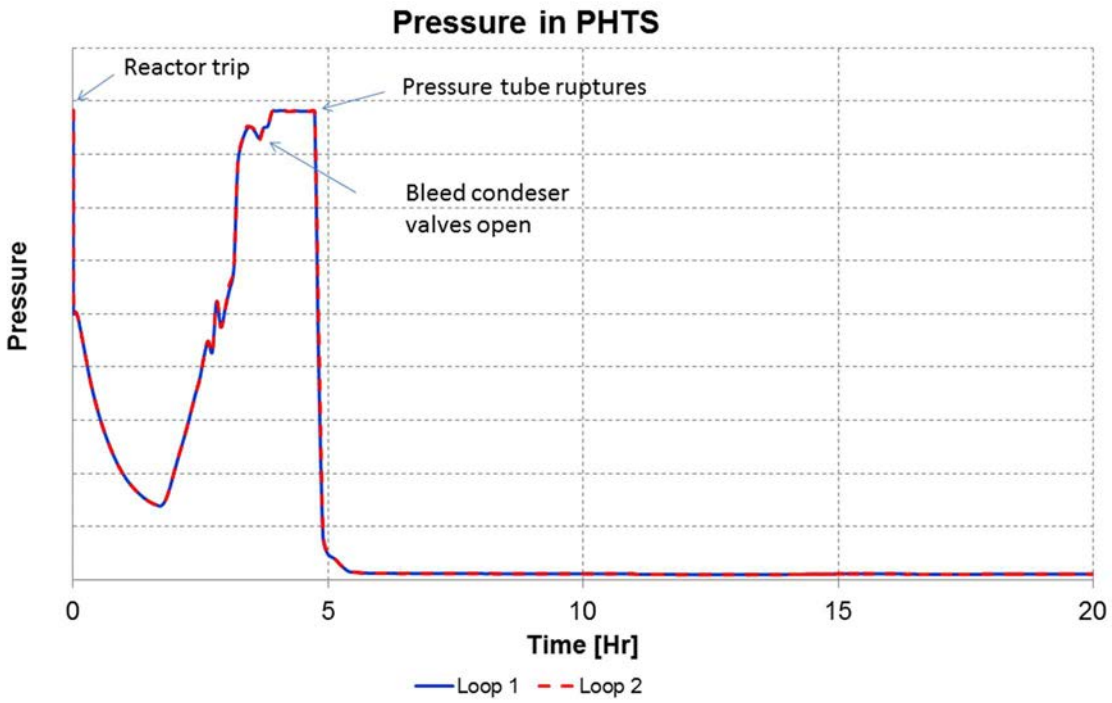

FIG. B-1 Primary Heat Transport System Pressure Response.

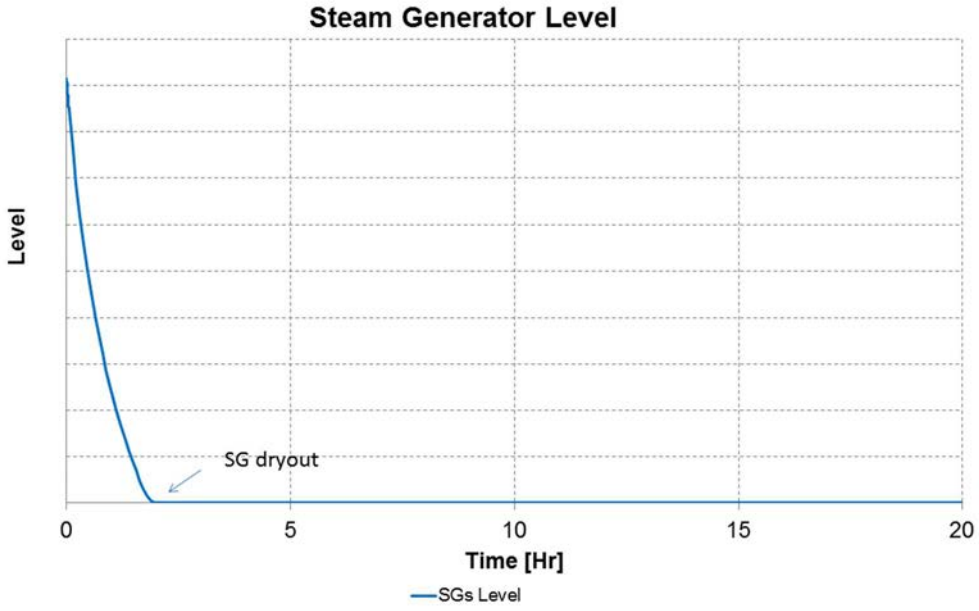

FIG. B-2 Steam Generator Level Response.

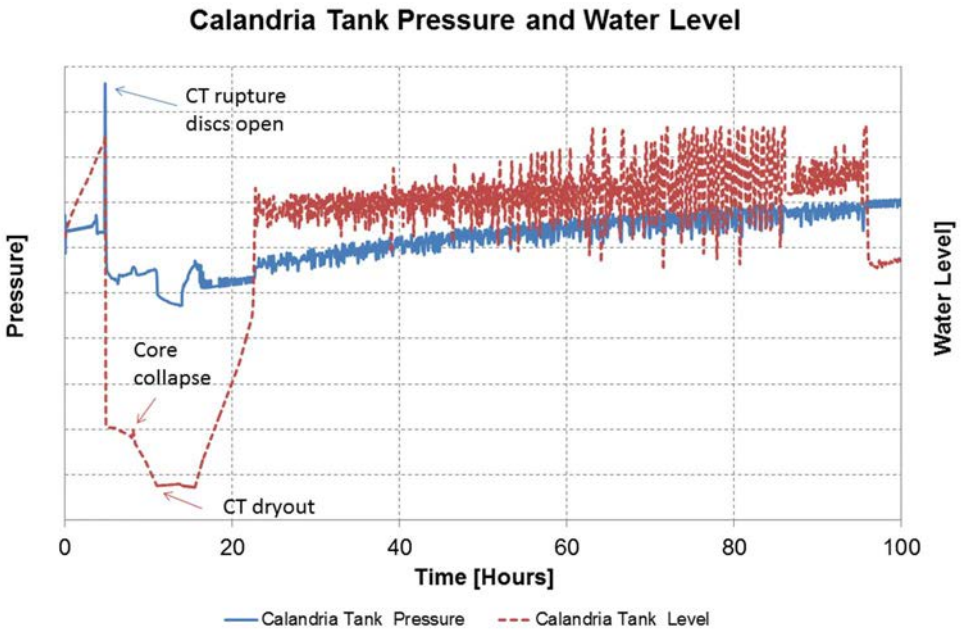

FIG. B-3 Calandria Tank Response.

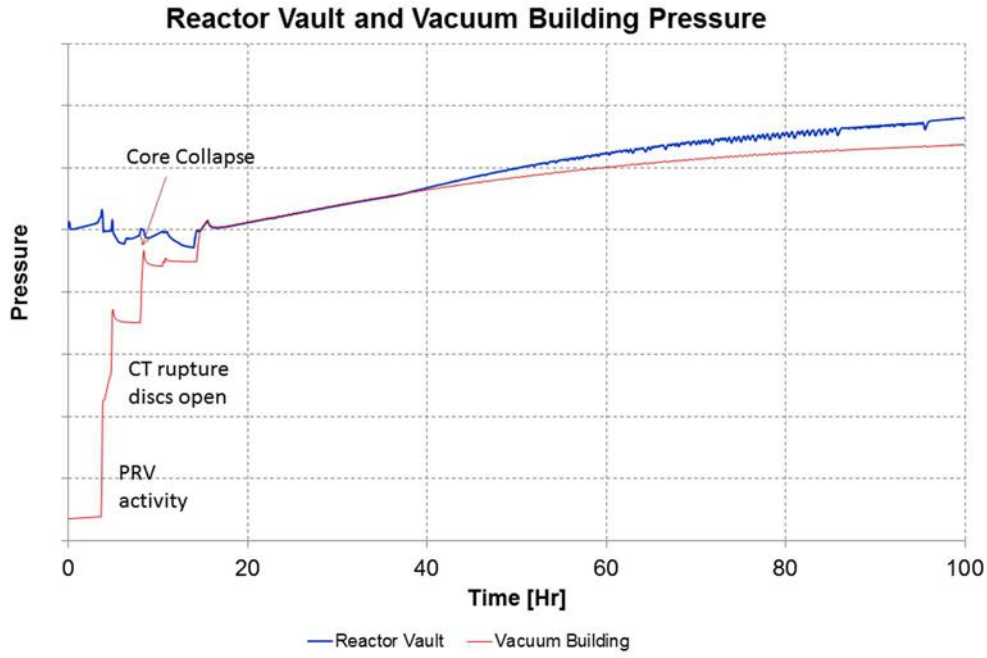

FIG. B-4 Reactor Building and Vacuum Building Pressure Response

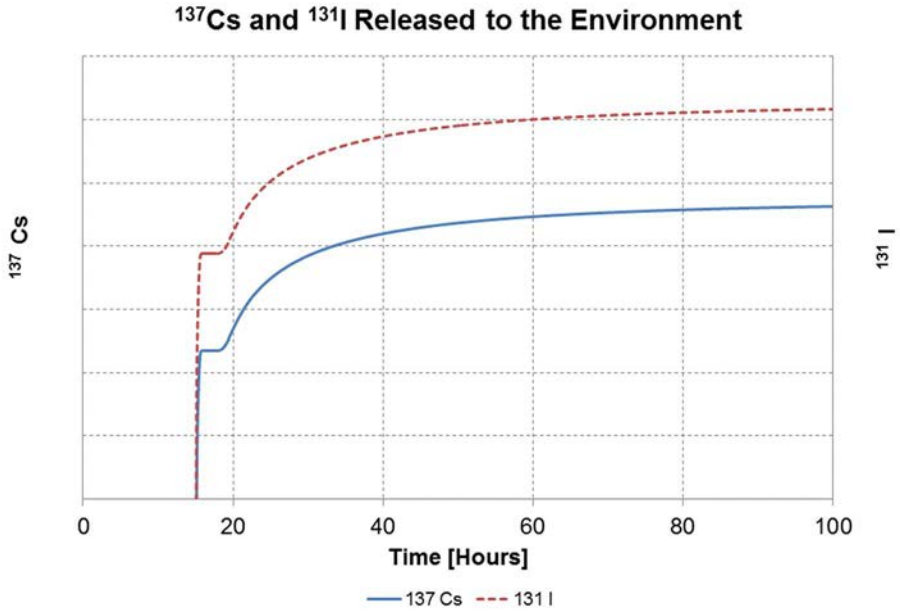

FIG. B-5 Airborne Activity Release to the Environment.

REFERENCES ANNEX II

[II-1]. CANADIAN NUCLEAR SAFETY COMMISSION, REGDOC-3.6, Glossary of CNSC Terminology, Ottawa, Canada (2019)

[II-2]. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[II-3]. CSA GROUP, Requirements for beyond design basis accidents, N290.16-16, Canada (2016)

[II-4]. CANADIAN NUCLEAR SAFETY COMMISSION, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada (2014).

[II-5]. CANADIAN NUCLEAR SAFETY COMMISSION, REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, Ottawa, Canada (2014).

[II-6]. WORLD ASSOCIATION OF NUCLEAR OPERATORS, SOER 2013-2-Rev. 1 Post-Fukushima Daiichi Nuclear Accident Lessons Learned, WANO, (2013)

[II-7]. WORLD ASSOCIATION OF NUCLEAR OPERATORS, SOER 2011-3 Fukushima Daiichi Nuclear Station Spent Fuel Pool/Pond Loss of Cooling and Makeup, WANO, (2011)

[II-8]. CSA GROUP, Quality assurance of analytical, scientific, and design computer programs, N286.7-16 (2016)

[II-9]. CANDU OWNERS GROUP, Guidelines for Application of the LOE/ROE Methodologies to Deterministic Safety Analysis, COG-11-9023 R1 (2014)

[II-10]. CANADIAN NUCLEAR SAFETY COMMISSION, REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, Ottawa, Canada (2014).

[II-11]. INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009).

[II-12]. CANADIAN NUCLEAR SAFETY COMMISSION, CNSC Integrated Action Plan on the Lessons Learned From the Fukushima Daiichi Nuclear Accident, Ottawa, Canada (2013).

ANNEX III. ANSWERS TO THE QUESTIONNAIRE PROVIDED BY PARTICIPATING TECHNICAL EXPERTS FROM FINLAND

Answer 1:

Definitions and terminology used in Finland are given in regulation STUK Y/1/2018 [III-1] and YVL-guides.

DEC A: an accident where an anticipated operational occurrence or class 1 postulated accident involves a common cause failure in a system required to execute a safety function.

DEC B: an accident caused by a combination of failures identified as significant on the basis of a probabilistic risk assessment.

DEC C: an accident caused by a rare external event and which the facility is required to withstand without severe fuel failure.

Severe accident: accident in which a considerable part of the fuel in a reactor or of the spent fuel in a spent fuel pool or storage loses its original structure.

Severe Reactor Accident: refers to an accident in which a considerable part of the fuel in a reactor loses its original structure. (Note that this condition stands for the same accident category as the IAEA term 'DEC with core melting').

Answer 2:

In Finland, as in the IAEA general safety requirements (e.g. Safety Assessment for Facilities and Activities, General Safety Requirements Part 4 No. GSR Part 4 (Rev. 1)), the safety of nuclear power plant needs to be assessed. It is required to demonstrate analytically, and experimentally if needed, that the NPP design fulfils the required safety level and safety requirements. The accident analyses need to provide a comprehensive assessment of the NPP behaviour during the accidents, as well as releases of radioactive substances and radiation doses arising from the accidents.

Severe accident analyses need to justify that the Severe Accident Management (SAM) strategy is feasible. Analyses need to investigate all the physical, chemical and mechanical phenomena associated with severe accidents and the SAM strategy.

The severe accident analyses, with the SAM strategy, are the base for the SAM guidelines. The operational strategy for SAM is based on the safety functions, operational actions and system design justified in the severe accident analyses.

Analyses need to confirm the design features of SAMs and the fulfilment of the acceptance criteria with the required safety margin and with high confidence. Some examples of design features assessed are the following:

(a) Depressurization of primary circuit;

(b) Cooling and stabilization of the molten core materials;

(c) Management of containment pressure, ensuring containment integrity and containment isolation;

(d) Heat transfer from the molten core and from containment to the ultimate heat sink;

(e) Justification of hydrogen management systems, hydrogen risk evaluation and prevention of hydrogen detonations;

(f) Justification of layout and design of passive system structures important for severe accident management (e.g. reactor pit, core catcher);

(g) Other systems designed for severe accident management;

(h) Systems designed for measuring and monitoring the progression of severe accident and the performance of SAM systems.

Severe accident analyses need to confirm the fulfilment of requirements for systems designed for SAM; active systems or components are required to be capable of performing its safety function even in the event of a most penalizing single failure. Other systems than those dedicated to SAM cannot be credited in severe accident analyses.

The severe accident analyses need to provide an assessment of the radiological consequences of severe accidents. These source term analyses need to justify the fulfilment of the acceptance criteria given in the Government Degree on the Safety of Nuclear Power Plants 717/2013 [III-2], STUK regulations and YVL-guides. In addition to deterministic analyses, level 2 probabilistic risk assessment (PRA) is used to assess the amount, probability and timing of radioactive releases from the NPP during severe accidents. Analyses includes the interactions between physical phenomena and safety systems and the reliability analysis of the systems intended for SAM, considering the accident conditions and human actions.

Containment analyses provides the environmental conditions anticipated during the severe accidents. These analyses are prepared for containment, but also for all other areas where a SAM system is located. It is required that the SAM systems be qualified for the environmental conditions of the location they are installed in. Containment analyses need to provide the (maximum) temperature, pressure, humidity and radiation levels anticipated during and after a severe accident. From the analyses results the most challenging environmental conditions are derived, in which the SAM systems need to be qualified for.

Qualification processes that demonstrate the SSCs are suitable for their intended use and fulfils the relevant safety requirements, includes also the environmental qualification process (corresponds to the qualification process of the ISO 9000 standard). The licensee needs to prepare and implement a qualification plan, where the verification and validation data of the SSCs is presented, the used external assessments, tests and analyses are identified, and the qualification roadmap, produced documentation and submission for regulatory review are presented. It is the licensee's responsibility to justify that the SSCs are qualified for the environmental conditions that they are designed for. YVL B.1 [III-3], chapter 3.9 'Qualification' gives the requirements related to the qualification of SSCs.

Most requirements for the severe accident analyses are given in STUK regulation Y/1/2018 'Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant' and YVL-guide B.3 'Deterministic Safety Analyses for a Nuclear Power Plant' [III-4].

STUK Regulation Y/1/2018 [III-1]:

Chapter 2, Section 3 Demonstration of compliance with safety requirements:

“1. The safety of a nuclear power plant shall be assessed when applying for a construction licence and operating licence, in connection with plant modifications, and at Periodic Safety Reviews during the operation of the plant. It shall be demonstrated in connection with the safety assessment that the nuclear power plant has been designed and implemented in a manner that meets the safety requirements. The safety assessment shall cover the operational states and accidents of the plant. The safety of a nuclear power plant shall also be assessed after accidents and, whenever necessary, on the basis of the safety research results.

2. Nuclear power plant safety and the technical solutions of its safety systems shall be assessed and substantiated analytically and, if necessary, experimentally.

3. The analyses shall be maintained and revised as necessary, taking into account operating experience from the plant itself and from other nuclear power plants, the results of safety research, plant modifications, and the advancement of calculation methods.

4. The analytical methods employed to demonstrate compliance with the safety requirements shall be reliable, verified and qualified for the purpose. The analyses shall demonstrate the conformity with the safety requirements with high certainty. Any uncertainty in the results shall be considered when assessing the meeting of the safety requirements.”

YVL-guide A.7 [III-5]:

“715. The severe accident management guidelines shall be based on the severe accident management strategy and the related analyses.”

YVL-guide B.1, 3.9 Qualification [III-3]:

“362. The systems, structures and components important to safety shall be qualified for their intended use. The qualification process shall demonstrate that the systems, structures and systems are suitable for intended use and satisfy the relevant safety requirements. Aside from the assurance of the correctness of the design bases and the sufficiency of the quality management of design and implementation, the qualification process shall also include environmental qualification.

363. A qualification plan shall be prepared and implemented for the system to guide the qualification process. The qualification plan shall:

1. present the data generated in connection with the quality assurance stages (verification and validation) of the systems, structures and components to be used for qualification purposes;

2. identify the external assessments, tests and analyses to be used the purpose of qualification, including the methods to be used, their relevance and the performer;

3. present a qualification roadmap complete with estimated timetables and dependencies relative to the progress of the project; and

4. specify the documentation to be produced in connection with the qualification process and its submission for regulatory review.

364. The licensee shall evaluate the acceptability of the qualification results and present a justified conclusion drawn from the results."

YVL-guide B.3 [III-4]:

"301. Analyses pertaining to the plant's behaviour as well as releases of radioactive substances and radiation doses shall cover the nuclear power plant's normal operational states, anticipated operational occurrences, postulated accidents, design extension conditions and severe reactor accidents.

302. The scope of the analysed events shall provide a comprehensive assessment of the nuclear power plant's behaviour during incidents and accidents as well as releases and doses due to incidents and accidents.

303. Operator actions shall be assessed to identify essential operator actions needed in accident management and to assess the effects of potential operator errors."

"308. Severe reactor accident analyses shall cover all actions required for the plant's severe reactor accident strategy and the phenomena associated with the strategy."

"401. Analyses shall cover anticipated operational occurrences and accidents that determine or limit the dimensioning of systems accomplishing safety functions.

402. Anticipated operational occurrences and accidents shall be analysed starting from the initiating event and ending in a safe state."

"426. The time needed for actions required for the severe reactor accident management strategy and other factors relating to the implementation of the actions (e.g. accessibility of locally operated equipment) shall be justified.

427. Analyses justifying the hydrogen management strategy shall separately evaluate cases in which the hydrogen generation rate increases."

Answer 3:

Classification and identification of severe accident analysis scenarios is done by the licensee applicant (or plant vendor). Justified expert judgement and operating experience feedback can be used to prove that Severe Accident analyses cover all the relevant scenarios.

Only accidents resulting in core melt are considered as severe reactor accident scenarios. Meaning that no other complex sequences or DEC scenarios are identified as severe accidents, if the transient does not propagate into a core melt.

The Probabilistic risk analysis results is used as a support in deciding which severe accident event sequences are analysed for radiation effects caused by an accident and in deciding which accident sequences are used in emergency planning. (see YVL A.7 [III-5]).

YVL-guide uses IAEA safety standards as references for examples of the events to be analysed. (More specifically, IAEA General Safety Requirements, Safety Assessment for Facilities and Activities, GSR Part 4 [III-6] and IAEA Specific Safety Guide, Deterministic Safety Analysis for Nuclear Power Plants SSG-2 [III-7]).

Severe accident scenarios ('DEC with core melting') need to cover all potential accident scenarios, phenomena related to severe reactor accidents and all operational states of the NPP. For example, scenarios for postulated severe reactor accidents can be classified as follows:

(a) According to their initiating event (e.g. loss of coolant accident, loss of outside power).

(b) According to the NPP operating state (e.g. power operation, startup, shutdown, refuelling).

(c) According to the analysis objective, as a representative, bounding or extreme scenario:

  (i) In representative scenarios, design of SAM systems and SAM strategy is analysed. Analyses are done with assumptions that systems functions are as designed.

  (ii) In bounding scenarios analyses, the robustness of SAM systems and Severe accident measures are studied. With these analyses existence of cliff edge effects is analysed. Analyses are done with failure assumptions or delays in the safety functions (accident management measures).

  (iii) In extreme scenarios analyses, highly energetic phenomena are studied. These scenarios are related to the Level 2 PSA.

YVL-guide B.3 [III-4]:

(a) "301. Analyses pertaining to the plant's behaviour as well as releases of radioactive substances and radiation doses shall cover the nuclear power plant's normal operational states, anticipated operational occurrences, postulated accidents, design extension conditions and severe reactor accidents. Examples of the events to be analysed are given in [Safety Assessment for Facilities and Activities, General Safety Requirements. IAEA Safety Standards Series No. GSR Part 4. IAEA, Vienna 2009. and Deterministic Safety Analysis for Nuclear Power Plants. IAEA Specific Safety Guide No. SSG-2. IAEA, Vienna 2009]"

(b) "302. The scope of the analysed events shall provide a comprehensive assessment of the nuclear power plant's behaviour during incidents and accidents as well as releases and doses due to incidents and accidents."

(c) "308. Severe reactor accident analyses shall cover all actions required for the plant's severe reactor accident strategy and the phenomena associated with the strategy."

(d) "401. Analyses shall cover anticipated operational occurrences and accidents that determine or limit the dimensioning of systems accomplishing safety functions."

YVL-guide A.7 [III-5] states the role of level 2 Probabilistic risk analysis:

(d) "324. The PRA shall be used as support in deciding which severe accident event sequences are analysed in accordance with Guide YVL B.3 for radiation effects (releases and doses) caused by an accident and also in deciding which accident sequences are used in emergency planning in accordance with Guide YVL C.5."

(e) “406. The Level 2 PRA shall assess the amount, probability and timing of a release of radioactive substances leaking from the nuclear power plant during severe accidents.

(i) The results of the Level 2 PRA shall present:

— a summary of the functionality of the severe accident management strategy, including assessments of the success probabilities of severe accident management functions by plant damage states and release categories.

(ii) The Level 2 PRA shall present at least the following:

— reliability analysis of the systems intended for severe accident management taking into account the conditions prevailing during an accident and also human action.”

Answer 4:

Controlled state following a severe reactor accident refers to a state where the removal of decay heat from the reactor core debris and the containment has been secured, the temperature of the reactor core debris is stable or decreasing, the reactor core debris is in a form that poses no risk of recriticality, and no significant volumes of fission products are any longer being released from the reactor core debris. (see STUK regulation Y/1/2018 [III-1])

Safe state following a severe reactor accident refers to a state where the conditions for the controlled state of a severe reactor accident are met and, in addition, the pressure inside the containment is low enough that leak from the containment is minor, even if the containment is not leaktight. (see STUK regulation Y/1/2018 [III-1])

Answer 5:

In the YVL-guides the best estimate approach is defined similarly, and refers, to the IAEA definition:

YVL B. 3 [III-4] 410. “Utilisation of the best estimate method shall be supplemented with an uncertainty analysis that is justifiable by statistical methods. Examples of such methods are given in ‘Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, IAEA SRS 52’.”

Applied Best estimate method can be other than mentioned in the IAEA SRS-52 referred above. Essential is that the applied method provides results of the examined parameter as distribution with required probability and confidence level.

YVL-guide B.3 [III-4] states requirements of the assumptions for severe reactor accident analysis:

(a) “423. In analysing severe reactor accidents, best estimate methods can be applied concerning assumptions of the plant's initial state and the performance of operating subsystems. However, the more essential the function, the better assurance for its successful accomplishment shall be provided.

(b) 424. In severe accident analyses, application of the best estimate method need not be complemented with an uncertainty analysis.”

(c) “602. In applying a best estimate method with uncertainty analysis, the result is acceptable if there is a 95% probability with 95% confidence that the examined parameter will not exceed the acceptance limit set for the conservative analysis method.”

Cliff edge effects are assessed with analysing bounding or extreme scenarios. In these analyses, for example, delay of primary depressurization is assumed.

YVL B.3 [III-4] “Operator actions shall be assessed to identify essential operator actions needed in accident management and to assess the effects of potential operator errors.”

No specific safety margins are set. The STUK Regulation Y/1/2018 [III-1], section 3 states that:

“4. The analytical methods employed to demonstrate compliance with the safety requirements shall be reliable, verified and qualified for the purpose. The analyses shall demonstrate the conformity with the safety requirements with high certainty. Any uncertainty in the results shall be considered when assessing the meeting of the safety requirements.”

Answer 6:

Validation and verification are required for the analysis tools used for severe accident analyses. Used calculation tools need to be suitable for their intended use.

The STUK Regulation Y/1/2018 [III-1], section 3 requires that:

“2. Nuclear power plant safety and the technical solutions of its safety systems shall be assessed and substantiated analytically and, if necessary, experimentally.

3. The analyses shall be maintained and revised as necessary, taking into account operating experience from the plant itself and from other nuclear power plants, the results of safety research, plant modifications, and the advancement of calculation methods.

4. The analytical methods employed to demonstrate compliance with the safety requirements shall be reliable, verified and qualified for the purpose. The analyses shall demonstrate the conformity with the safety requirements with high certainty. Any uncertainty in the results shall be considered when assessing the meeting of the safety requirements.”

YVL B.3 [III-4] requires that:

“403. The suitability of analysis methods for their purpose shall be justified.

404. A description of the models and calculation methods used in the analyses shall be given. The models shall be described to a level of detail that facilitates conducting of verifying analyses. The information to be presented shall include the analysis model representing the plant or its component (e.g. the division into nodes applied in the model), justification of the selected model parameters as well as the plant data used for the analyses or a reference to the source of the available plant data.

405. The validation of the physical models and computer code used for the analyses shall be substantiated by comparing their calculation results to separate effects tests or tests carried out

on entire systems, or to disturbances that have occurred at nuclear power plants. Comparison with models that have already been validated may also be utilised.

406. The plant and fuel type specific experimental correlations used in the calculation methods shall be justified by presenting the measurement data from which the correlations have been derived. If the correlation is commonly known and the measurement data are publicly available, a bibliographic reference is sufficient.

407. If reliable calculation methods are not available, the acceptability of the technical solution in question shall be justified by means of experiments."

In Finland, the regulatory body does not review or approve the codes used for the safety demonstration. Input data files or similar specific analysis tool documentation is not required to be submitted to STUK.

Answer 7:

(f) Facility representation and modelling: The facility representation is realistic and/or best estimate, based on the real geometrics of NPP. Conservative or best estimate analysis method is accepted; the suitability of the chosen method needs to be justified.

(g) Initial and boundary conditions: They are conservative or best estimate, depending on used method. Needs to be justified.

  (i) YVL B.3 [III-4] "411. The initial conditions of the conservative analyses and the conservativeness of the parameters chosen shall be justified. If the choice that is the least beneficial in terms of the acceptability of the end result is not unambiguous, analysis results covering the parameter's entire range of variation shall be presented."

  (ii) "423: In analysing severe reactor accidents, best estimate methods can be applied concerning assumptions of the plant's initial state and the performance of operating subsystems. However, the more essential the function, the better assurance for its successful accomplishment shall be provided."

Common practice is to model the NPP and its SSCs as realistically as possible and to use best estimate models in the analyses.

(h) Considerations on uncertainty and sensitivity as applicable: no systematic uncertainty or sensitivity analysis are required. However, justification of used parameters and modelling assumptions is required, (see above).

(i) Availability of systems and components: qualified severe accident management systems are assumed to be in operation and available as designed. All active SAM systems are required to fulfil the single failure criterion and most penalizing single failure is assumed in the analyses.

  (i) B.3 [III-4] "425. In severe reactor accident analyses, the most penalising failure according to the failure criterion presented in chapter 4.3 of Guide YVL B.1 [III-3] shall be assumed for systems designed for severe reactor accident management. Consequences of the initiating event shall also be taken into account."

(j) Systems credited in the analyses (use of safety features and other systems): Only the systems designed for SAM can be credited in severe accident analyses. These systems are functionally and physically independent from systems intended for normal operation and

anticipated operational occurrences and for controlling postulated accidents and design extension conditions.

Common practice is that non-permanent equipment is not credited in the safety analyses. Basis design principle in Finland is that all systems credited in the NPPs safety demonstration are permanently fixed systems.

(k) Operator actions (time and action): The time needed for actions required for the severe reactor accident management strategy and other factors relating to the implementation of the actions (e.g. accessibility of locally operated equipment) need to be justified. In the representative scenarios, the operational actions are assumed to be performed correctly and timely. In bounding scenarios, delayed operator actions (time and fulfilment of needed action) are assumed.

   (i) YVL B.3 [III-4] "413: The selected consideration time preceding operator actions and the time to accomplish the actions shall be sufficiently long. The durations chosen shall be justified. Operators can be assumed to act on each analysed event in accordance with the procedures available in written or electronic form."

   (ii) YVL B.3 [III-4] "426: The time needed for actions required for the severe reactor accident management strategy and other factors relating to the implementation of the actions (e.g. accessibility of locally operated equipment) shall be justified."

(l) Equipment qualification: All severe accident systems and equipment need to be qualified for their purpose and for severe accident conditions. In analyses these systems are assumed to withstand the environmental conditions they are qualified in.

   (i) YVL B.1 [III-3]: "362: The systems, structures and components important to safety shall be qualified for their intended use. The qualification process shall demonstrate that the systems, structures and systems are suitable for intended use and satisfy the relevant safety requirements. Aside from the assurance of the correctness of the design bases and the sufficiency of the quality management of design and implementation, the qualification process shall also include environmental qualification."

(m) Operator action in a harsh environment: Not assumed in analyses. Emergency control room is required in Finland and environmental conditions (e.g. radiation levels, temperature) need to be analysed for locally executed manual operator actions. Accessibility, including radiation protection, of local operational actions need to be justified.

   (i) YBL B3 [III-4]: "426. The time needed for actions required for the severe reactor accident management strategy and other factors relating to the implementation of the actions (e.g. accessibility of locally operated equipment) shall be justified."

(n) Analysis end-state: the analysis needs to provide justification for reaching the controlled and safe state after a severe accident. Maintaining the safe state for a long time has to be presented as identifying the systems needed in long time and their qualification. Justification of the design path how to reach and maintain a controlled state or a safe state following a severe reactor accident for a long time is required.

   (i) YVL B.3 [III-4] "402: Anticipated operational occurrences and accidents shall be analysed starting from the initiating event and ending in a safe state."

Answer 8:

The main quantitative criteria of severe accident analyses, the limit values for radioactive substances and requirements about environmental consequences arising from a severe accident are given in Government Decree on the Safety of Nuclear Power Plants 717/2013 [III-2]:

"The release of radioactive substances arising from a severe accident shall not necessitate large scale protective measures for the public nor any long-term restrictions on the use of extensive areas of land and water.

In order to restrict long term effects, the limit for the atmospheric release of caesium-137 is 100 terabecquerel (TBq). The possibility of exceeding the set limit shall be extremely small.

The possibility of a release in the early stages of the accident requiring measures to protect the public shall be extremely small."

YVL-guide A7 [III-5] specifies these requirements further:

(a) "305. The design of a nuclear power plant unit shall be such that the mean value of the frequency of reactor core damage is less than 10-5/year.

(b) 306. A nuclear power plant unit shall be designed in compliance with the principles set forth in Section 10 of Government Decree (717/2013) (Nuclear Energy Decree 22b) in a way that:

   (i) the mean value of the frequency of a release of radioactive substances from the plant during an accident involving a Cs-137 release into the atmosphere in excess of 100 TBq is less than 5·10-7 per year;

   (ii) the accident sequences, in which the containment function fails or is lost in the early phase of a severe accident, have only a small contribution to the reactor core damage frequency."

STUK regulation Y/1/2018 [III-1]: Section 3 Demonstration of compliance with safety requirements:

"1. The safety of a nuclear power plant shall be assessed when applying for a construction license and operating license, in connection with plant modifications, and at Periodic Safety Reviews during the operation of the plant. It shall be demonstrated in connection with the safety assessment that the nuclear power plant has been designed and implemented in a manner that meets the safety requirements. The safety assessment shall cover the operational states and accidents of the plant. The safety of a nuclear power plant shall also be assessed after accidents and, whenever necessary, on the basis of the safety research results."

Answer 9:

YVL-guide B.3 [III-4] chapter 7 defines the documents of deterministic safety analyses that are required to be submitted to STUK:

(a) "703. The preliminary safety analysis report shall present the calculation methods for transient and accident analyses and their validation, as well as the preliminary

transient and accident analyses demonstrating the acceptability of the systems' technical solutions.

(b) 704. The final safety analysis report shall present the calculation methods for transient and accident analyses and their validation, as well as the final transient and accident analyses demonstrating the acceptability of the systems' technical solutions.

(c) 705. The essential results of the analyses shall be presented in the preliminary and final safety analysis reports. Detailed information on the assumptions and calculation methods used in the analyses may be presented in either the safety analysis report or the topical reports.

(d) 706. The description of the models and analysis methods as required in para 404 shall be delivered to STUK for information as part of the preliminary and final safety analysis reports.

(e) 707. The analyses of the preliminary safety analysis report shall describe the plant to the level of detail that is possible at this design stage, in order to facilitate analyses of the plant's operation in all operational conditions during anticipated operational occurrences and accidents."

(f) "710. An assessment on the effects of the planned modification to plant behaviour during transient and accidents, and a summary of design analysis results shall be provided a part of the conceptual plan required for modifications to an operating nuclear power plant's systems in safety classes 1, 2 and 3. Analyses verifying the acceptability of the technical solutions shall be provided as part of the pre-inspection documentation.

(g) 711. In connection with periodic safety assessments, the licensee shall evaluate the scope of and need for updates in transient and accident analyses, and update the analyses for the final safety analysis report, where necessary."

Answer 10:

No answer provided.

Answer 11:

No answer provided.

REFERENCES ANNEX III

[III-1]. Radiation and Nuclear Safety Authority in Finland (STUK), Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant, STUK Y/1/2018 (2018).

[III-2]. Government Degree on the Safety of Nuclear Power Plants, Ministry of Employment and the Economy 717/2013.

[III-3]. Radiation and Nuclear Safety Authority in Finland (STUK), Safety Design of a Nuclear Power Plant, STUK YVL B.1 (2013).

[III-4]. Radiation and Nuclear Safety Authority in Finland (STUK), Deterministic Safety Analyses For A Nuclear Power Plant, STUK YVL B.3 (2013).

[III-5]. Radiation and Nuclear Safety Authority in Finland (STUK), Probabilistic Risk Assessment and Risk Management of a Nuclear Power Plant, STUK YVL A.7 (2013).

[III-6]. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR PART 4, IAEA, VIENNA (2009).

[III-7]. INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, VIENNA (2009).

ANNEX IV. ANSWERS TO THE QUESTIONNAIRE PROVIDED BY PARTICIPATING TECHNICAL EXPERTS FROM FRANCE

Answer 1:

Definitions of accidents are given in the Authorité de Sûreté Nucléaire (ASN)technical guide number 22 [1] [IV-1]. According to this technical guide, sequences to be addressed in DEC include:

(a) Conditions called 'DEC-A' where core melting has to be prevented. A list of multiple failure conditions, to be assessed deterministically in order to design additional measures, is postulated. The results of the probabilistic safety studies done at design stage are used to check and adjust the preliminary list of multiple failures conditions and to check the appropriateness of the foreseen additional measures;

(b) Conditions called 'DEC-B' where core melting is postulated despite the measures taken to prevent it;

(c) Natural external hazards of higher severity than those considered in the design basis.

Answer 2:

The objectives of DEC analysis can be summarized as follows:

(c) DEC analyses are used to confirm that features, credited for DEC, have the requested performances to meet their relevant safety objectives, in addition to DBA studies:
   (i) No core melting such as to ensure prevention of core melting for DEC-A.
   (ii) Protection actions that are limited in terms of lengths of time and areas of application need to be sufficient to protect people and the environment, this meaning limitation of radiological consequences in DEC-B.

(d) In particular, the demonstration needs to meet the following requirements:
   (i) DEC-A conditions are considered in emergency operating procedures (with other specific procedures or guidelines when applicable). DEC-B conditions need to be considered by SAM guidelines (with other specific procedures or guidelines when applicable).
   (ii) Any equipment credited in a DEC analysis needs to be adequately qualified to perform its safety functions in the environmental conditions resulting from this DEC situation.
   (iii) SSCs that are necessary to meet the safety requirements in DEC analyses need to be considered as items important to safety and to be safety classified accordingly.

[1] Conception des réacteurs à eau sous pression, Guide de l'ASN n°22, Version du 18/07/2017

Answer 3:

According to the French TG [IV-2] (Technical Guidelines-IPSN and GRS - Technical Guidelines for the design and construction of the next generation of nuclear power plants with pressurized water reactors, adopted by the [French] Advisory Committee for Nuclear Reactors (GPR) and German experts plenary meetings held on October 19th and 26th 2000), the DEC identification has to be derived on the basis of deterministic and probabilistic assessments which can be reinforced by engineering judgment.

For new reactors, at an early design stage, a preliminary list of DEC-A is developed based on a deterministic basis. To this purpose, the applied method consists of the following:

(a) Systematic study of Design Basis Conditions 2 and Design Basis Conditions 3 with a relevant postulated Common Cause Failure on the protection systems or some engineered safety systems credited in the Design Basis Conditions analysis;

(b) Systematic study of Design Basis Conditions 1 with a postulated Common Cause Failure on the safety systems in operation in normal operation conditions.

Note that Design Basis Conditions 4 are excluded from these analyses considering that the occurrence of a Design Basis Conditions 4 combined with a Common Cause Failure has a frequency of occurrence making it unlikely to occur.

In order to confirm this list, additional DEC-A probabilistic criteria are considered. The DEC-A list is screened using the Level 1 PSA (internal events) as soon as it is made available. For example, a DEC-A provision is added to the design only if the core melting frequency calculated for the functional sequence, without crediting the provision, is higher than 10^{-8}/y.r. (for new reactors).

A combination of a deterministic approach and probabilistic insights allows to start early on the basis of deterministic consideration only, with later refinements when PSA insights are made available.

The DEC-B analysed in the safety report of a new reactor correspond to situations where the capability of the plant to prevent severe fuel damage is exceeded or where measures intended to prevent severe fuel damage are assumed to fail totally or partially. Such situations are identified thanks to Level 1 PSA studies, but also thanks to deterministic consideration.

Answer 4:

The controlled state and the safe state are defined by the ASN technical guide n°22 [IV-1] with a very similar wording, hence are also in use in the design of NPPs. However, practically, these precise definitions are not used for DEC analyses. They are appropriate and therefore used in the context of Design Basis Conditions analyses, as the SSCs necessary to reach the controlled state in Design Basis Conditions and the SSCs necessary to reach the safe state in DBC might be rather different and are considered in different approaches, especially with specific criteria in terms of classification approach, resulting in assigning them to different safety classes.

In DEC-A analyses, consistent with the ASN technical guide n°22 [IV-1], the definition used is ‘end state’. The end state to be reached is defined as follows: the core is subcritical, the decay

heat is removed by primary or secondary systems, the containment is ensured so that the activity releases remain tolerable.

For DEC-B, the plant is considered to be in a stabilized and controlled state when: (a) all parts of the degraded core, either still in place and/or relocated ex-vessel, are in a coolable and subcritical configuration, and any stored spent fuel is also in a coolable and subcritical configuration; (b) dispositions have been taken to limit as far as possible any further dispersion of radioactive products or any release to the environment; (c) there is no apparent nor urgent risk of combustible gas explosions

Answer 5:

Identification of a list of DEC situations has been developed in the previous answer above and nothing more is added below.

The best estimate approach means that the analysis could be performed as 'realistically as possible' according to the state of the art knowledge. In France, this is applied to computer codes used, boundary and initial conditions, and availability of the systems and operator actions.

Considering boundary and initial conditions, the plant is considered initially in normal operation with regulations, equipment and system at their set point according to the normal operating procedures. Then a bounding case (bounding several sequences leading to a similar situation) is considered where the main relevant parameters for the situation (i.e. the parameters which have a major effect, a first order impact on the study results) are set at a reasonably bounding value, whereas other parameters may be set to their nominal value.

As a general principle, all systems can be deemed available, except those which are assumed to have failed in the multiple failure combination (directly or consequently) and those which are not demonstrated to be able to perform their function in the environmental conditions corresponding to DEC. No additional failure or unavailability for maintenance has to be deterministically postulated in the systems required to reach the end state.

Nevertheless, in practice, DEC-A analyses are generally performed using the same computer codes and conservative assumptions for initial and boundary conditions than in DBC analyses. This applies typically to the values of the main relevant parameters, which are set at the same value than for DBC analyses. The consideration of such conservative assumptions is there to demonstrate sufficient margins to avoid cliff edge effects, without the need to expand too much on additional sensitivity analyses.

DEC-B analyses are generally based on best estimate codes and assumptions. In that case, the existence of sufficient margins to avoid cliff edge effects is demonstrated by performing additional sensitivity studies.

Answer 6:

Although, in France, there is no formal procedure of selection of analytical tools, we usually rely on such tools, where maturity of development and user feedback are significant. Tools and codes have been developed with combined efforts from public R&D supported by EDF R&D teams and also the technical safety organization (Institut de Radioprotection et de Sûreté Nucléaire) of the regulatory body (ASN). Numerical verification is standardized while

experimental validation with respect to establishment of field of application and all kind of extrapolation are based mainly on expert judgment, where possible on R&D experimentations.

Nevertheless, the French Regulation, recalled in the ASN technical guide n°22 [IV-1], (previously this was also required by the TG [IV-2]) indicate that nuclear safety assessment is based on:

(a) Up to date and documented data;

(b) Appropriate, explicitly mentioned and validated methods taking account of assumptions and rules adapted to uncertainties and knowledge limits about the addressed phenomena;

(c) Tools and codes validated for the extent of area they are used;

(d) The licensee has to justify the criteria used for selection, validation and qualification of the codes and model tools, as well as for assessment of the obtained results.

EDF has developed a quality assurance process for validation and qualification of codes and tools, considering a periodic review. Any code or tool have to follow this process before being able to be used as part of the safety demonstration. This includes the definition of the 'domain of validity' of the code. All codes and tools used for a dedicated study are clearly identified in the report of the study with the justification, rationale for their use and verification that they are fit for purpose, including to ensure that the codes are appropriately used in their domain of validity.

There is no major difference for DEC-A and DEC-B studies on these principles, apart from the limitation on knowledge on some specific severe accident phenomena, justifying some sensitivity studies as explained in the previous answer above. However, DEC-B are using different codes and tools dedicated to severe accident.

Answer 7:

For DEC-A analyses as already explained above:

(a) Facility representation and modelling: generally, very similar to DBC analyses, i.e. conservative;

(b) Initial and boundary conditions: conservative for parameters of major influence;

(c) Considerations on uncertainty and sensitivity as applicable: N/A (see above: codes and assumptions are conservative enough);

(d) Availability of systems and components: no additional failure (e.g. no application of the single failure criterion);

(e) Systems credited in the analysis (use of safety features and other systems): the systems necessary to meet the criteria need to be considered as important to safety, and safety classified accordingly. However, a non-classified system may be credited if already in service before the initiating event and if not affected by the transient, with an appropriate justification;

(f) Operator actions (time and action): actions credited in DEC analyses need to be required by emergency operating procedures. No operator actions are credited before 30 min after the initiating event for actions from the control room, and before 1 h for local to plant actions;

(g) Equipment qualification: equipment credited in a DEC analysis needs to be demonstrated to operate in the environmental conditions corresponding to these DEC, therefore they are classified and assigned to relevant requirements including qualification;

(h) Operator action in a harsh environment: if the DEC analysis relies on local to plant actions, the feasibility of these actions has to be demonstrated (accessibility, from a physical and radiological point of view) via a human factor analysis;

(i) Analysis end-state: see answer to question 4.

For DEC-B analyses: Scenarios analyses are performed within the objective to demonstrate that the core melting accidents meet the qualitative acceptance criteria for DEC-B with core melting (see question 10) using:

(a) Facility representation and modelling: best estimate;

(b) Initial and boundary conditions: best estimate;

(c) Considerations on uncertainty and sensitivity as applicable: yes, to demonstrate sufficient margins to avoid cliff edge effects (i.e. large or early radioactive release);

(d) Systems credited in the analysis: only systems qualified under severe accident conditions;

(e) Operator actions (time and action): as defined in the SAM guidelines;

(f) Equipment qualification: all equipment used in severe accident mitigation are required to be qualified;

(g) Operator action in a harsh environment: if the DEC analysis relies on local plant actions, the feasibility of these actions has to be demonstrated (accessibility, from a

physical and radiological point of view) via a human factor analysis. Habitability of control room and other rooms from where the staff is controlling the plant such as the crisis rooms is checked;

(h) Analysis of end-state: see answer to question 4.

Answer 8:

In the French regulations, acceptance criteria for DEC-A and DEC-B are not precisely defined. It is only recommended that these criteria are defined by the licensee with possible adaptation from the ones used for DBC, to meet the general objectives and requirements presented below.

In DEC-A, as in DBC, the radiological consequences are required to be as low as reasonably practicable, and, in any case, do not necessitate to implement protective measures for the public (no sheltering, no evacuation, and no iodine prophylaxis). Practically, the qualitative acceptance criteria for DEC-A are the same as for DBAs, DBC-4.

The acceptance criteria for DEC-B are specific to the severe accident situation and defined as follows:

(a) Accident situations with core melt which would lead to large and early releases have to be 'practically eliminated': if they cannot be considered as physically impossible, design provisions have to be considered allowing to exclude those accident situations from the design.

(b) Accident situations with core melt that are not 'practically eliminated': 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 (on the basis of International Commission on Radiological Protection criteria).

These qualitative acceptance criteria for DEC-B are based on the 'continuous safety improvement' concept, i.e. no regulatory fixed figures are linked to them.

Based on that, quantitative criteria are defined for:

(a) The containment (Diagram of maximum pressure and temperature for short and long term);

(b) Control of hydrogen concentration within the containment.

Answer 9:

In practice, a chapter of the safety report deals with DEC A and another one with DEC B. They refer to supporting documents for the main details: assumptions, codes, rules followed, themselves supported by additional shared supporting documents about the model and detailed assumptions in relation to the codes and/or tools used. The information provided in these chapters is not particular for those analysis.

Answer 10:

The robustness of the safety demonstration for core melting accident or DEC-B results is further assessed. Practically, the behaviour of the nuclear plant facing an extended loss of AC power and loss of ultimate heat sink is analysed, despite the significantly low frequency of such accident situation.

DEC for spent fuel pool: some DEC-A are identified to address the spent fuel pool specific case. The provisions credited for DEC-A are sufficiently reliable so that a severe accident (DEC-B) in the fuel pool is considered with a high level of confidence to be extremely unlikely to occur.

Answer 11:

Example of EPR DEC-A: Station Black-Out (SBO)

SBO corresponds to the loss of off-site power (LOOP) cumulated with a CCF on all the main emergency diesel generators. The potential consequences of these accident conditions are a degradation of the residual heat removal, hence a fuel degradation and a challenge to the reactor coolant pressure boundary integrity.

A DEC-A provision is designed to cope with the SBO accident: Dedicated SBO diesel generators, started manually from the main control room, supply emergency feedwater pumps.

The SBO analysis aims at demonstrating that the manual start of SBO diesels allows to prevent the steam generators dry out, then to maintain the core residual heat removal.

Example of EPR DEC-B: Corium retention in the core catcher

Due to the high projected power rating of the EPR, in-vessel melt retention by external cooling of the reactor pressure vessel has been discarded from the beginning. Instead, an ex-vessel core melt stabilisation system is implemented. Its function is based on the spreading of the melt onto the surface of a water-cooled metallic plate and a concrete core catcher, followed by subsequent quenching with water drained passively from the in-containment-refuelling-water-storage-tank (IRWST). The efficiency of the stabilization process strongly benefits from the achieved increase in the surface-to-volume ratio of the melt.

Furthermore, unintentional flooding of the core catcher during power operation is not critical to the safety of the plant. As a consequence of this dissociation, power operation and design basis mitigation measures remain unaffected by the provision of a core catcher.

Prior to the relocation of the melt from the pit into the core catcher there is a phase of temporary retention in the reactor pit. This measure reduces the likelihood that the release of the molten material from the reactor pressure vessel (RPV) do not take place in one pour, but in several stages. Temporary retention is based on the provision of a layer of sacrificial concrete that needs to be penetrated by the melt prior to its release from the pit. The resulting delay and the

admixture of sacrificial concrete is making the characteristics of the relocated melt and subsequent spreading and stabilization predictable and independent of the inherent uncertainties associated with in-vessel melt pool formation and RPV failure.

Melt arrival in the core catcher initiates the gravity-driven outflow of water from the IRWST. This water cools the core catcher from the outside and brings the melt into a stable state by means of passive systems only. As an additional option, the containment heat removal system can be used to provide water to the core catcher actively. This will completely submerge the spreading compartment and the reactor pit and stop further steam discharge into the containment as a pre-condition for reaching atmospheric pressure conditions in the long term without the need for a venting system.

REFERENCES ANNEX IV

[IV-1]. Autorité de Sûreté Nucléaire, Conception des réacteurs à eau sous pression, Guide de l'ASN n°22, Version du 18/07/2017.

[IV-2]. Technical Guidelines - IPSN and GRS, Technical Guidelines for the design and construction of the next generation of nuclear power plants with pressurized water reactors, adopted by the French Advisory Committee for Nuclear Reactors (GPR) and German experts plenary meetings held on October 19th and 26th 2000.

ANNEX V. ANSWERS TO THE QUESTIONNAIRE PROVIDED BY PARTICIPATING TECHNICAL EXPERTS FROM INDIA

Answer 1:

Definition of DEC is in compliance with IAEA definition and provided below.

Accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. DEC could include severe accident conditions.

In DEC, normally multiple failures are considered. These multiple failures include single initiating events along with mitigating system failures. From external hazards considerations, some common cause may knockout some or all supporting systems. These failures are also considered under DEC (multiple failures and rare events).

In Indian regulatory document, Atomic Energy Regulatory Board (AERB) safety code, Design of Light Water Reactor Based Nuclear Power Plants (AERB/NPP-LWR/SC/D), 2015 [V-1], defines the conditions and requirements for DEC.

The dose criteria for DEC with and without core melt are provided in AERB safety code, Site Evaluation of Nuclear Facilities, AERB/NF/SC/S (Rev.1), 2014 [V-2].

Answer 2:

(a) Getting the design parameters for DEC mitigation systems;

(b) To confirm the adequacy and capabilities of DEC mitigation systems;

(c) Establishing compliance against regulatory acceptance criterion;

(d) Inputs for establishing and validating emergency operating procedures and accident management guidelines;

(e) Inputs for the DEC mitigating systems equipment qualification;

(f) To arrive at performance requirements for design of Additional Safety Systems and Complementary Safety Features;

(g) Assist in establishing and validating accident management strategies, procedures and guidelines, aid for adhering operating procedures, EOPs, SAM guidelines and human factor aspects;

(h) Confirm that modifications to the design and operation of the NPP have no significant adverse effects on safety;

(i) Predict source term and doses during accident conditions to support emergency preparedness and response.

Answer 3:

The DEC scenarios are identified by Defence-in-Depth Philosophy, operating experience feedback, PSA, type of technology (e.g. pressurized heavy water reactor (PHWR), pressurized water reactor (PWR), boiling water reactor (BWR)) and expert judgment.

(e) Design Extension Condition (DEC) without Core Melting: The initial selection of DEC sequences without core melt need to be based on the consideration of multiple failures. These multiple failures are of very low frequency. Multiple failures considered are based on an initiating event simultaneous with non-availability or beyond the capability of a safety system (or safety related systems). The failures of safety support system need to implicitly be included among the causes of failure of safety systems. DEC without core melt conditions includes postulated event along with failure of safety systems (or safety related system) provided in DiD level 3 resulting in propagation of accident to Level 4 of DiD but has not escalated to core melt condition due to provisions of additional safety systems/features.

(f) Design Extension Condition (DEC) with Core Melting: DEC with core melt include postulated event along with failure of safety systems (or safety related system) provided in DiD level 3 resulting in propagation of accident to Level 4 of DiD that had escalated to core melt condition and mitigation of consequences requires use of complementary safety features. A selection of specific sequences with core melting (severe accidents) needs to be made in order to establish the design basis for the safety features for mitigating core melting accidents, according to the plant safety objectives. These sequences need to be selected in order to represent all main physical phenomena involved in core melt sequences. Representative sequences that could challenge containment structural integrity need to be used to provide input to the design of the containment and of those safety features necessary to mitigate the consequences of such DEC.

Answer 4:

Design needs to ensure that following anticipated operational occurrences or accident conditions, the fundamental safety functions are ensured, and the reactor is maintained at safe states.

Controlled state

This is a state of the plant, following an anticipated operational occurrence or accident condition, in which the fundamental safety functions can be ensured and can be maintained for a time sufficient to implement provisions to reach a safe state /safe shutdown state.

This state is characterized by:

(a) Core is subcritical;

(b) Core heat is adequately removed;

(c) Activity discharges are within acceptable limits.

In case of a DBA, it is mandatory to reach the safe shutdown state following a controlled state. During an accident (DBA and DEC without core melt), controlled state is not to be continued for more than 24 hours.

Safe Shutdown State

Safe shutdown state is the state of the plant, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and maintained continuously.

This state is characterized by:

(a) Reactor under shutdown with desired margin below subcriticality;

(b) Continuous decay heat removal up to ultimate heat sink through designed cooling chain;

(c) Availability of containment functions. During a design basis accident, it is mandatory to reach the safe shutdown state following a controlled state.

Safe State

State of plant, following DEC without core melt, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.

This state is characterized by:

(a) Core is in long term subcritical state;

(b) Long term decay heat removal is established;

(c) Containment functions are available and activity discharges are in accordance with the acceptable limits. Design provisions need to be made to achieve and maintain safe state for 72 hours from the initiation of accident (DEC without core melt). Subsequently it is desirable to reach safe shutdown state.

Severe Accident Safe State

Severe accident safe state is a state achieved subsequent to a DEC with significant core damage or core melt phenomena. Severe accident safe state needs to be reached at the earliest after an accident initiation. It needs to be possible to maintain this state indefinitely.

During this state there is:

(a) No possibility of recriticality;

(b) Fuel or debris are continuously cooled;

(c) Uncontrolled release of radioactivity to environment is stopped ;

(d) Means to maintain above conditions are available in the long term, including critical parameter monitoring;

(e) Monitoring of radiological releases and containment conditions.

As the plant state is in design extension condition with core melt (severe accident), the severe accident safe state needs to be preferably reached within about one week from accident initiation.

Answer 5:

A best estimate approach is defined as the combination of best estimate computer code, best estimate assumptions on system availability, best estimate input conditions and boundary conditions which will give a realistic result.

Best estimate code: A combination of the best estimate models necessary to provide a realistic estimate of the overall response of the plant during an accident. Best estimate model provides a realistic estimate of a physical process to the degree consistent with the currently available data and knowledge of the phenomena concerned. The term 'best estimate code' means that the code is free of deliberate conservatism and contains sufficiently detailed models and correlations to describe the relevant processes for the transients that the code is designed to model. Best estimate type of initial and boundary conditions: Plant parameters, initial and boundary conditions plant conditions corresponds to nominal value corresponding to operating condition.

For evaluating, probable event sequences for DEC with core melt, best estimate approach is adopted.

A systematic process involving expert engineering judgment needs to be used to identify potential cliff edge effects, such as fuel dry-out, pressure boundary failure and inventory depletion and identify the dominant parameters by assessing their influence on analysis results for each acceptance criterion. Where the likelihood is considered to be high and the potential impact large sensitivity analyses need to be used to demonstrate to the extent practicable that, when more conservative assumptions are considered for dominant parameters, there are still margins with respect to cliff edge.

Answer 6:

Best estimate computer codes are considered for DEC analysis: A combination of the best estimate models necessary to provide a realistic estimate of the overall response of the plant during an accident. Best estimate model provides a realistic estimate of a physical process to the degree consistent with the currently available data and knowledge of the phenomena concerned.

All the important phenomena identified need to be represented in the models embedded in the computer code used for calculation. The models and computer code applicability to the analysed event need to be demonstrated. Model of the plant systems needs to be verified to reflect as built plant condition. User of the computer codes need to make sure that codes are appropriate for their end use.

The verification of the code design needs to be performed by means of review, inspection and audit. Independent verification process by independent group other than the group involved in the development of the code needs to be carried out. Comparisons with independent calculations need to be carried out where practicable to verify that the mathematical operations are performed correctly.

Computer code validation needs to be performed and documented for all computer codes that are used for the deterministic safety analysis of nuclear power plants.

For validation of computer codes, combination of the following approaches as applicable are acceptable:

(a) Computational checks: checking of individual model against analytical solutions or with exiting correlations derived from experimental data wherever possible;

(b) Separate effect test: Separate effect tests addresses specific phenomena that might occur on a nuclear power plant, but the test does not address the other phenomena that might occur at the same time;

(c) Integral test: Integral tests are directly related to a nuclear power plant. All or most of the relevant physical process are represented. However, these tests might be at reduced scale, use substitute material or be performed at low pressure;

(d) Operational transients: Operational transients occur either in an actual nuclear power plant or an experimental rig which represents the plant at full scale and in realistic conditions. Validation through operational transients together with NPP tests is crucial to qualify the plant model. Though it is noted that data from actual operational transients are subject to measurement as available at the time of incident;

(e) Inter code comparisons;

(f) Solving the standard/benchmark problem;

(g) Commissioning data and operational data.

Answer 7:

(a) Systems and components required for the analysis will be considered;

(b) Nominal value Initial conditions and realistic boundary conditions will be considered;

(c) Considerations on uncertainty and sensitivity as applicable. Uncertainty associated with the models and correlations, the solution scheme, model options, and data libraries. Uncertainty in representing or idealizing the real plant, such as that due to the inability to model a complex geometry accurately, three dimensional effects, scaling, control and system simplifications;

(d) The systems which survive the condition and that was not considered as failed in the event progression will be considered;

(e) Other systems will be considered in the long-term mitigation;

(f) Mostly remote control and 30 minutes minimum. Uncertainty in operator actions will also be considered;

(g) Equipment qualification: Systems credited in the analysis are undergone proper EQ;

(h) Mostly from remote control and provisions exists for easy and quick field actions;

(i) The requirement of end state for DEC is mentioned in Answer 2.

Answer 8:

Design extension condition (DEC) without core melt (multiple failure situations and rare external events) For accidents without core melt within DEC (multiple failure situations and rare external events), it is required that there is no necessity of protective measures in terms of sheltering or evacuation for people living beyond Exclusion Zone. Required control on agriculture or food banning is 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 which is 20.0mSv/ year following the event.

The following is required: Reactor is tripped following an event and maintained in a safe shutdown state; no prompt criticality following event; fuel channels integrity is maintained; containment structural integrity is ensured for those events having radiological consequences; global hydrogen concentration in the containment is maintained outside the bounds of deflagration limit on ternary diagram; local hydrogen concentration is such as to prevent local detonation.

Design extension condition (DEC) with core melt (severe accident): In case of severe accident (e.g. accidents with core melt within DEC), the release of radioactive material needs to cause no permanent relocation of population. The necessity for off-site interventions needs to be limited in area and time.

In the DEC with core melt, the containment system and its safety features need to be able to perform in extreme scenarios that include, among other things, melting of the reactor core. The containment is required to maintain its role as a leaktight barrier for a period that allows sufficient time for the implementation of off-site emergency procedures following the onset of core damage, and to prevent uncontrolled releases of radioactivity after this period.

The design is required to be such that DEC that could lead to large or early releases of radioactivity are practically eliminated. For DEC that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time are necessary for protection of the public, and sufficient time needs to be made available to implement these measures.

Prevention of re-criticality of the partial or complete core melting needs to be achieved. Sufficient cooling of core debris is to be maintained within the containment -Prevention of hydrogen detonation needs to be achieved, which could result in containment failure.

Answer 9:

Enveloping analysis in DEC without core melt and DEC with core melt have been covered as part of Safety Analysis Report (SAR). DEC with core melting analysis which are relevant to SAM guidelines have been covered in SAM guidelines Technical Basis documents.

Answer 10:

Multiple failures and Common cause failures from External Hazards.

Answer 11:

PHWR: Loss of coolant accident along with Emergency Core Cooling System (ECCS) failure is considered under DEC without significant fuel degradation. In this scenario, fuel heat up leads to sagging of Pressure tube and it sags and touches the calandria tube. This contact path establishes the heat transfer to moderator and moderator acts as heat sink. The objective of the study is to fix design parameters such as Moderator sub cooling margin, heat load. for the mitigation of the scenario and establish the capability of moderator system to mitigate the events. These analyses will also be important for SAM guideline action basis.

The above scenario, along with moderator circulation failure is considered under DEC with core melting case. The safety assessment is required to establish the calandria capability to withstand the loads and Corium cooling through Calandria vault water. These analyses will be carried out for design input and verification check of Hydrogen mitigation provisions and containment conditions. These analyses will also be important for SAM guideline action basis.

REFERENCES ANNEX V

[V-1]. AERB safety code, Design of Light Water Reactor Based Nuclear Power Plants (AERB/NPP-LWR/SC/D), 2015.

[V-2]. AERB safety code, Site Evaluation of Nuclear Facilities, AERB/NF/SC/S (Rev.1), 2014.

ANNEX VI. ANSWERS TO THE QUESTIONNAIRE PROVIDED BY PARTICIPATING TECHNICAL EXPERTS FROM THE ISLAMIC REPUBLIC OF IRAN

Answer 1:

According to Iran Nuclear Regulatory Authority (INRA) regulation titled as 'General Safety Regulation for Nuclear Facilities and Activities' issued in April 2017, Design Extension Conditions (DEC) are defined as follows:

"Accident conditions that are not considered for Design Basis Accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive materials are kept within acceptable limits. Design Extension Conditions could include sever accident conditions (Beyond design basis accidents and related design consideration)".

In the above-mentioned regulatory document, of requirements 19.2 and 19.3, INRA has emphasized:

"19.2 A list of PIEs shall be established to cover all events that could affect the safety of the plant. From this list, a set of Anticipated Operational Occurrences (AOOs) and Design Basis Accidents (DBAs) shall be selected using deterministic or probabilistic methods or a combination of both, as well as engineering judgment. The Design Basis Events (DBEs) shall be used to set the boundary conditions according to which the SSCs important to safety shall be designed, in order to demonstrate that the necessary safety functions are accomplished, and the safety objectives met.

19.3 Credible combinations of individual events, including internal and external and human induced hazards that could lead to AOOs or DBAs shall be considered in the design."

Note:

For construction of new nuclear power plant in Bushehr (WWER-1000, AES-92) in accordance with the 'technical assignment' that has to be approved by INRA, DEC for extreme internal and external events such as seismic hazard, blast wave, event combination and others has been covered.

Answer 2:

In accordance with requirement 20 of the INRA regulatory document 'General Safety Regulation for Nuclear Facilities and Activities' issued in April 2017, the objectives of DEC analysis are as follows:

(a) For further improving the safety of the NPPs by:
   (i) Enhancing the plant's capability to withstand more challenging events or conditions than those considered in the design basis,
   (ii) Minimizing radioactive releases harmful to the public and the environment as far as reasonably practicable, in such events or conditions.

(b) Plant needs to be able to fulfil confinement of radioactive materials,

(c) Demonstrate capabilities of SSCs and sufficient margin to avoid cliff edge effects (20.4)

Note: Based on the ‘technical assignment’ for the construction of new nuclear power plant (BNPP-2) the objective of BDBA analysis as follows:

(a) Prevention of initiating events development into BDBA (From DBA into BDBA);

(b) Mitigation of accidents that could not be prevented, by confinement of radioactive emissions.

Answer 3:

In accordance with Requirements 19.2 and 20.1 of the above-mentioned regulatory document, a set of AOOs, DBAs and DEC are derived, selected and justified based on a combination of deterministic safety assessments (DSA and probabilistic safety assessments (PSA) as well as engineering judgments.

Note: In accordance with the ‘technical assignment’ prepared by the Operating Organization and approved by INRA, BDBA are triggered by initiating events, the occurrence of which is not expected, but postulated for the design. The frequency of occurrence of such event is less than 10^{-6} per year.

List of BDBA with and without fuel melting (fuel melting is considered under severe accidents) has been presented in the ‘technical assignment’.

Acceptance criteria for BDBA in two categories with fuel melting and without it are considered in the Table 1.8.2.4.4 of the ‘technical assignment’ for BNPP-2.

Some Acceptance Criteria for BDBA without core degradation would be summarized as follows:

(a) The pressure in the primary and secondary system does not exceed 115% of the design value (for anticipated transient without scram (ATWS):135%);

(b) Emergency core cooling is be met: the fraction of reacted Zirconium is not more than 1% of its mass in fuel rod claddings, the maximum cladding temperature during the accident will not exceed 1200^0C;

(c) The average radial enthalpy of Nuclear fuel does not exceed its limiting value;

(d) Melting of fuel pellets is excluded.

For BDBA with core melting, criteria are based on exposure doses for critical groups.

Answer 4:

In the INRA approach, there is just controlled mode definition that is stated as follows:

“controlled mode, when a self-sustained chain reaction is stopped, reactor fuel is constantly cooled down and radioactive substances are kept within the specified boundary”.

Answer 5:

In the INRA, unfortunately, there is not any internal procedure for elaborating and conducting accident analysis with both best estimate and conservative approaches.

There is no uncertainty and sensitivity evaluations considered in INRA analysis as well as no cliff edge effects assessments and safety margins. In other words, INRA does not conduct by itself independent analyses of own certified computer codes and the assessments are outsourced to its legal consultants.

Note: INRA for some sanctions and restriction has not any access for certified codes and tools to conduct accident analysis, in this regard for independent analysis, all accident analysis of the Safety Analysis Report (SAR) was conducted by Russian consultant based on Russian tools and codes.

Answer 6:

INRA does not perform any accident analysis by its own, and it has not any certified code and analysis tools.

Regarding Code validation and verification, INRA has issued regulation entitled as 'Software Certification Process' that is mandatory for using any computer code performing accident analysis for all operating organizations in the Islamic Republic of Iran.

In performing accident analysis by Russian organization engaged in accident analysis, it is required on behalf of INRA to use validated codes approved by the Russian Regulatory Authority (Rostechnadzor).

Answer 7:

INRA by its own does not perform any DEC analysis.

Answer 8:

In INRA there is not any quantitative as well as qualitative acceptance criteria reflected in its own regulatory documents for DEC with core melting and without fuel degradation, but there are qualitative and quantitative acceptance criteria in the 'technical assignment' prepared by the operating organization and approved by Iran Nuclear Regulatory Authority, in general and details such as:

(e) Control over reactor core, pressure, emergency core cooling, clad temperature and oxidation, gas release, radial enthalpy, and others;

(f) Relevant limits on radiological release and dose limits on population and critical groups.

Answer 9:

In INRA, there is no special considerations regarding documentation of analysis of DEC, because INRA does not conduct by its own any analysis of DEC as mentioned in the above replies.

Answer 10:

Further guidance is needed for dealing with DEC analysis such as:

(a) Preparation of comprehensive guidance on performing DEC issues for example: degree on conservatism when there is no realistic data, methods of analysing results, Qualitative/Quantitative acceptance criteria for DEC, safety system and safety features issues,

(b) Basic requirements on engineering and organization solution in performing DEC analysis such as:

  (i) Maintaining the exposure level;

  (ii) Using modular and special equipment;

  (iii) Double-shell containment with ventilated Gap;

  (iv) Using an automated radiation monitoring system;

  (v) Permissible value of all leaks.

Answer 11:

This is not applicable as mentioned in the above replies.

ANNEX VII. ANSWERS TO THE QUESTIONNAIRE PROVIDED BY PARTICIPATING TECHNICAL EXPERTS FROM THE RUSSIAN FEDERATION

Answer 1:

The definition 'DEC' was not implemented in regulatory documents in the Russian Federation. The term 'beyond design basis accident' (BDBA) is defined as the following:

'*Beyond design basis accident*' is an accident caused by the initial events not taken into account for design basis accidents or accompanied by additional failures of safety system's elements above of a single failure or by the implementation of erroneous personnel decisions.

The meaning of BDBA is the same as for DEC. BDBA, according to paragraph 1.2.16 of the *General Provisions of Safety of Nuclear Power Plants* (NP-001-15), Ref. [VII-1], comprises BDBA without core damage and BDBA with severe core damage (melting). To be consistent with the title of the TECDOC term 'DEC with core melting' will be used further in this annex.

In accordance with the requirements of Ref. [VII-1], a representative set DEC, including representative DEC with core melting needs to be developed based on the results of deterministic and probabilistic analysis, taking into account all internal initiating events caused by equipment failures, floods, fires, and by the external impacts of natural and man-made origin. All locations of nuclear fuel and radioactive substances need to be taken into account.

Answer 2:

Results of DEC analyses with core melting, presented in the Safety Analysis Report (SAR), are the basis for the developing of action plans for the protection of personnel and the population in case of severe accidents, and for developing of SAMGs as well.

Results of DEC with core melting analysis presented in SAR need to confirm the compliance the design with the established requirements for DEC with core melting. It needs to be demonstrated that:

(a) radiation impact on personnel, population and the environment is limited in case of DEC, including DEC with core melting (see para. 1.2.1 of Ref. [VII-1]);

(b) containment maintains the properties of strength and leak tightness under DEC with core melting (see para. 3.6.3 of [VII-1]);

(c) formation of the critical masses in the damaged core is prevented (see para. 3.2.4 of Ref. [VII-1]);

(d) detonation of flammable gases in the containment is prevented (see para. 2.1. of Ref. [VII-2]).

Answer 3:

A general list of DEC with core melting for VVER reactors is included in *Requirements to the Content of Safety Analysis Report of Power Unit VVER reactor type* (NP-006-16), Appendix

No. 9. The final set of DEC (including DEC with core melting) which is specific for each power unit needs to be developed by licensee and presented in the SAR [VII-2].

The final (specific) set of DEC needs to be developed taking into account:

(a) an approximate list of DEC, given in Appendix No. 9 of Ref. [VII-2] (exclusion of recommended scenarios need to be justified);

(b) results of existent deterministic and probabilistic analyses;

(c) operational experience of power unit and of analogue units. (see para. 15.2.1 of Ref. [VII-2]).

The representativeness of DEC scenarios is provided by consideration of possible combinations of the severity of damage of the protective physical barriers (fuel, cladding, primary boundary, containment) as well as by consideration of operability or inoperability of safety systems and special technical means, designed for prevention and mitigation of severe accidents (see para. 1.2.16 of Ref. [VII-1]).

Classification of DEC scenario with core melting could be done in respect to operational states: reactor in shutdown condition; reactor at power level. For each of these operational states, DEC scenarios could be classified by initiating events:

(a) leaks from the primary side under containment;

(b) leaks from the primary side with containment bypass;

(c) leaks from secondary side;

(d) long-term loss of on-site and off-site energy source.

This regulatory guide '*Recommendations on the development of a final (specific) list of beyond design basis accidents, for consideration in design of nuclear power plants with VVER reactors*' (RB-150-18) includes the recommendations on how to develop the representative sets of DEC with core melting and without it. Main objectives of these recommendations are to develop the set of DEC scenarios which will allow based on the results of the analysis DEC included into that set, to develop the strategies for SAM that to undertake correct actions in any situation, including extremely unlikely scenarios [VII-5].

Answer 4:

Definition of the 'controlled state' is connected with main objective level 4 D&D: "To return the power unit into the controlled state in which the fission reaction is stopped, continuous fuel cooling and localization are provided, measures undertaken to protect the containment and the radioactive consequences of the accident are limited" (see para. 1.2.4 of Ref. [VII-1]).

Controlled safe state after severe accident is defined in more details in the SAM guidelines, as a set of criteria to finalize the severe accident management. These criteria include temperature at the outlet of the core (in case of successful in-vessel melt retention), temperature of the core catcher vessel (in case of ex-vessel melt retention), temperature in the spent fuel, no risk of detonation and deflagration in the containment, pressure in the containment is low, and there is a general improvement in the radiation situation at the NPP site.

Answer 5:

There is no definition of 'Best estimate approach' in Russian regulatory documents. Instead of that, the requirement to perform DEC analysis using realistic (non-conservative) approach is implemented (see para. 1.2.16 of Ref. [VII-1])

The initial and boundary conditions for DEC analysis need to be assumed without conservative assumptions. The computer codes used for any safety analyses need to be certified (see para. 1.2.9 of Ref. [VII-1]).

If operator's intervention is required to bring the power unit into a safe controlled state, DEC needs to be performed as for a scenario without operator actions (to define the main stages of accident course and the available time for operator's actions) and for a scenario with consideration of operator actions to confirm the efficiency of the strategy (see para. 15.2.2 of Ref. [VII-2]).

Sensitivity study is applicable to optimize SAM strategy and to indicate the potential cliff edge effects. There are indications concerning cliff edge effect in para. 1.2.4 of Ref. [VII-1] that development of the design needs to include the measures to prevent cliff edge effect. There are no indications in the regulatory guides how to fulfil this requirement, especially in relation to accidents with core melting. In practice the sensitivity study is used to identify the cliff edge effect in case of DEC with core melting to identify the margin before the damage of physical barriers under the DEC.

Answer 6:

The selection of a tool (code for accident analysis) is licensee's prerogative. According to the requirement of Article 26 of the Federal law No.170 *On the use of atomic energy* all computer codes used for safety analysis have to pass through the process of certification. This process of certification is carried out within specially established procedure. The objective of the process of certification is the assessment of sufficiency of the validation and verification process for a given computer program [VII-6]. This assessment is performed on the basis of V&V report developed by licensee. Requirements for structure and content of code V&V report are described in RD-035-2002.

The process of certification results on issuing the code's certificate, where it is presented the intended use of the code, the field of its application, restrictions for its application (if they exist), the list of parameters which were compared to experimental data and errors of calculation of these parameters. All computer codes used for safety analyses have to be certified (see para. 1.2.9 of Ref. [VII-1]).

The process of certification of computer codes started in the Russian Federation in 1999. The practice of certification of the computer codes intended for severe accident analysis is not so extensive, as for thermal hydraulic codes intended for the analysis of accident without core melting due to insufficiency of experimental data, variety and complexity of phenomenology of severe accidents.

Answer 7:

Assumptions, used for DEC analysis performance concerning:

— **Facility representation and modelling**

DEC without core melting – no special requirements concerning facility representation and modelling, realistic approach.

DEC with core melting – special severe accident codes are applied with fine nodalization of the reactor vessel to model the melt initiation and progression, as realistic as achievable at the moment, according state of art knowledge.

— **Initial and boundary conditions**

Realistic initial and boundary condition without special conservative assumptions.

— **Considerations on uncertainty and sensitivity as applicable**

It is recommended to conduct uncertainty and sensitivity analysis. Activity for development of methodological recommendations concerning the uncertainty analysis for severe accidents with core melting is under progress. Sensitivity study is performed to clarify and to assess the influence for assessment of the phenomena which are not well investigated.

— **Availability of systems and components**

According to the requirements p. 1.2.19 of Ref. [VII-1], the mitigation of consequences of DEC, including DEC with core melting, needs to be provided using special technical features designed for DEC and also using other applicable technical means regardless their intended purpose and by means of organizational measures including SAMGs and protection plan of personnel and public against consequences of those accidents.

— **Systems credited in the analysis (use of safety features and other systems)**

Additional failures of equipment besides those that are defined by scenario of DEC with core melting are not considered (see para. 1.2.11 of Ref. [VII-1]).

— **Operator actions (time and action)**

If operator actions are required to bring the power unit in a safe controlled state, the DEC analyses need to be performed as for scenario without operator actions (to define the main stages of accident course and the available time operator's actions) and for scenario taking into account operator actions to confirm the effectiveness of accident management (see para. 15.2.2 of Ref. [VII-2]).

If safety analysis is performed considering of operator actions, time necessary for preparation and performance of these actions have to be taken into account.

— **Equipment qualification**

Systems (elements) designed for DEC and could be called for operation within the first three days (not less than 3 days) after initial event need to be qualified as systems (components) are important for safety (safety class 3) (see para. 2.5 of Ref. [VII-1]).

— **Operator action in a harsh environment**

Operator actions in a harsh environment taking into account multi-unit accident need to be foreseen in para. 4.5.2 of Ref. [VII-1].

Time necessary to perform the operator actions in harsh condition could be assessed based on the results of emergency drills.

— **Analysis end state**

In General, end state for DEC with core melting is a state at which main safety functions (subcriticality, fuel cooling, localization) are provided, measures for protection of the containment are taken and radiation consequences of accident are limited (see para. 1.2.4 of Ref. [VII-1])

In practice, the duration of analyses for DEC with core melting is defined by its objectives. Criteria of analyses end state are different to demonstrate subcriticality or the melt stabilization or hydrogen safety.

Answer 8:

General requirement:

(a) the results of DEC with core melting analysis needs to demonstrate the achievement of a controlled safe state;

(b) the radiological consequences for BDBA are restricted.

It needs to be demonstrated that:

(a) Absorbed dose to the population at the border and beyond of the protection zone does not exceed the values established by safety standards for decision-making on protective measures in case of a radioactive accident with contamination of the territory (see para. 3.3.2 of Ref. [VII-4]);

(b) Containment maintains their functions (strength and leak tightness) under the DEC with core melting (see para. 3.6.3 of Ref. [VII-1]).

Detonation of the flammable gases is excluded for DEC with core melting (see para. 2.1 of Ref. [VII-3]).

Recriticality of the damaged core under DEC with core melting is prevented (see para. 3.2.4 of Ref. [VII-1]).

Answer 9:

The results of DEC analysis, including the result of analyses for representative scenario with core melting need to be presented in Chapter 15 of SAR. These results should be supplemented by assessments of scenario's probability and the radioactive impacts.

The assessment of the equivalent dose for the population regarding BDBA needs to be performed for the critical group of population under the most unfavourable weather conditions (with a 95% coverage) typical for the area of site.

For BDBA with core melting additional information need to be presented:

(a) time schedule of the fuel degradation from the initial phase to the final condition of melt stabilization;

(b) speed of generation of combustible gases at all stages of the accident;

(c) composition of the vapor-gas medium in the compartments of the containment;

(d) proof of the subcriticality of the damaged core at the different stages of severe accidents;

(e) evolution of the parameters (P, T) in the containment, considering all mass and energy sources;

(f) set of plots of representative parameter evolution to prove safe stabilization of the corium in the core catcher:

  (i) temperature and composition of the melt in the core catcher;

  (ii) heat flux from the corium to the wall compare with critical heat flux (for the new design);

  (iii) confirmation of the melt inversion;

  (iv) confirmation of the melt stabilization.

Answer 10:

If the probability of a large radioactive release is more than 10^{-7}, additional technical solutions (including special technical features for severe accident management) need to be provided in order to reduce the probability of accidents and to mitigate their consequences (see para. 1.2.17 of Ref. [VII-1]).

For BDBA, which are not excluded due to inherent properties of the reactor and the principles of the design, regardless of their probability, organizational measures need to be developed to manage such beyond-design accidents, including measures to reduce the radioactive impact on the personnel, public and on the environment, including implementation of Emergency Plan (see para. 1.2.19 of Ref. [VII-1]).

Special technical means designed for DEC, including core melting need to be able to perform their functions considering external hazards (earthquakes, tornadoes, floodingss and other possible phenomena in the site area), external human-induced hazards and internal hazards inducing mechanical, thermal, chemical and other loads arising from DEC itself for which the operation of those technical means are required (see para. 3.1.8 of Ref.). Design provisions need to be considered in the design to protect the special technical means designed for DEC

from common cause failures by implementing the principles of diversity, redundancy and independency (see para. 3.1.9 of Ref. [VII-1]).

Sufficiency of special technical means dedicated for DEC need to be proved for multi-unit accident (see para. 3.1.13 of Ref. [VII-1]).

The possibility of technical diagnostics (checking) of the state of dedicated special technical means for DEC, need to be provided (see para. 3.1.14 of Ref. [VII-1]).

Answer 11:

The requirements for the presentation of analysis results for postulated severe accidents are largely similar to the requirements for the presentation of analysis results for accidents without core melting.

According to para. 15.2.2 of Ref. [VII-2], it is required to submitted in Chapter 15 of SAR for any BDBA safety analysis:

(a) time sequence of the events and phenomena arising in the course of accidents;

(b) text description of the course of the accidents;

(c) plots of representative parameters vs. time as in reactor and in the containment.

Additional requirements for presentation of the results of analysis for DEC with core melting depend on the objectives of the analysis and on the postulated scenario. Taking into account the safety features are considered in the design of new WWER-1200 (core catcher), it should be proven for DEC with core melting:

(a) safe corium stabilization (evolution of the corium temperature as in reactor and in the core catcher) if the course of accident resulted on corium release in the core catcher;

(b) reasonable confidence of margin before critical heat flux at the wall of the core catcher;

(c) melt inversion in the core catcher

(d) subcriticality of the damaged core at all stages of severe accidents;

(e) prevention of hydrogen detonation;

(f) strength and leak tightness of the containment;

(g) limitation of the radiological consequences (no protection actions beyond the boundary 25 km).

REFERENCES

[VII-1]. SCIENTIFIC AND TECHNICAL CENTER FOR NUCLEAR AND RADIATION SAFETY, General Provisions of Safety of Nuclear Power Plants, NP-001-15, Moscow (2016).

[VII-2]. SCIENTIFIC AND TECHNICAL CENTER FOR NUCLEAR AND RADIATION SAFETY, Requirements to the Content of Safety Analysis Report of Power Unit VVER reactor type, NP-006-16, Moscow (2017)

[VII-3]. SCIENTIFIC AND TECHNICAL CENTER FOR NUCLEAR AND RADIATION SAFETY, Rules of Ensuring of Hydrogen Explosion Protection on Nuclear Power Plant, NP-040-02, Moscow (2003)

[VII-4]. SCIENTIFIC AND TECHNICAL CENTER FOR NUCLEAR AND RADIATION SAFETY, Siting of Nuclear Power Plants. Main Criteria and Requirements on Safety Ensuring, NP-032-01, Moscow (2002)

[VII-5]. SCIENTIFIC AND TECHNICAL CENTER FOR NUCLEAR AND RADIATION SAFETY, Recommendations on the development of a final list of beyond design basis accidents to be taken into account in the design of nuclear power plants with VVER-type reactors, RB-150-18, Moscow (2018).

[VII-6]. DUMA, Federal Law No. 170-Fz of November 21, 1995, on the use of Atomic Energy.
www.wto.org/english/thewto_e/acc_e/rus_e/WTACCRUS58_LEG_269.pdf

ANNEX VIII. ANSWERS TO THE QUESTIONNAIRE PROVIDED BY PARTICIPATING TECHNICAL EXPERTS FROM THE UNITED STATES OF AMERICA

Answer 1:

While the United States Nuclear Regulatory Commission (NRC) does not use the term DEC in its regulatory infrastructure, it has regulations [VIII-1] for the following beyond design basis events:

(a) combustible gas control [VIII-2];

(b) anticipated transient without scram (ATWS) [VIII-3];

(c) station blackout (SBO) [VIII-4];

(d) effects on the facility of a large commercial aircraft impact [VIII-5];

(e) mitigation of beyond design basis external events from natural phenomena and mitigation of extensive damage associated with loss of large areas of the plant due to explosions or fire [VIII-6].

Applicants need also to include a description and analysis of design features for the prevention and mitigation of severe accidents and address challenges to containment integrity from phenomena such as core-concrete interaction, steam explosion, high-pressure core melt ejection, hydrogen combustion, and containment bypass ([VIII-7], [VIII-8]).

Answer 2:

Applicants/Licensees may use the analyses of beyond design basis events (1) to confirm that features, credited for the design extension conditions, have the requested performances to meet the Commission Safety Goals on LRF [VIII-9] and containment performance [VIII-10]; (2) to assist in establishing and validating emergency operating procedures and accident management guidelines; (3) to provide the environmental conditions for equipment survivability analysis; (4) to identify the SSCs to be included in the reliability assurance program (RAP) or subject to regulatory control of non-safety systems (RTNSS) [VIII-11], (5) to provide input for analysis of severe accident mitigation alternatives [VIII-12]; (6) as input to the source term calculations used in off-site emergency planning.

Answer 3:

The identification of beyond-design-basis events warranting regulatory actions were identified as potential vulnerabilities through operating experience, Probabilistic Risk Assessments (PRA), and security studies. Expert judgement is inherently included in each evaluation.

DEC without significant fuel degradation are generally classified by sequence (e.g. ATWS, SBO) while DEC with core melting are generally classified in terms of the physical phenomena that may occur during the course of core melt progression (e.g. core-concrete interaction, steam explosion).

Answer 4:

For SBO, safe shutdown means bringing the plant to shutdown conditions specified in plant technical specifications as Hot Standby or Hot Shutdown, as appropriate (plants have the option of maintaining the reactor coolant system at normal operating temperatures or at reduced temperatures) [VIII-13].

Aircraft impact assessments need to show that, with reduced use of operator actions the reactor core remains cooled, or the containment remains intact; and spent fuel cooling or spent fuel pool integrity is maintained. Assessments of beyond design basis external events from natural phenomena and of extensive damage associated with loss of large areas need to include strategies to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities. The latter need also to address actions to minimize radiological release.

While not specifically identified as a 'safe state', containment performance goals specify that for more likely severe accident challenges, the containment function is to provide a leaktight barrier for 24 hours. After 24 hours, the containment function needs to continue to provide a barrier against uncontrolled release of radionuclides.

Answer 5:

NRC does not provide specific guidance on how to perform analysis for DEC with core melting, but generally uses the following:

(a) The best estimate approach is appropriate to reflect a realistic plant response. It includes model parameters set to obtain a good fit to experimental results and the design dimensions of the reactor. The level of confidence is commensurate with the representativeness of the experiments to the design being analysed;

(b) Sensitivity and uncertainty studies are expected over a realistic range of input. In some instances, conservative values can be used in the base case to simplify uncertainty calculations. Examples of uncertainty and sensitivity studies can be found in NUREG/CR-6849, 'Analysis of In-Vessel Retention and Ex-Vessel Fuel Coolant Interaction for AP1000.' [VIII-17];

(c) The sensitivity analysis needs to address cliff edge effects. Safety margins are commensurate with confidence in assumptions.

Answer 6:

Regarding DEC with core melting, the NRC does not provide specific guidance on computer code selection, verification, or validation, but all new reactor applicants have used either MELCOR or MAAP to analyse severe accident progression, and the NRC has extensive experience with and confidence in both of these codes. Additionally, the NRC runs independent MELCOR confirmatory calculations for select accident sequences to provide additional validation of the submittal [VIII-14]. MELCOR is a well-established severe accident code sponsored by the NRC and validated and assessed through the Cooperative Severe Accident Research Program (CSARP) [VIII-15].

Answer 7:

When demonstrating combustible gas control for a beyond-design-basis accident, the applicant needs to use the amount of hydrogen equivalent to that generated from a 100% fuel-clad coolant reaction.

For other phenomenon associated with DEC with core melting, the NRC does not provide specific guidance on assumptions, but generally uses the following:

(a) Facility representation and modelling (geometry) – best estimate, nominal;

(b) Initial and boundary conditions – best estimate, realistic;

(c) Considerations on uncertainty and sensitivity are addressed by performing sensitivity (change one parameter at a time) and uncertainty (vary all parameters) over a realistic range of input and determine probability of failure. Applicant may choose to use conservatisms to simplify uncertainty analysis;

(d) Availability of systems and components – allowed if not failed in accident sequence and it's demonstrated they function under severe accident environment; applicants may conservatively choose to assume they fail to reduce uncertainty analysis;

(e) Systems credited in the analysis – allowed if not failed in accident sequence and it's demonstrated they function under severe accident environment; applicants may conservatively choose to assume they fail to reduce uncertainty analysis;

(f) Operator actions – best estimate;

(g) Equipment qualification – In the US, severe accident design features are demonstrated to survive the severe accident conditions, which is referred to as equipment survivability;

(h) Operator action in a harsh environment – best estimate;

(i) Analysis end state – For severe accidents, demonstrate containment performance goals (described in Question 8) are met.

Answer 8:

NRC requirements for specified beyond-design-basis events (e.g. SBO, ATWS) generally require the addition of plant capabilities to provide increased confidence that a plant can be brought to and maintained at conditions specified in plant technical specifications as Hot Standby or Hot Shutdown. PRA evaluations may categorize scenarios by those with success paths for critical safety functions related to reactivity and core cooling and those progressing to core damage. The estimated frequency and consequences of events involving significant core damage are evaluated against the NRC's new reactor safety goals:

(a) Large release frequency less than 10-6 reactor/year;

(b) Conditional containment failure probability less than 0.1, given core damage;

(c) For the more likely severe accident challenges, the containment needs to provide a leaktight barrier for 24 hours. After 24 hours, the containment needs to continue to provide a barrier against uncontrolled release of radionuclides.

Answer 9:

The analysis description and results are documented in the final safety analysis report (FSAR), with possibly separate supporting documentation available for audit.

Answer 10:

No, all considerations have been discussed in previous responses.

Answer 11:

An example for the AP-1000 design related to a beyond-design-basis event without significant fuel degradation relates to capabilities added to address ATWS. The diverse instrumentation and control system is a non-safety related instrumentation and control system and provides a diverse and independent method for tripping the reactor and performing several engineered safety features in order to meet the requirements of 10 CFR 50.62.

The AP-1000 design includes several features to address possible severe accident scenarios. These features include a reflective reactor vessel insulation system that provides an engineered flow path to allow water ingress and venting of steam for external reactor vessel cooling in the event of a severe accident involving core relocation to the lower plenum or the reactor vessel. The AP1000 containment is also provided with non-safety-related hydrogen igniters to control the concentration of combustible gases. Within the severe accident management guidelines for AP1000, additional procedures were defined for accident management in the in-vessel severe accident phase and the ex-vessel severe accident phase. Methods of injecting water into the containment were added (e.g. providing makeup to overflow the in-containment refuelling water storage tank by the decay heat removal system). The use of containment spray was also identified as a severe accident strategy (e.g. injecting water into containment and containment heat removal) [VIII-16].

REFERENCES

[VIII-1]. NUCLEAR REGULATORY COMMISSION, Title 10, Code of Federal Regulations, Washington DC, USA (2020)

[VIII-2]. NUCLEAR REGULATORY COMMISSION, § 50.44 Combustible gas control for nuclear power reactors, Washington DC, USA (2017)

[VIII-3]. NUCLEAR REGULATORY COMMISSION, § 50.62 Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants, Washington DC, USA (2017)

[VIII-4]. NUCLEAR REGULATORY COMMISSION, § 50.63 Loss of all alternating current power, Washington DC, USA (2017)

[VIII-5]. NUCLEAR REGULATORY COMMISSION, § 50.150 Aircraft impact assessment, Washington DC, USA (2017)

[VIII-6]. NUCLEAR REGULATORY COMMISSION, § 50.155 Mitigation of beyond-design-basis events. Washington DC, USA

[VIII-7]. NUCLEAR REGULATORY COMMISSION, § 52.47 Contents of applications; technical information. Washington DC, USA

[VIII-8]. NUCLEAR REGULATORY COMMISSION, § 52.79 Contents of applications; technical information in final safety analysis report. Washington DC, USA

[VIII-9]. NUCLEAR REGULATORY COMMISSION, Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationships to Current Regulatory Requirements. SECY-90-16, Washington DC, USA (1990)

[VIII-10]. NUCLEAR REGULATORY COMMISSION, Policy, Technical, and Licensing Issues Pertinent to Evolutionary and Advanced Light-Water Reactor Designs, SECY-93-087, Washington DC, USA (1993)

[VIII-11]. NUCLEAR REGULATORY COMMISSION, Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs, SECY-95-132, Washington DC, USA (1995)

[VIII-12]. NUCLEAR REGULATORY COMMISSION, Environmental report-standard design certification, 10 CFR 51.55, Washington DC, USA (2017)

[VIII-13]. NUCLEAR REGULATORY COMMISSION, § 50.2 Definitions, Washington DC, USA (2017)

[VIII-14]. NUCLEAR REGULATORY COMMISSION, Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors, NUREG-0800, Washington DC, USA (2015)

[VIII-15]. SANDIA NATIONAL LABORATORIES, MELCOR Computer Code Manuals, Vol. 3: MELCOR Assessment Problems, Version 2.1.7347 2015, Albuquerque, New Mexico, USA (2015)

[VIII-16]. NUCLEAR REGULATORY COMMISSION, Severe Accident Phenomena Treatment, Probabilistic Risk Assessment AP1000 Design Control Document, Revision 19, ML11171A405

[VIII-17]. NUCLEAR REGULATORY COMMISSION, Analysis of In-Vessel Retention and Ex-Vessel Fuel Coolant Interaction for AP1000, NUREG/CR-6849, Washington DC, USA (2004).

ANNEX IX. DEC APPROACH FORMS FILLED BY PARTICIPATING TECHNICAL EXPERTS

Annex IX depicts condensed forms that have been filled in by participating technical experts from Bulgaria, Canada, Finland, France, Germany, India, the Islamic Republic of Iran, Japan, Romania, the Russian Federation, Sweden and the United States of America, and provided at the end of or after the Technical Meeting on Current Approaches in Member States to Analysis of Design Extension Conditions for New Nuclear Power Plants, organized by IAEA on 19–23 March 2018. The relevant answers are indicated either with an **X** or a brief explanatory text**.**

IX-1. DEC APPROACH IN BULGARIA

TABLE IX-1.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

Topic	Option 1	Option 2	Option 3
List of sequences	Generic (vendor and/or IAEA list…)	Justified by deterministic systematic methodology **X**	PSA based **X**
Type of DEC-A sequences (several possibilities)	DBA+CCF **X**	CCF as initiating event	Rare single events **X**
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF **X**	DEC-A feature only
Proof of operability	Survivability	Qualification + engineering assessment **X**	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criteria	Yes	No **X**	

TABLE IX-1.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION (cont.)

Topic	Option 1	Option 2	Option 3
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (2 h) **X**	No	
Off-site mobile equipment	Yes (time delay?) **X**	No	
Means of connecting mobile equipment included in the design	Yes (additionally, it is installed) **X**	No	
Operator action delay	BE	Same as DBA **X**	
Safety criteria	No impact on population **X**	Limited impact on population (specify area and time)	

TABLE IX-1.2. DEC WITH CORE MELTING

Topic	Option 1	Option 2	Option 3
List of sequences	Generic	Based on physical phenomenon to be analysed **X**	PSA based
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any system not affected **X**	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified
Proof of operability	Survivability	Qualification + engineering assessment **X**	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criteria	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (2 h) **X**	No	
Off-site mobile equipment	Yes (time delay?) **X**	No	
Means of connecting mobile equipment included in the design	Yes (additionally, it is installed) **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population	Limited impact on population (specify area and time) **X**	Practical elimination of large OR early releases **X**

IX-2. DEC APPROACH IN CANADA

Canada does not have separate requirements for DEC without significant fuel degradation (DEC-A) and DEC with fuel melting (DEC-B). Events are categorized primarily by their frequency for the purposes of design and analysis. It is not considered advisable to categorize events on the basis of the event consequences which are an output from the design and analysis, not an input. "Events that do not lead to fuel melting shall not lead to fuel melting" is a circular requirement.

TABLE IX-2.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic (vendor and/or IAEA list…) **X**	Justified by deterministic systematic methodology **X**	PSA based **X**
	Canada permits use of all of these options. Canadian requirements are based on IAEA SSR-2/1 (Rev. 1) which requires: "*A set of design extension conditions shall be derived on the basis of* ***engineering judgement, deterministic assessments and probabilistic assessments*** *for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures.*"		
Type of DEC-A sequences (several possibilities)	DBA+CCF **X**	CCF as initiating event **X**	Rare single events **X**
	Canada uses identification based on the list from item 1 above. That would include these options and multiple failures from any cause, not limited to CCF, e.g. including unidentified pre-existing failures.		
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes	No	Partly **X**
	Sensitivity analysis is not a specific requirement but would be used to demonstrate adequate margin to cliff edge effects.		
Quantification of uncertainties	Yes	No	Partly **X**
	Quantification of uncertainties is not as rigorous as for DBA, but major sources of uncertainty are identified and taken into account by adding conservatism, or sensitivity analysis.		
Systems credited	Any **X**	DEC-A feature + DBA systems not affected by CCF	DEC-A feature only
	Equipment can be credited if there is reasonable confidence of its operability, through survivability assessments, time for operator action, appropriate training, etc.		
Proof of operability	Survivability **X**	Qualification	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes	No	Case by case **X**
	Design of equipment for DEC needs to provide reasonable confidence of operability in the conditions where it may be required. Safety analysis for DEC can credit equipment with demonstrated survivability.		
Power supply	Main diesel generators (DBA)	Diversified power source	Case by case **X**
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	

TABLE IX-2.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION (cont.)

Topic	Option 1	Option 2	Option 3
On-site mobile equipment	Yes (time delay minimum of 8 hours) **X**	No	
Off-site mobile equipment	Yes (time delay minimum of 72 hours) **X**	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population	Limited impact on population (specify area and time) **X**	
	Canadian requirement for new NPPs is based on IAEA SSR-2/1 (Rev. 1) paragraphs 5.31 and 5.31A and is not specific in terms of area or time. Canadian requirement reads: "*The design shall be such that plant states that could lead to significant radioactive releases are practically eliminated. For plant states that are not practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.*"		

Canada does not have separate requirements for DEC without significant fuel degradation (DEC-A) and DEC with fuel melting (DEC-B). For additional details, see DEC-A responses.

TABLE IX-2.2. DEC WITH CORE MELTING

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic **X**	Based on physical phenomenon to be analysed **X**	PSA based **X**
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes	No	Partly **X**
Quantification of uncertainties	Yes	No	Partly **X**
Systems credited	Any system not affected **X**	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified
Proof of operability	Survivability **X**	Qualification	
Seismic requirement	Yes	No	Case by case **X**
Protection against extreme external hazards	Yes	No	Case by case **X**
Power supply	Main diesel generators (DBA)	Diversified power source	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (time delay minimum of 8 hours) **X**	No	
Off-site mobile equipment	Yes (time delay minimum of 72 hours) **X**	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population	Limited impact on population (specify area and time) **X**	

IX-3. DEC APPROACH IN FINLAND

TABLE IX-3.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic (vendor and/or IAEA list…) **X**	Justified by deterministic methodology + PSA check	PSA based
Type of DEC-A sequences (several possibilities)	DBA+CCF	CCF as initiating event **X**	Rare single events **X**
Code model	BE **X**	Conservative **X**	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%) **X**	
Boundary conditions (System performances)	BE **X**	Min/Max **X**	
Additional sensitivity analysis	Yes (conservative) **X**	No	If needed **X**
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF	DEC-A feature only **X**
Proof of operability	Survivability	Qualification **X**	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes **X**	No	
Preventive maintenance	Yes **X**	No	
On-site mobile equipment	Yes (time delay?)	No **X**	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes	No **X**	
Operator action delay	BE	Same as DBA	Needs to be justified **X**
Safety criteria	No impact on population	Limited impact on population (specify area and time) **X**	

TABLE IX-3.2. DEC WITH CORE MELTING

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic	Based on physical phenomenon to be analysed **X**	PSA based **X**
Code model	BE **X**	Conservative **X**	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%) **X**	
Boundary conditions (System performances)	BE **X**	Min/Max **X**	
Additional sensitivity analysis	Yes (conservative analysis + if needed) **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any system not affected	Dedicated to DEC-B only **X**	Dedicated to DEC-B exceptions to be justified
Proof of operability	Survivability	Qualification **X**	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes **X**	No	
Preventive maintenance	Yes **X**	No	
On-site mobile equipment	Yes (time delay?)	No **X**	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes	No **X**	
Operator action delay	BE	Same as DBA	Needs to be justified **X**
Safety criteria	No impact on population	Limited impact on population **X**	

IX-4. DEC APPROACH IN FRANCE

TABLE IX-3.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic (vendor and/or IAEA list…)	Justified by deterministic methodology + PSA check **X**	PSA based
Type of DEC-A sequences (several possibilities)	AOO+CCF **X**	CCF as initiating event **X**	Rare single events
Code model	BE **X**	Conservative	
Initial conditions	BE	Conservative for parameters of major influence **X**	
Boundary conditions (System performances)	BE	Min/Max **X**	
Additional sensitivity analysis	Yes	No **X**	
Quantification of uncertainties	Yes	No **X**	Implicitly taken into account by choosing bounding values for dominant parameters (95% coverage rate). **X**
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF **X**	DEC-A feature only
Proof of operability	Survivability	Qualification **X**	
Seismic requirement	Yes	No	**Case by case** **X**
Protection against extreme external hazards	Yes	No	Case by case **X**
Power supply	Main diesel generators (DBA)	Diversified power source (for SBO situation) **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (with delay compatible with the time required for the implementation) **X**	No	
Off-site mobile equipment	Yes (with delay compatible with the time required for the implementation) **X**	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE	Same as DBA **X**	
Safety criteria	No countermeasures needed **X**	Limited impact on population (specify area and time)	

TABLE IX-3.2. DEC WITH CORE MELTING

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic	Based on physical phenomenon to be analysed **X**	PSA based
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any system not affected	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified **X**
Proof of operability	Survivability	Qualification **X**	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (with delay compatible with the time required for the implementation) **X**	No	
Off-site mobile equipment	Yes (with delay compatible with the time required for the implementation) **X**	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE	Same as DBA **X**	
Safety criteria	No impact on population	Limited impact on population **X**	No evacuation before 24h Evacuation: max 3 km Confinement and iodine prophylaxis: max 5km No permanent relocation **X**
Safety Classification of DEC features	Yes **X**	No	Class3 **X**

IX-5. DEC APPROACH IN GERMANY

TABLE IX-5.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic (vendor and/or IAEA list…)	Justified by deterministic systematic methodology **X**	PSA based **X**
Type of DEC-A sequences (several possibilities)	DBA+CCF **X**	CCF as initiating event	Rare single events
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes	No **Up to now no, but underway**	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF **X**	DEC-A feature only
Proof of operability	Survivability **X**	Qualification	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA) **X**	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (time delay?) **X (up to 10 hours)**	No	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population **X**	Limited impact on population (specify area and time)	

TABLE IX-5.2. DEC WITH CORE MELTING

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic	Based on physical phenomenon to be analysed	PSA based **X**
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes	No Up to now no, but underway **X**	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any system not affected **X**	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified
Proof of operability	Survivability **X**	Qualification	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA) **X**	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (time delay?) **X (up to 10 hours)**	No	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population	Limited impact on population (specify area and time) **X (ALARA principle)**	

IX-6. DEC APPROACH IN INDIA

TABLE IX-6.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

Topic	Option 1	Option 2	Option 3
List of sequences	Generic (vendor and/or IAEA list…)	Justified by deterministic systematic methodology **X**	PSA based
Type of DEC-A sequences (several possibilities)	DBA+CCF **X**	CCF as initiating event	Rare single events
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF **X**	DEC-A feature only
Proof of operability	Survivability	Qualification **X**	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes	No	Case by case **X**
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (time delay?) >24 hours **X**	No	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes **X**	No	

TABLE IX-6.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION (cont.)

Topic	Option 1	Option 2	Option 3
Operator action delay	BE	Same as DBA **X**	
Safety criteria	No impact on population	Limited impact on population (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. The target for effective dose calculated using realistic methodology shall be less than 20.0 mSv/ year following the event.) (specify area and time) **X**	

TABLE IX-6.2. DEC WITH CORE MELTING

Topic	Option 1	Option 2	Option 3
List of sequences	Generic **X**	Based on physical phenomenon to be analysed	PSA based
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any system not affected **X**	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified
Proof of operability	Survivability **X**	Qualification	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes	No **X**	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (time delay?) >24 hours **X**	No	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population	Limited impact on population (specify area and time) **The release of radioactive materials should cause no permanent relocation of population. The need for offsite interventions should be limited in area and time.** **X**	

IX-7. DEC APPROACH IN THE ISLAMIC REPUBLIC OF IRAN

TABLE IX-7.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

Topic	Option 1	Option 2	Option 3
List of sequences	Generic (vendor and/or IAEA list…) **X**	Justified by deterministic systematic methodology	PSA based
Type of DEC-A sequences (several possibilities)	DBA+CCF **X**	CCF as initiating event	Rare single events
Code model	BE	Conservative **X**	
Initial conditions	BE	Conservative for parameters of major influence (95%/95%) **X**	
Boundary conditions (System performances)	BE	Min/Max **X**	
Additional sensitivity analysis	Yes	No **X**	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF **X**	DEC-A feature only
Proof of operability	Survivability	Qualification **X**	
Seismic requirement	Yes	No **X**	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes **X**	No	
On-site mobile equipment	Yes (time delay?) **X**	No	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE	Same as DBA **X**	
Safety criteria	No impact on population **X**	Limited impact on population (specify area and time)	

TABLE IX-7.2. DEC WITH CORE MELTING

Topic	Option 1	Option 2	Option 3
List of sequences	Generic	Based on physical phenomenon to be analysed **X**	PSA based
Code model	BE	Conservative **X**	
Initial conditions	BE	Conservative for parameters of major influence (95%/95%) **X**	
Boundary conditions (System performances)	BE	Min/Max **X**	
Additional sensitivity analysis	Yes	No **X**	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any system not affected	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified **X**
Proof of operability	Survivability	Qualification **X**	
Seismic requirement	Yes	No **X**	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance		No	
On-site mobile equipment	Yes (time delay?) **X**	No	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE	Same as DBA **X**	
Safety criteria	No impact on population **X**	Limited impact on population (specify area and time)	

IX-8. DEC APPROACH IN JAPAN (TEPCO)

TABLE IX-8.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

Topic	Option 1	Option 2	Option 3
List of sequences	Generic (vendor and/or IAEA list…)	Justified by deterministic systematic methodology	PSA based (Certainly Sequences to include to DEC-A are provided by NRA guide. PSA is used for reflecting Plant specific sequences additionally.) **X**
Type of DEC-A sequences (several possibilities)	DBA+CCF	CCF as initiating event	Rare single events (for IE only) IE: single event except ATWS, Mitigation system failure: CCF Example TQUV: AOO + all ECCS failure TQUX: AOO + ECCS (High-pressure only) + ADS failure SBO: AOO + EDG failure ISLOCA: Human error Small LOCA: s-LOCA + ECCS failure ATWS: AOO (with MSIV close) + scrum failure **X**
Code model	BE	Conservative	BE **X**
Initial conditions	BE	Conservative for parameters of major influence (95%/95%)	BE (using average value for parameters) **X**
Boundary conditions (System performances)	BE	Min/Max	BE **X**
Additional sensitivity analysis	Yes	No	Yes **X**
Quantification of uncertainties	Yes	No	Yes **X**

TABLE IX-8.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION (cont.)

Topic	Option 1	Option 2	Option 3
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF	DEC-A feature + DBA systems not affected by CCF **X**
Proof of operability	Survivability	Qualification	Survivability **X**
Seismic requirement	Yes	No	Yes **X**
Protection against extreme external hazards	Yes	No	Yes **X**
Power supply	Main diesel generators (DBA)	Diversified power source	Diversified power source **X**
Single failure criterion	Yes	No	No (Other requirements for DEC equipment Core Injection and Power supply (AC); Permanent + mobile. Mobile; keep spare vehicle.) **X**
Preventive maintenance	Yes	No	Yes **X**
On-site mobile equipment	Yes (time delay?)	No	Yes (time delay:12h [TEPCO's case]) **X**
Off-site mobile equipment	Yes (time delay?)	No	No **X**
Means of connecting mobile equipment included in the design	Yes	No	Yes **X**
Operator action delay	BE	Same as DBA	BE **X**
Safety criteria	No impact on population	Limited impact on population (specify area and time)	Fuel: PCT 1200 degree ECR 15% Dose: 5mSv on site boundary (venting case only) **X**

TABLE IX-8.2. DEC WITH CORE MELTING

Topic	Option 1	Option 2	Option 3
List of sequences	Generic	Based on physical phenomenon to be analysed	PSA based (Certainly Sequences to include to DEC-B are provided by NRA guide. PSA is used for reflecting Plant specific sequences additionally.) **X**
Code model	BE	Conservative	BE **X**
Initial conditions	BE	Conservative for parameters of major influence (95%/95%)	BE (using average value for parameters) **X**
Boundary conditions (System performances)	BE	Min/Max	BE **X**
Additional sensitivity analysis	Yes	No	Yes **X**
Quantification of uncertainties	Yes	No	Yes **X**
Systems credited	Any system not affected	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified **X**
Proof of operability	Survivability	Qualification	Survivability **X**
Seismic requirement	Yes	No	Yes **X**
Protection against extreme external hazards	Yes	No	Yes **X**
Power supply	Main diesel generators (DBA)	Diversified power source	Diversified power source **X**
Single failure criterion	Yes	No	No (Other requirements for DEC equipment Core Injection and AC Power supply; Permanent + mobile. Mobile; securement spare mobile) **X**
Preventive maintenance	Yes	No	Yes **X**
On-site mobile equipment	Yes (time delay?)	No	Yes (time delay:12h [TEPCO's case]) **X**

TABLE IX-8.2. DEC WITH CORE MELTING (cont.)

Topic	Option 1	Option 2	Option 3
Off-site mobile equipment	Yes (time delay?)	No	No **X**
Means of connecting mobile equipment included in the design	Yes	No	Yes **X**
Operator action delay	BE	Same as DBA	BE **X**
Safety criteria	No impact on population	Limited impact on population (specify area and time)	PCV Pressure: 620 kPa (2PD), Temp: 200 degree Total Cs release: less than 100 TBq Direct containment heating: RPV depressurize molten corium-concrete interaction: erosion does not reach PCV bottom liner Fuel coolant interaction: no PCV failure by pressure spike Hydrogen explosion: Flammability limit **X**

IX-9. DEC APPROACH IN ROMANIA

TABLE IX-9.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic (vendor and/or IAEA list…)	Justified by deterministic systematic methodology	PSA based **X**
Type of DEC-A sequences (several possibilities)	DBA+CCF **X**	CCF as initiating event **X**	Rare single events
Code model	BE **X** *In the limits of MAAP4-CANDU® code*	Conservative	
Initial conditions	BE	Conservative for parameters of major influence (95%/95%) **X**	
Boundary conditions (System performances)	BE X *At the most probable values*	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF **X**	DEC-A feature only
Proof of operability	Survivability	Qualification **X**	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes	No	Case by case **X**
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No	
On-site mobile equipment	Yes (time delay?) **X** *According to the tests' results*	No	
Off-site mobile equipment	Yes (time delay?)	No **X**	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population	Limited impact on population (specify area and time) **X** *Dose limits (at the exclusion zone limit), based on accident sequence frequency – established by regulatory requirements in NSN-02*	

TABLE IX-9.2. DEC WITH CORE MELTING

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic	Based on physical phenomenon to be analysed **X**	PSA based
Code model	BE **X** *In the limits of MAAP4-CANDU® code*	Conservative	
Initial conditions	BE	Conservative for parameters of major influence (95%/95%) **X**	
Boundary conditions (System performances)	BE **X** *Reasonable conservatism is considered to cover uncertainties*	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any system not affected	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified **X**
Proof of operability	Survivability **X** *Survivability analysed for the specific operating conditions*	Qualification	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes	No	Case by case **X**
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (time delay?) **X**	No	
Off-site mobile equipment	Yes (time delay?) **X** *After 72 hours*	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X** *According to tests performed for SAM guideline validation*	Same as DBA	
Safety criteria	No impact on population	Limited impact on population (specify area and time) **X** *Dose limits (at the exclusion zone limit), based on accident sequence frequency – established by regulatory requirements in NSN-02, up to 10·E-7 events/year*	

IX-10. DEC APPROACH IN THE RUSSIAN FEDERATION

TABLE IX-10.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic in regulatory documents **X**	Justified by deterministic systematic methodology **X**	PSA based **X**
Type of DEC-A sequences (several possibilities)	DBA+CCF **X**	CCF as initiating event **X**	Rare single events
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max (depending on objectives analyses) **X**	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes **X**	No	
Systems credited	Any system not affected **X**	DEC-A feature + DBA systems not affected by CCF	DEC-A feature only
Proof of operability	Survivability	Qualification + engineering assessment **X**	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA) **X**	Diversified power source	
Single failure criterion	Yes **X**	Diversified power source	
Preventive maintenance	Yes **X**	No	
On-site mobile equipment	acceptable time delay should be proven by the results of the analyses and confirmed by emergency training results **X**	No	
Off-site mobile equipment	No	Yes **X**	
Means of connecting mobile equipment included in the design	Yes **X**	Limited impact on population (specify area and time)	
Operator action delay	BE	Same as DBA **X**	
Safety criteria	No impact on population	Limited impact on population (no protection actions on the boundary beyond the PPMZ (PPZM not more 25 км) from the site boundary) **X**	

TABLE IX-10.2. DEC WITH CORE MELTING

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences		Based on physical phenomenon to be analysed **X**	PSA related **X**
Code model	BE (as realistic as possible) **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties		No **X**	
Systems credited	Any system not affected **X**	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified
Proof of operability	Survivability **X**	Qualification	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA) **X**	Diversified power source **X**	
Single failure criterion		No **X**	
Preventive maintenance	Yes **X**	No	
On-site mobile equipment	acceptable time delay should be proven by the results of the deterministic analyses and confirmed by emergency training results **X**	No	
Off-site mobile equipment	acceptable time delay should be proven by the results of the deterministic analyses and confirmed by full scale training results **X**	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE	Same as DBA **X**	
Safety criteria	No impact on population	Limited impact on population (no protection actions on the boundary beyond the PPMZ (PPZM not more 25 km) from the site boundary **X**	

IX-11. DEC APPROACH IN SWEDEN

TABLE IX-11.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic (vendor and/or IAEA list…)	Justified by deterministic systematic methodology	PSA based
Type of DEC-A sequences (several possibilities)	DBA+CCF (AOO and DBA) + CCF (instead of Single failure) **X**	CCF as initiating event	Rare single events
Code model	BE	Conservative, Same as for DBA **X**	
Initial conditions	BE	Conservative for parameters of major influence (95%/95%)	Same as for the normal analysis – Conservative **X**
Boundary conditions (System performances)	BE	Min/Max	Start with Conservative and go to BE if needed **X**
Additional sensitivity analysis	Yes	No **X**	If BE is used, sensitivity analysis is needed **X**
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any	DEC-A feature + DBA systems not affected by CCF **X**	DEC-A feature only
Proof of operability	Survivability	Qualification	
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source, totally independent **X**	
Single failure criterion	Yes	No, CCF instead of single failure **X**	
Preventive maintenance	Yes **X**	No	
On-site mobile equipment	Yes (time delay?) after 8 h if needed **X**	No	
Off-site mobile equipment	Yes (time delay?) after 72 h **X**	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE	Same as DBA	No action needed before 8 h **X**
Safety criteria	No impact on population **X**	Limited impact on population (specify area and time)	Same criteria as for DBA **X**

TABLE IX-11.2. DEC WITH CORE MELTING

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic Frequency based and 2 postulated events **X**	Based on physical phenomenon to be analysed	PSA based
Code model	BE **X**	Conservative	
Initial conditions	BE	Conservative for parameters of major influence (95%/95%) **X**	
Boundary conditions (System performances)	BE? **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes	No **X**	
Systems credited	Any system not affected	Dedicated to DEC-B only	Dedicated to DEC-B exceptions to be justified **X**
Proof of operability	Survivability	Qualification	?, Will be updated **X**
Seismic requirement	Yes **X**	No	Case by case
Protection against extreme external hazards	Yes **X**	No	Case by case
Power supply	Main diesel generators (DBA)	Diversified power source **X**	
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes **X**	No	
On-site mobile equipment	Yes (time delay?) 8 h **X**	No	
Off-site mobile equipment	Yes (time delay?) after 24 h **X**	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE	Same as DBA	8 h **X**
Safety criteria	No impact on population	Limited impact on population (specify area and time) Filtered Venting System with filters. **X**	

IX-12. DEC APPROACH IN THE UNITED STATES OF AMERICA

TABLE IX-12.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic (vendor and/or IAEA list…) **X**	Justified by deterministic systematic methodology	PSA based **X**
Type of DEC-A sequences (several possibilities)	DBA+CCF **X**	CCF as initiating event **X**	Rare single events *(if identified)* **X**
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%) **X**	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes **X**	No	
Systems credited	Any (not affected by CCF) **X**	DEC-A feature + DBA systems not affected by CCF	DEC-A feature only
Proof of operability	Survivability *(for those not subject to EQ)* **X**	Qualification *(some NSR SSCs include in reliability assurance programs & have some level of qualification)* **X**	
Seismic requirement	Yes	No	Case by case **X**
Protection against extreme external hazards	Yes	No	Case by case **X**
Power supply	Main diesel generators (DBA)	Diversified power source *(or passive)* **X**	

TABLE IX-12.1. DEC WITHOUT SIGNIFICANT FUEL DEGRADATION (cont.)

TOPIC	OPTION 1	OPTION 2	OPTION 3
Single failure criterion	Yes	No **X**	
Preventive maintenance	Yes **X**	No	
On-site mobile equipment	Yes (time delay?)	No	*if used in mitigating strategies* **X**
Off-site mobile equipment	Yes (time delay?) *after transition phase of mitigating strategy (days)* **X**	No	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population (prevent core damage) **X**	Limited impact on population (specify area and time)	

TABLE IX-12.2. DEC WITH CORE MELTING

TOPIC	OPTION 1	OPTION 2	OPTION 3
List of sequences	Generic	Based on physical phenomenon to be analysed **X**	PSA based **X**
Code model	BE **X**	Conservative	
Initial conditions	BE **X**	Conservative for parameters of major influence (95%/95%)	
Boundary conditions (System performances)	BE **X**	Min/Max	
Additional sensitivity analysis	Yes **X**	No	
Quantification of uncertainties	Yes **X**	No	
Systems credited	Any system not affected **X**	Dedicated to DEC-B only *(Special assessment of severe accident design features)* **X**	Dedicated to DEC-B exceptions to be justified
Proof of operability	Survivability *(for those not subject to EQ)* **X**	Qualification *(some NSR SSCs included in reliability assurance programmes and have some level of qualification)* **X**	
Seismic requirement	Yes *(robust, also influenced by degree to which feature is incorporated into containment design)* **X**	No	Case by case
Protection against extreme external hazards	Yes *(robust, relation to containment)* **X**	No	Case by case
Power supply	Main diesel generators (DBA) **X**	Diversified power source *(if needed, also passive features)* **X**	
Single failure criterion	Yes **X**	No **X**	

TABLE IX-12.2. DEC WITH CORE MELTING (cont.)

TOPIC	OPTION 1	OPTION 2	OPTION 3
Preventive maintenance	Yes	No **X**	
On-site mobile equipment	Yes (time delay?) **X**	No **X**	*note: portable equipment could be allowed but this approach not taken by designers*
Off-site mobile equipment	Yes (time delay?) **X**	No **X**	
Means of connecting mobile equipment included in the design	Yes **X**	No	
Operator action delay	BE **X**	Same as DBA	
Safety criteria	No impact on population **X**	Limited impact on population (specify area and time)	*overall results compared to safety goal* **X**

ABBREVIATIONS

ATWS:	Anticipated transient without scram
BDBA:	Beyond design basis accident
DBA:	Design basis accident
DiD:	Defence in depth
DSA:	Deterministic safety analysis
LOCA:	Loss of coolant accident
PSA:	Probabilistic safety assessment
SAM:	Severe accident management
SAMG:	Severe accident management guidelines
SAR:	Safety analysis report
SBO:	Station blackout

CONTRIBUTORS TO DRAFTING AND REVIEW

Amri, A.	International Atomic Energy Agency
Bentaib, A.	Institut de Radioprotection et de Sûreté Nucléaire, France
Courtin, E.	Framatome, France
Deo, A.K.	Atomic Energy Regulatory Board, India
Dinca, E.	National Commission for Nuclear Activities Control (CNCAN), Romania
Dubreuil Chambardel, A.	Électricité de France (EDF), France
Hakala, E.	Radiation and Nuclear Safety Authority (STUK), Finland
Hanberg, J.	Swedish Radiation safety Authority (SSM), Sweden
Hayes, M.	Nuclear Regulatory Commission (NRC), the United States of America
Kheshtpaz, H.	Atomic Energy Organization of Iran (AEOI), the Islamic Republic of Iran
Kozlova, N.	Scientific and Engineering Centre for Nuclear and Radiation Safety (SEC NRS), the Russian Federation
Kumar, P.K.	Nuclear Power Corporation of India Limited (NPCIL), India
Lau, V.	SNC Lavalin, Canada
Luis Hernandez, J.	International Atomic Energy Agency
Mesmous, N.	Canadian Nuclear Safety Commission (CNSC), Canada
Rashkov, K.	Kozloduy Nuclear Power Plant, Bulgaria
Reckley, W.	Nuclear Regulatory Commission (NRC), United States of America
Steinroetter, T.	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Germany
Takashi, U.	Tokyo Electric Power Company (TEPCO), Japan

Technical meeting, Vienna, Austria, 19-23 March 2018

Consultancy meetings, Vienna, Austria, 5-9 December 2016; 11-15 September 2017; 29 October – 2 November 2018; 23-27 September 2019.

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

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.

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550

Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group

Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:

www.eurospanbookstore.com/iaea

For further information:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.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 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

21-02834E

International Atomic Energy Agency
Vienna