IAEA TECDOC SERIES

IAEA-TECDOC-1791

IAEA-TECDOC-1791

Considerations on the Application of the IAEA Safety Requirements for the Design of 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 on the IAEA Internet site

http://www-ns.iaea.org/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.

CONSIDERATIONS ON THE APPLICATION OF THE IAEA SAFETY REQUIREMENTS FOR THE DESIGN OF 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
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
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
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
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
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-1791

CONSIDERATIONS ON THE APPLICATION OF THE IAEA SAFETY REQUIREMENTS FOR THE DESIGN OF NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

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
May 2016

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Considerations on the application of the IAEA safety requirements for the design of nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2016. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1791 | Includes bibliographical references.
Identifiers: IAEAL 16-01040 | ISBN 978–92–0–104116–6 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Safety measures. | Nuclear power plants — Accidents — Prevention. | Nuclear power plants — Design and construction.

FOREWORD

Revised to take into consideration findings from the Fukushima Daiichi nuclear power plant accident, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design, has introduced some new concepts with respect to the earlier safety standard published in the year 2000.

The preparation of SSR-2/1 (Rev. 1) was carried out with constant and intense involvement of IAEA Member States, but some new requirements, because of the novelty of the concepts introduced and the complexity of the issues, are not always interpreted in a unique way. The IAEA is confident that a complete clarification and a full understanding of the new requirements will be available when the supporting safety guides for design and safety assessment of nuclear power plants are prepared. The IAEA expects that the effort devoted to the preparation of this publication, which received input and comments from several Member States and experts, will also facilitate and harmonize the preparation or revision of these supporting standards.

This publication has been prepared by IAEA staff members who were involved in the preparation and revision of SSR-2/1 (Rev. 1), with the support of experts from Member States. It has received and considered the feedback from a group of members of the Nuclear Safety Standards Committee, but it is not intended as a consensus publication. The IAEA is grateful to the experts who contributed to the drafting and review of this publication. The IAEA officer responsible for this publication was J. Yllera 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 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

In 2012, a new IAEA Specific Safety Requirements, SSR-2/1 [1] was published with the objective to reflect safety developments and experience accumulated in the area of NPP design until that time. SSR-2/1 [1] was intended to ensure higher level of safety of NPPs taking into account the achieved state of the art in science and technology, and to reflect large consensus among the Member States. Among the most significant changes as compared with the previous IAEA Safety Requirements (NS-R-1 [16]) published in year 2000, are the inclusion of design extension conditions in the plant states to consider in the plant design envelope, and the strengthened independence of different levels of defence in depth. In accordance with SSR-2/1 [1], the design is required also to address the necessary provisions for the mitigation of severe accidents and the practical elimination of event sequences that could lead to early or large releases.

Although SSR-2/1 Rev. 0 [1] was published in the year 2012 it was prepared prior to the Fukushima Daiichi accident (March 2011). SSR-2/1 Rev. 0 [1] was approved by the Commission for Safety Standards few weeks after the accident. On the basis of the knowledge on the accident available at that time, the Commission considered the document to be suitable for publication. At the same time the IAEA started an action for a review of SSR-2/1 Rev. 0 [1] to check whether the lessons learned from the Fukushima Daiichi accident that, in the following months, became more and more clear were appropriately captured in SSR-2/1 Rev. 0 [1]. This effort resulted in the preparation of SSR-2/1 [1] under the IAEA Action Plan on Nuclear Safety[1].

The lessons learned from the Fukushima Daiichi accident have led to the reinforcement of some requirements in SSR-2/1 [1] related to important topics such as the robustness of the design against external natural hazards exceeding those derived from the site hazard evaluation, the independence of different levels of defence in depth, the emergency power supply, the capability for using of non-permanent sources of electric power and coolant and the reliability of the heat transfer to the ultimate heat sink.

The application and implications of the new requirements introduced in SSR-2/1 [1] are currently discussed and being addressed in different countries.

The novelty of the concepts introduced and the complexity of the issues can lead to different approaches to certain extent. By having developed this publication the IAEA intends to contribute to the identification of approaches and to coalesce or minimize diverging views.

It is understood that SSR-2/1 [1] establishes a very high level of safety that can be achieved by new plant designs. The considerations of this publication may however also be used for existing NPPs[2], e.g., within a Periodic Safety Review or a design review.

[1] In the aftermath of the Fukushima Daiichi NPP accident, the IAEA Action Plan on Nuclear Safety was approved by the Board of Governors in September 2011 and endorsed by all Member States at the 55th regular session of the General Conference in September 2011. It includes an action to "Review and strengthen IAEA Safety Standards and improve their implementation." The document is available at https://www.iaea.org/sites/default/files/actionplanns.pdf

[2] SSR-2/1 Rev.1 [1] Paragraph 1.3: "It might not be practicable to apply all the requirements of this Safety Requirements publication to nuclear power plants that are already in operation or under construction. In addition, it might not be feasible to modify designs that have already been approved by regulatory bodies."

1.2 OBJECTIVE

The main purpose of this publication is to provide insights and approaches in support of the practical application of the new crucial requirements introduced in SSR-2/1 [1] and subsequently reinforced in SSR-2/1 [1]. The TECDOC also identifies some terms that need to be explained consistent with the requirements.

The IAEA Secretariat expects that the effort devoted to the preparation of this publication will also facilitate and harmonize the preparation/revision of supporting Safety Guides for design and safety assessment of NPPs that are related to SSR-2/1 [1]. This publication could also be used as the basis for a future Safety Guide.

1.3 SCOPE

This publication provides a technical discussion on the following selected topics:

- *Categories of plant states*: discussion is provided on the interpretation of terms such as design basis, design envelope, design basis accidents, design extension conditions, beyond design basis accidents for both nuclear reactor and spent fuel pools (SFPs). Basic rules for identification of the plant states and relevant systems to cope with these states are indicated.

- *Concept of defence in depth*: the concept as adopted in the IAEA Safety Standards is analysed focusing on the correspondence between levels of defence in depth and plant states and, in particular on the implications on levels 3 and 4 of defence in depth due to the introduction of design extension conditions.

- *Concept of independence of the safety provisions at different levels of defence in depth*: discussion is provided on applicability and feasibility of implementation of the requirement for the independence specifically for plant systems at different levels of defence in depth, including also supporting systems (power supply, I&C, etc.). The methods for justification of adequacy of provisions at different levels of defence are also addressed. Discussion is provided on dependent failures and defensive measures against different root causes of these failures that could jeopardize the independence of levels of defence in depth.

- *Concept of 'practical elimination'*: the concept has been investigated and discussed to achieve a common understanding. Effort has been done to identify conditions that are expected to be 'practically eliminated' and how the demonstration of 'practical elimination' can be achieved.

- *Cliff edge effects and safety margins:* the requirements addressing cliff edge effects and safety margins are discussed to provide a more detailed understanding of the concepts and their implications on the design.

- *Design for external hazards*: the implications of the new requirements of SSR-2/1 [1] on the design for external hazards have been investigated also to address events possibly initiated by natural external hazards exceeding those derived from the site evaluation and to provide support for design and safety assessment of equipment for different levels of defence. Considerations on design against external hazards of equipment 'ultimately necessary' to prevent early or large releases have also been included.

- *Use of non-permanent equipment for accident management*: the document describes the issue and indicates limitations in using non-permanent sources of cooling water and power supply and identifies additional preconditions for facilitating their use, such as adequately robust preassembled connecting points. The need for adequate testing of the systems, availability of procedures and training of personnel is also emphasized.

- *Reliability of the ultimate heat sink*: the document describes the issue and provides guidance on the understanding of the ultimate heat sink, the relevant challenges to reliable heat transfer including the need for diversity as well as comprehensiveness of the systems and components to be covered.

1.4 STRUCTURE

Section 2 provides a description of the plant states that have to be considered in the design of a new NPP including extensive lists of examples and guidance for the safety assessment. Section 3 clarifies the concepts of design envelope, design basis for a single structure, system and component, (SSC) and the concept of beyond the design envelope. Sections 4, 5 and 6 deeply investigate the concept of defence in depth and its evolution from the original concept proposed by INSAG to the latest interpretation proposed by SSR-2/1 [1] with particular attention to the concept of independence of different levels of defence.

Sections 7 to 11 provide information on specific aspects in SSR-2/1 [1] such as: interpretation of the concept of practical elimination, safety margins and cliff edge effects, design for external hazards, use of non-permanent sources of electric power and coolant and reliability of the ultimate heat sink. Section 12 proposes some definitions for consideration during the preparation/revision of Safety Standards for possible inclusion in the IAEA Safety Glossary [4].

Appendix 1 provides examples of design extension conditions for LWR technology, Appendix 2 provides examples of acceptance criteria for different plant states, Appendix 3 provides an expanded discussion on dependent failures, Appendix 4 provides example of accident conditions to be practically eliminated and Appendix 5 provides a discussion on the chain to transfer heat from items important to safety to the ultimate heat sink.

2. PLANT STATES CONSIDERED IN THE DESIGN OF NUCLEAR POWER PLANTS

2.1 STATES CONSIDERED FOR THE DESIGN OF THE REACTOR

Compliance with the fundamental safety objective in IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [2] in the design of a NPP is required to be demonstrated for the broad spectrum of plant states including: operational states (normal operation and anticipated operational occurrences) and accident conditions (see Table 1).

TABLE 1. PLANT STATES CONSIDERED IN THE DESIGN

Operational states		Accident conditions		
Normal operation (NO)	Anticipated operational occurrences (AOO)	Design basis accidents (DBA)	Design extension conditions (DEC)	
			without significant fuel degradation	with core melt

In accordance with Requirement 14 of SSR-2/1 [1] the necessary capability, reliability and functionality for items important to safety for individual plant states shall be also specified in their design bases. In accordance with Requirement 13 of SSR-2/1 [1] the subdivision/grouping of the plant states into categories shall be primarily based on their frequency of occurrence at the NPP.

Table 2 shows indicative values of the frequency of occurrence of individual plant states associated with postulated initiating events (PIEs). These values are consistent with the generally established acceptable value for core damage frequency (CDF) for new plants to be below 10^{-5}/y (INSAG-12 [3]).

Although boundaries between plant states are shown as specific numbers they need to be considered as qualitative indicators rather than rigid limits. In particular there may be events which are traditionally considered as DBAs (e.g. large break loss of coolant accidents (LOCAs)) although they may have lower frequencies than those indicated in Table 2 for DBAs. Frequency of occurrence in spite of its prime importance is not to be used as the only basis for categorization of plant states.

The descriptions below refer mainly to water cooled reactors. For other kinds of reactors, specific considerations are made on a case by case basis.

TABLE 2. INDICATIVE EXPECTED FREQUENCIES OF OCCURRENCE OF DIFFERENT PLANT STATES

Plant state	Indicative expected frequency of occurrence
Normal operation	-
Anticipated operational occurrences	$> 10^{-2}$ events per year
Design basis accidents	$10^{-2} – 10^{-6}$ events per year
Design extension conditions without significant fuel degradation	$10^{-4} – 10^{-6}$ events per year
Design extension conditions with core melt	$< 10^{-6}$ events per year

2.1.1 Normal operation

The safety analysis for NO is required to address all the plant conditions under which systems and equipment are being operated. This includes all the phases of operation for which the plant was designed to operate in the course of NOs and maintenance over the life of the plant, both at power and shut down. These different operational conditions are often called 'modes of operation'.

The NO of an NPP typically includes the following conditions:

- Initial approach to reactor criticality;
- Normal reactor start-up from shutdown through criticality to power;
- Power operation including both full and low power;
- Changes in the reactor power level including house load operation and load follow modes if employed;
- Reactor shutdown from power operation:
  - Shutdown in a hot standby mode;
  - Shutdown in a cold shutdown mode;
  - Shutdown in a refuelling mode or equivalent maintenance mode that opens major closures in the reactor coolant pressure boundary (RCPB) or containment;
  - Shutdown in other modes or plant configurations with unique temperature, pressure or coolant inventory conditions;
  - Handling and storage of fresh and irradiated fuel.

2.1.2 Anticipated Operational Occurrences[3]

AOOs are events more complex than the manoeuvres carried out during NO that have the potential to challenge the safety of the reactor. These occurrences might be expected to occur at least once during the lifetime of the plant. Generally they have a frequency of occurrence greater than 10^{-2} per reactor-year.

[3] ***Anticipated operational occurrence*** (IAEA Safety Glossary [4]) An operational *process* deviating from *normal operation* which is expected to occur at least once during the *operating lifetime* of a *facility* but which, in view of appropriate *design* provisions, does not cause any significant damage to *items important to safety* or lead to *accident conditions*.

Typical examples of PIEs leading to AOOs could include those given below. This list is broadly indicative. The actual list will depend on the type of reactor and the actual design of the plant systems:

- *Increase in reactor heat removal:* inadvertent opening of steam relief valves; secondary pressure control malfunctions leading to an increase in steam flow rate; feedwater system malfunctions leading to an increase in the heat removal rate.
- *Decrease in reactor heat removal:* trip of one main feedwater pump; reduction in the steam flow rate for various reasons (control malfunctions, main steam valve closure, turbine trip, loss of external load, loss of condenser vacuum).
- *Decrease in reactor coolant system flow rate:* trip of one main coolant pump (MCP); inadvertent isolation of one main coolant system loop (if applicable), loss of off-site power (LOOP).
- *Reactivity and power distribution anomalies:* inadvertent control rod withdrawal; boron dilution due to a malfunction in the volume control system (for a pressurized water reactor (PWR)); wrong positioning of a fuel assembly.
- *Increase in reactor coolant inventory:* malfunctions of the chemical and volume control system (CVCS).
- *Decrease in reactor coolant inventory:* very small LOCA due to the failure of an instrument line.
- *Release of radioactive material from a subsystem or component:* minor leakage from a radioactive waste system or fuel failure.

2.1.3 Design Basis Accidents[4]

DBAs are postulated for the purpose of establishing the design bases of the safety systems.

Typical examples of PIEs leading to DBAs could include those given below. This list is broadly indicative and the actual list will depend on the type of reactor and actual design:

- *Increase in reactor heat removal:* steam line breaks.
- *Decrease in reactor heat removal:* feedwater line breaks.
- *Decrease in reactor coolant system flow rate*: trip of all MCPs; MCP seizure or shaft break.
- *Reactivity and power distribution anomalies:* uncontrolled control rod withdrawal; control rod ejection; boron dilution due to the startup of an inactive loop (for a PWR).
- *Increase in reactor coolant inventory:* inadvertent operation of emergency core cooling.
- *Decrease in reactor coolant inventory:* a spectrum of possible LOCAs; inadvertent opening of the primary system relief valves; leaks of primary coolant into the secondary system.
- *Release of radioactive material from a subsystem or component:* overheating of or damage to used fuel in transit or storage; break in a gaseous or liquid waste treatment system.

[4] ***Design basis accident*** (The definition is from SSR-2/1 [1] and supersedes the definition in the IAEA Safety Glossary [4]): A postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.

2.1.4 Design Extension Conditions

DECs were introduced in the requirements for the design of NPPs SSR-2/1 [1] for the purpose to further improve safety by enhancing the plant's capability to withstand the conditions generated by accidents that are more severe than DBAs.

The concept of DEC is not completely new since some multiple failures of safety systems have been considered in the design and safety assessment of existing NPPs or their importance was recognized and requirements were issued to backfit the existing designs. This is the case of the Station Blackout (SBO) and Anticipated Transients without Scram (ATWS). These conditions are beyond the traditional design basis accidents because they involve failures of the safety system designed to cope with the respective abnormal event (emergency power supply for LOOP or reactor shutdown system for a PIE requiring the actuation of the reactor trip system).

According to SSR-2/1 [1], DECs 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[5]."

DECs are those conditions not included in the DBAs, and which have a frequency of occurrence that cannot be neglected and in some cases comparable with the frequency of some DBAs.

A deviation from NO can escalate into DECs either due to extraordinary severity of the event itself or more typically due to multiple failures of safety systems caused either by equipment malfunctions or human errors.

The most plausible reason for the failure of safety functions (such as reactivity control and core cooling) is the occurrence of dependent failures that may cause the failure of redundant trains simultaneously. Common cause failures (CCFs) are a predominant group that are given high attention and provisions are implemented in the design either to eliminate them or reduce their likelihood to the extent possible or to cope with their consequences. Systematic analysis of dependences between SSCs important to safety is a good practice to conclude whether CCFs have been adequately considered.

Following the publication of SSR-2/1 Rev. 0 [1] in 2012 the term 'design extension conditions' is widely used and very often referred to even by Member States that do not explicitly use this term in their regulations.

Some national regulations require the demonstration that the capabilities of the design are such as to withstand some external events exceeding those derived from the site evaluation without causing large releases. This approach has been reinforced after the Fukushima accident and also adopted in SSR-2/1 [1]. However, some considerations are necessary to avoid misunderstandings on the definitions of DEC adopted by in SSR-2/1 [1] since some Member States tend to include in the list of DECs also some external hazards that were not considered in the past (e.g. earthquake exceeding the design basis earthquake, commercial air

[5] According to the IAEA practice, new definitions that are included in the IAEA safety standards will be included in the IAEA Safety Glossary [4].

craft impact, etc.). In the IAEA terminology, a DEC is a postulated plant state (see Table 1) that is determined by a postulated sequence of events, and for the same reasons that design basis hazards are not considered DBAs, more severe hazards are not considered DECs although they might result in a DBA or possibly in DEC. According to SSR-2/1 [1], external hazards are considered in the design by assuming appropriate loads, load combinations and margins as detailed in requirements 5.21 and 5.21a for DBA equipment, and requirements 5.21a and 5.29 for DEC equipment.

The control of DECs is expected to be achieved primarily by features implemented in the design (safety features for DECs) and not only by accident management measures that are using equipment designed for other purposes. This means that in principle a DEC is such if its consideration in the design leads to the need of additional equipment or to an upgraded classification of lower class equipment to mitigate the DEC.

Requirement 20 of SSR-2/1 [1] specifies that a set of DECs be considered in the NPP design derived on the basis of engineering judgement as well as deterministic and probabilistic assessment. Operating experience and lessons learned from accidents as well as research results are also important bases for the engineering judgement that informs the set of DECs.

DECs, which are addressed in Requirement 20 and supplemented in several other system requirements of SSR-2/1 Rev.1 [1], include events without significant fuel damage and with core melt, as described below.

2.1.4.1 Design extension conditions without significant fuel degradation

In general, at least three types of DECs can be considered according to the postulated assumptions:

- Very unlikely events that could lead to situations beyond the capability of safety systems for DBAs. The regulatory body may accept a demonstration based on best estimate analyses that the safety systems are indeed capable of and qualified for mitigating the event under consideration. In general however, the inclusion of specific safety features for DEC is necessary.
- Multiple failures (e.g. CCFs in redundant trains) that prevent the safety systems from performing their intended function to control the PIE. An example is LOCA without actuation of a safety injection system. The failures of supporting systems are implicitly included among the causes of failure of safety systems.
- Multiple failures that cause the loss of a safety system while this system is used to fulfil the fundamental safety functions in NO. This applies to those designs that use, for example, the same system for the heat removal in accident conditions and during shutdown.

The use of both deterministic and probabilistic insights is essential in the identification and control of DECs is an important approach. This combination of insights is an effective design technique whether considering the entire NPP design or evaluating a specific safety function such as the containment function. Due to the extensive operating experience with the light water technology, research results and the numerous risk assessment studies performed over time in Member States, there are some typical DECs without fuel degradation that are not strongly design-dependent and commonly postulated. The list, that in some countries is also referred to as deterministically identified, may include:

- ATWS;
- SBO;
- Loss of core cooling in the residual heat removal mode;
- Extended loss of cooling of fuel pool and inventory;
- Loss of normal access to the ultimate heat sink.

These DECs are further discussed in Appendix 1.

In addition to these DECs commonly agreed by some regulatory bodies that are systematically addressed in several reactor designs, there are other DECs that are more technology dependent and can be derived on the basis of probabilistic considerations. For this purpose a PSA can be carried out at the design stage and taking account also of applicable knowledge gained from previous studies. The aim of the PSA would be to identify those areas of the design, in which the introduction of safety features for DEC may help to reduce the probability of severe accidents, and balance the contribution to risk of different accident sequences. The PSA can be used also to compare the effectiveness of different design options and accident management measures.

Although a PSA at the design phase will have some limitations to address some site or plant specific issues and operational aspects, the PSA can be used to identify relevant risk contributors either from the accident sequences or from the component importance analysis in the generic design. The goal of the safety features for DECs would be to reinforce the safety provisions at previous levels of defence in depth for reaching the CDF required by the regulatory body considering the uncertainties of a PSA at that stage, and balancing the risk profile. The PSA includes considerations of multiple failures, so that sequences with multiple failures can be assessed for their risk significance.

The PSA is accomplished to demonstrate that the target established for CDF is met and it is performed on a design-specific or plant-specific basis with the following objectives:

- Identify and address potential design features and plant operational vulnerabilities not previously addressed;
- Reduce the significant risk contributors by introducing appropriate features;
- Select among alternative features, operational strategies, and design options assess support systems (i.e. ventilation, cooling, electrical supply) for their potential of causing immediate or delayed consequential multiple failures in both operational and safety systems.

The list of these additional DECs derived from PSA, according to some practice in Member States that is reported here only as an example might include:

- Total loss of feed water;
- LOCA plus loss of one emergency core cooling system (either the high pressure or the low pressure emergency cooling system);
- Loss of the component cooling water system or the essential service water system (ESWS);
- Uncontrolled boron dilution;
- Multiple steam generator tube ruptures (MSGTR) (for PWRs);
- Steam generator (SG) tube ruptures induced by main steam line break (MSLB) (for PWRs);
- Uncontrolled level drop during mid-loop operation (for PWRs) or during refuelling.

It has to be stressed that the purpose of safety features for DEC is not to compensate for unreliable safety systems but to reinforce the plant safety by establishing supplementary design provisions in case of exceptional initiators or complex accident sequences that are also associated with significant uncertainty. In several cases for instance, the safety features for DEC provide diversity against CCFs of singular importance and difficult to estimate accurately (e.g. ATWS).

2.1.4.2 Design extension conditions with core melt

SSR-2/1 [1] requires that the design is such to ensure the capability to mitigate the consequences of severe degradation of the reactor core. Therefore, it is necessary to select a representative group of severe accident conditions (DECs with core melt) to be used for defining the design basis of the mitigatory safety features for these conditions. For this purpose, it is also important to have sufficient knowledge about the phenomena associated with different severe accidents.

For postulating the DECs to be considered in the design, the accident sequences that lead to core melt and the plant conditions at the onset of the core melt are clearly identified.

The features for the mitigation of DEC with core melt are such to prevent that those severe accident phenomena, such as hydrogen detonation, basemat melt through due to core-concrete interaction and steam explosions, cause the loss of containment integrity (see Section 7).

For DECs with core melt, maintaining the integrity of the containment is the main objective. This also implies that the cooling and stabilization of the molten fuel and the removal of heat from the containment need to be achieved in the long term.

The progression of a severe accident involves a highly complex set of physical and chemical phenomena that have been the subject of extensive programs of research after the Three Mile Island (TMI) accident. The knowledge available today provides a sound basis for the identification of DECs and associated phenomena that are addressed in the design.

2.1.4.3 Acceptance Criteria for DECs

The objective of the safety assessment of the design is to demonstrate that relevant safety requirements for all plant states (including DEC) are met. The assessment also demonstrates, with an adequate degree of confidence, that the radiological consequences will remain within the established acceptance criteria and will be as low as reasonably achievable. Examples of acceptance criteria for maintaining the integrity of barriers and radiological acceptance criteria for each plant state are provided in Appendix 2.

SSR-2/1 [1] sets out the general requirement for DECs (Req. 20) where it 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."

Requirement 20 is supplemented by paragraphs 5.31 and 5.31A:

5.31. "The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release[6] is 'practically eliminated'."

5.31A. "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."

Designers and regulators often develop subsidiary objectives in terms of radiological consequences (effective doses at specific distances from the site boundary) or containment leak tightness (e.g. leak for 24 hours) to demonstrate that the implementation of protective measures for the public would not be necessary or minor in the event of accidents without significant fuel damage or would be limited in time and areas in the event of accidents with core melt.

The safety features necessary to mitigate the consequences of DECs without significant fuel damage are such that their reliability is adequate to meet the probabilistic target for CDF.

2.1.4.4 Considerations on operator actions for DECs

Reliance on the use of operator actions is generally minimized when considering event sequences. For example, in DBAs, operator actions are not normally necessary in the short term. However, as a sequence extends in time, operator actions from the control room are needed, then if the sequence continues to extend, more actions are needed from a variety of plant personnel. In general, credit for operator action can be given when there is sufficient margin between the time required to perform an operation and the time available in the sequence to perform the operation. Therefore, a similar approach when considering operator actions for DECs could be taken. For DECs, which can involve multiple failure scenarios, greater reliance on operator actions, is likely needed.

a) Implication of DECs on the definition of plant equipment

The introduction of the concept of DECs in the design and the implementation of the 'safety features for DECs' suggest an amendment to the definition of 'plant equipment' in the current IAEA Safety Glossary [4]. The 'safety features for DECs' are obviously items important to safety but, although their safety functions are similar to those performed by 'safety systems,' they are considered separately since they may be designed with rules and acceptance criteria different from those used for safety systems. Figure 1 is proposed for consideration[7].

[6] The definitions below are from SSR-2/1 [1]
Early radioactive release: a release for which off-site protective measures are necessary but unlikely to be fully effective in due time.
Large radioactive release: a release for which off-site protective measures limited in terms of times and area of application are insufficient to protect people and the environment.
[7] Amended definitions and new definitions proposed for inclusion in the Glossary are collected in Section 12.

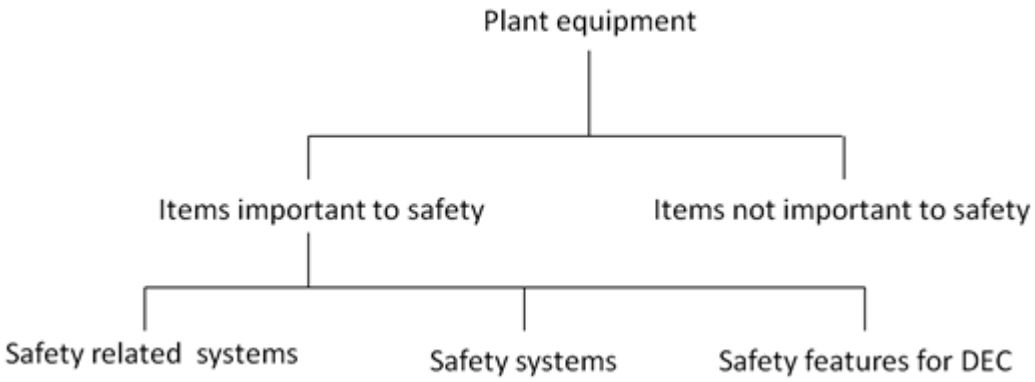

FIG. 1. Plant equipment.

3. PLANT DESIGN ENVELOPE AND DESIGN BASIS OF PLANT EQUIPMENT

It is rather common to make reference to 'design basis of the plant' or simply to 'design basis' to indicate the range of specific conditions, design criteria and rules that have been considered in the design of the plant. This terminology is not very precise and, in some cases, it can be misleading because the engineering rules and design requirements for items important to safety for different plant states can be considerably different. Each single structure, system or component to be correctly designed needs its own design basis and the design basis can be different for different structures, systems or components. The introduction of safety features for DECs in the design of NPPs would suggest that the design basis of the plant would cover also DECs. However, this extension of the meaning has implications for existing regulations in some Member States and can create conflicts with uses of the term for existing NPPs not designed for DECs. Therefore, after consultation with Member States, this publication uses the term 'plant design envelope' to refer, in a simplified way, to the initiating events, internal and external hazards and other conditions considered in the design of the NPP.

The paragraph below (that reflects what is detailed in Requirements. 13-28 of SSR-2/1) [1] summarizes the concept of design basis for a structure, system or component[8].

The design basis of a structure, system or component is the set of information that identifies conditions, needs and requirements necessary for the design, including the*:*

- Functions to be performed by a structure, system or component of a facility;
- Conditions generated by operational states and accident conditions that the structure, system or component has to withstand;
- Conditions generated by internal and external hazards that the structure, system or component has to withstand;
- Acceptance criteria for the necessary capability, reliability, availability and functionality;
- Specific assumptions and design rules*.*

The design basis of a structure, systems or component is completed and supplemented by Specification Sheets and by detailed design calculations.

The term design basis of a structure, system or component, as defined above, could be included as a new term in the IAEA Safety Glossary [4]. Saying, for example, that a specific accident is included in the design envelope of the plant (e.g. it is a DBA) means in practice that the conditions generated by this accident are included in the design basis of a set of structures, systems and components that have the function to deal with and control that accident.

'Design basis accidents' is the set of postulated accident conditions that the plant has to withstand meeting the criteria and following the rules specified in SSR-2/1 [1]. DBAs are used, together with other factors, to define the design basis for safety systems and other items important to safety that are necessary to control the conditions generated by the DBAs.

Figure 2 represents in a simplified graphical form the different elements that contribute to the definition of the design basis of the main sets of equipment important to safety for different plant states.

[8] Amended definitions and new definitions proposed for inclusion in the Glossary are collected in Section 12.

The Operational states (NO and AOOs) mainly provide input to the design basis of the process equipment for NO and for control system, limitation systems and the reactor trip system.

The Accident conditions (DBAs and DECs) provide input to the design basis of Safety systems (control of DBAs) and Safety features for DECs (control of DECs).

The safety features for DECs include design features for multiple system failures for core melt prevention and mitigatory design features for core melt scenarios.

SSR-2/1 [1] (paragraphs 4.11 and 5.21) requires that conditions moderately exceeding those considered for the design shall not result in cliff edge effects (see Section 8).

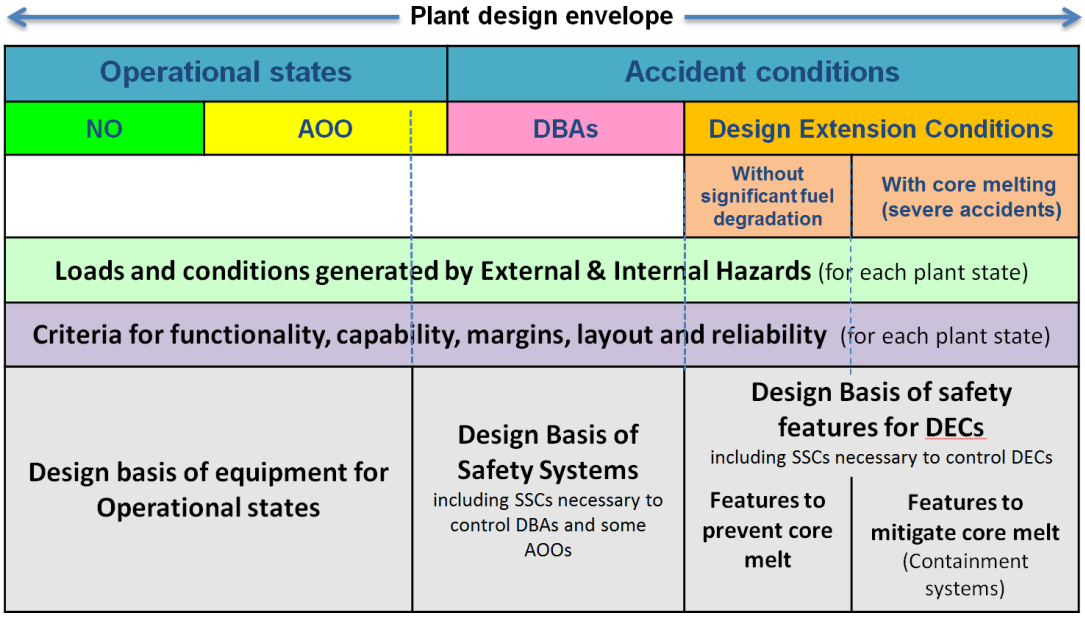

FIG. 2. Main elements of the design basis of SSCs for different plant states.

Figure 2 also shows that the conditions generated by external and internal hazards and criteria for functionality, capability, layout, margins and reliability, provide input to the design basis of the plant equipment. Figure 2 is synthetic and does not show the differences in the conditions and criteria applicable for the different classes of equipment, which depend on the safety classification of the specific SSCs. For example, SSR-2/1 [1] requires the application of the single failure criterion for the design of safety systems while the application of this criterion is not required for the design of safety features for DECs.

Note that features to facilitate the use of non-permanent equipment are outside of the plant design envelope.

4. DEFENCE IN DEPTH STRATEGY FOR NEW NUCLEAR POWER PLANTS

Following the Chernobyl accident the defence in depth concept was defined and recognized as a fundamental and overarching principle of nuclear safety for preventing accidents and mitigating their consequences.

Although the implementation of the defence in depth concept has been required for long time, the Fukushima Daiichi accident and the complementary safety assessments (termed 'stress tests' in the European Union and other countries) conducted in different Member States thereafter have revealed weaknesses in its implementation in some plants. Therefore, how to interpret the requirements embedded in the concept of defence in depth is an important element in ensuring its correct and full implementation.

Table 3 is taken from INSAG-10 [5] and represents a synthetic description of the concept of defence in depth formalized in five levels of defence as defined in 1996. This scheme has been fully adopted and incorporated in the Safety Standards of the IAEA for nuclear installations and it has also been followed, with some elaboration, for the preparation of SSR-2/1 [1]. This formulation of defence in depth also allows a rather straight correspondence between plant states and levels of defence in depth to be established.

TABLE 3. LEVELS OF DEFENCE IN DEPTH IN EXISTING NUCLEAR POWER

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

The defence in depth concept is not to be understood as merely limited to the request for the implementation of a number of consecutive barriers and protection levels, but is to be understood as the main general principle that leads to the formulation of safety requirements including requirements necessary to achieve the quality and reliability expected for the barriers and for systems ensuring their integrity.

Some aspects such as vulnerabilities for CCFs, appropriate independence between the different levels, robustness and avoidance of cliff edge effects, are key issues to reinforce the overall effectiveness of the implementation of the defence in depth. The sections below address specific aspects of the defence in depth concept to support a better understanding.

4.1 PREVENTION AND MITIGATION

Prevention and mitigation are terms widely used in nuclear safety and they are mostly referred to accidents (prevention of accidents and mitigation of the consequences of accidents). With references to defence in depth, the essential means of each level prevent the need for activation of the essential means of the following level and, at the same time, they mitigate the consequences of the failure of the previous ones. Level 1, being the first level, has a predominant preventive function and level 5, being the last, has only a mitigatory function.

Mitigation is interpreted as controlling or stopping the evolution of an event sequence so that the consequences on the plant and the environment are kept under control and below acceptable limits. At any stage of a given event sequence, theoretically evolving from an initiating event to very severe conditions, prevention refers to what has not happened yet and mitigation to what has already happened. Considering for example the level 2 of defence in depth, the essential means are active to control or mitigating the consequences of an AOO while, at the same time, preventing the escalation of the AOO into an accident. Similar considerations can be made (*mutatis mutandis)* for level 3 and level 4.

4.2 DEFENSE IN DEPTH FOR NEW NUCLEAR POWER PLANTS

The concept of defence in depth as used in the IAEA Safety Standards is mainly based on INSAG-10 [5] and SSR-2/1 [1]. SSR-2/1 [1] provides additional information for its practical implementation.

Below is a description of the purpose of each level of defence and the means to accomplish it. This description is taken directly from Section 2 of SSR-2/1 [1]. Some additional considerations about each level are provided after the descriptions. It is important to notice that currently there is not a unanimous understanding among Member States about the association of all the levels of defence in depth with the plant states defined in SSR-2/1 [1]. The point of discrepancy is the association of DECs without fuel degradation to one of the levels of defence in depth defined in SSR-2/1 [1]. Some Member States associate them to the level 3 and others associate them to the level 4. A description of both approaches is provided.

"(1) The purpose of the first level of defence is to prevent deviations from NO and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the

requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.

(2) The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent AOOs at the plant from escalating to accident conditions. This is in recognition of the fact that PIEs are likely to occur over the operating lifetime of a NPP, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or else to minimize their consequences, and to return the plant to a safe state.

(3) For the third level of defence, it is assumed that, although very unlikely, the escalation of certain AOOs or PIEs might not be controlled at a preceding level and that an accident could develop. In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be provided that are capable of preventing damage to the reactor core or significant off-site releases and returning the plant to a safe state.

(4) The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of the accident and mitigating the consequences of a severe accident. The safety objective in the case of a severe accident is that only protective measures that are limited in terms of times and areas of application would be necessary and that off-site contamination would be avoided. Sequences that lead to large or early radioactive releases are required to be 'practically eliminated'.

(5) The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents. This requires the provision of an adequately equipped emergency control centre and emergency plans and emergency procedures for on-site and off-site emergency response."

4.2.1 Elaboration on Level 1

The essential means required to meet the objective of the level 1 of defence in depth are, as indicated in Table 3, a conservative design and high quality in construction and operation. More generally this level includes all provisions implemented to avoid challenging the subsequent levels by preventing equipment failure, system malfunctioning and human errors.

The need of an effective plant control system is not explicitly mentioned in the description of level 1 in SSR-2/1 [1]. The control system has the functions to maintain the values of the process parameters inside the NO range and to prevent abnormal operations. Malfunctioning of the control system are among the main causes of AOOs, therefore this system and the systems designed to control AOOs are not included in the same level of defence.

The reliability of the equipment of level 1 of defence in depth is in general expected to be such that frequency of occurrence of an AOO is less than 1/reactor-year and the frequency of occurrence of accident caused by equipment failure less than 10^{-2} /reactor-year as indicated in

Table 2. Accidents not considered for the design of the plant are expected to have a likelihood that is very low.

Although the level 1 of defence in depth is normally associated with NO, the essential means of this level such as conservative design and high quality in construction and operation are understood as applied also to SSCs that are designed for other plant states.

4.2.2 Elaboration on Level 2

For level 2 the intervention of the limitation or protection system may be necessary for the shutdown of the reactor power to control some postulated abnormal conditions (e.g. AOOs). Modern designs avail on a limitation system that reacts upon some perturbations of the NO regime that cannot be handled by the control systems, preventing or delaying a reactor trip by quickly reducing the power of the reactor and providing signals to key plant systems and components to stabilize the plant. For most reactor designs, the reactor trip system is a safety system that is also required for the control of accidents at the Level 3 of defence in depth. Also a typical AOO like the LOOP requires either the house-load operation or the intervention of the onsite emergency power that has also relevant functions on level 3. This shows specific cases of difficulty to implement independence between level 2 and level 3 of defence in depth (see paragraph 4.13A of SSR-2/1 [1] in section 4.3).

Equipment of level 2 of defence in depth is aimed at reducing the number of challenges to the defence in depth level 3. Their reliability is at least expected to be such that level 3 of defence in depth is not necessary to intervene with a frequency higher than 10^{-2} per reactor-year as indicated in Table 2. In practice, the frequency of an evolution from and AOO into an accident condition is expected to be lower.

4.2.3 Elaboration on Levels 3 & 4

As indicated above there are basically two different interpretations in Member States about the association of DECs without core melt with level 3 or level 4 of defence in depth. This leads to two different approaches:

4.2.3.1 Approach 1

a) Level 3

In this approach it is considered that level 3 deals with the mitigation of those postulated accident conditions the evolution of which can be controlled and the core melt prevented. This means that these accident conditions include DBAs and DECs without core melt. For practical purposes the Level 3 of defence in depth is considered as formed by two sub levels indicated as 3a (DBAs) and 3b (DECs without core melt). The distinction of DBAs and DECs without core melt serves to achieve a better alignment the design rules for safety systems and for safety features for DECs may be different as well as the acceptance criteria for DBAs and for DECs. If there were no differences, the safety features for DEC would be just additional safety systems.

The essential means of achieving the objective of level 3a are the safety systems and the accident procedures for DBAs. The safety systems are designed with a set of conservative, prescriptive rules and criteria (e.g. application of the single failure criterion) which provide high confidence in their success to meet the relevant acceptance criteria and safety limits. The

reliability of equipment of level 3a of defence in depth is expected to be such that the probability of failure per demand of level 3a is in the range of 10^{-3} - 10^{-4}.

DECs without core melt can typically be generated by multiple failures occurring in safety systems either in NO (e.g. loss of RHR during shutdown) or following an AOO or a DBA. It is important to note that in some cases the failure of level 2 can lead directly to level 3b (e.g. ATWS, SBO) because some safety systems might be shared between level 2 and level 3a.

Level 3b is mainly aimed at ensuring that for complex sequences based on internal events, the risk that the successive failure of the levels of defence in depth leading to a core melt (level 4) is consistent with the targets defined in Table 1. Therefore level 3b is further enhancing the prevention of core melt implemented by the previous level of defence in depth. Design rules for SSCs for level 3b may be less conservative than those for level 3a.

b) Level 4

In this approach it is understood that level 4 deals with the control of severe accidents and the major objective of level 4 is to mitigate the consequences of DECs with core melt. The essential means of achieving the objective of level 4 include safety features for DECs and severe accident management procedures and guidelines.

DECs with core melt, i.e. severe accidents, may be caused by the failure of level 3a or 3b. A DEC with core melt is expected not to result directly from failures of level 2.

Additionally, since in SSR-2/1 [1], the single failure criterion is required to be applied to each safety group, the application of this criterion is not required for the safety features for DEC because they are not considered as part of the safety group[9]. It holds, however, the requirement that the reliability of any item important to safety shall be commensurate to its significance to safety.

Equipment belonging to defence in depth level 4 is implemented to limit the radiological releases in case of core melt and is aimed at maintaining the confinement functions.

Accident management encompasses both hardware and procedures necessary to maintain the radiological release as low as reasonably possible in any accident. In particular SSR-2/1 [1] requires (Requirement 67) the implementation of a Technical Support Centre (TSC) to provide technical support to the operation staff during accident conditions. Given its function, the TSC is an important feature for the level 4 of the defence in depth. The activation of the TSC for level 3 is expected not to be necessary, but it may be done to support accident management.

The use of non-permanent equipment (see Section 10) is also a measure to facilitate the accident management and for dealing with non-postulated conditions beyond the DECs.

[9] The assembly of equipment designated to perform all actions required for a particular *postulated initiating event* to ensure that the *limits* specified in the *design basis* for *anticipated operational occurrences* and *design basis accidents* are not exceeded.

4.2.3.2 Approach 2

a) Level 3

In this approach it is understood that Level 3 deals only with the postulated set of DBAs. The essential means of achieving the objective of level 3 are the safety systems and the emergency operating procedures for DBAs. The safety systems are designed with a set of conservative, prescriptive rules and criteria (e.g. application of the single failure criterion) which provide high confidence in their success to meet the relevant acceptance criteria and safety limits.

The reliability of equipment of level 3 of defence in depth is expected to be such that the probability of failure per demand of level 3 is, at least, in the range of 10^{-3} - 10^{-4}).

b) Level 4

In this approach level 4 deals with both, the control of postulated multiple failures without core melt and with postulated severe accident conditions. The essential means of achieving the general objective of level 4 include safety features for DECs and accident management procedures and guidelines.

In this approach the level 4 of defence in depth can be considered as formed by two sub levels indicated as 4a and 4b. Level 4a is mainly aimed at ensuring that for complex sequences based on internal events, the risk that the successive failure of the levels of defence in depth leading to a core melt (level 4b) is consistent with the targets defined in Table 1. Therefore level 4a is further enhancing the prevention of core melt implemented by the previous level of defence in depth. Design rules for SSCs for level 4a may be less conservative than those for level 3.

The objective of level 4a deals with the mitigation of those postulated accident conditions the evolution of which can be controlled and the core melt prevented.

Equipment belonging to defence in depth level 4b is used to limit the radiological releases in case of core melt and is aimed at maintaining the containment functions.

DECs can be generated by multiple failures of safety systems either in NO (e.g. loss of RHR during shutdown) or following an AOO or a DBA. In this approach Level 4 includes DEC without and with core melt. The failure of level 2 can lead directly to DECs without core melt while the failure of level 3 can also lead to DECs with core melt. The two major objectives of Level 4 are: (a) to prevent DECs without core melt from progressing to core melt situations and (b) to mitigate the consequences of DECs with core melt.

It is important to notice that since the failure of safety systems following an AOO can lead directly to a DEC, it is possible that the Level 3 of defence in depth is bypassed (e.g. ATWS, SBO).

Unlike the safety systems for DBAs the safety features for DECs are not required to be designed to meet the single failure criterion.

4.2.4 Elaboration on Level 5

According to the IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [6], the on-site emergency response facilities (which are separated from the control room and the supplementary control room) include the TSC,

the operational support centre (OSC) and the emergency centre (EC). While the TSC is considered as an essential mean of level 4 of defence in depth, the operational support centre and the EC are essential means of level 5 of defence in depth.

4.3 SUMMARY

The current approach to defence in depth in SSR-2/1 [1] is presented in Table 4. The main difference with the original table of INSAG-10 [5] is represented by the introduction of the DECs. This fact, without impairing the general approach, has requested a slight elaboration of the third and fourth levels of defence in depth and minor changes in the wording. The column of the essential means has been split in two to better indicate essential means related to design and those related to operation. Table 4 displays in addition the plant states associated with each level of defence in depth for the two different approaches described above.

Approach 1, i.e. the association of DECs without core melt to level 3, has the advantage that each level has clear objectives regarding the progression of the accident and the protection of the barriers, i.e. level 3 to prevent damage to the reactor core and level 4 to mitigate severe accidents for preventing off site contamination.

Approach 2, i.e. the grouping of DECs without core melt and with core melt in level 4, facilitates however the differentiation between the set of rules for design and safety assessment to be applied for DECs from those for DBA.

It is not practical to carry on two parallel formulations through the document. In the following sections the formulation of the Approach 1 is being used. It is important to notice that the only difference is the terminology used in the association of DECs without core melt. Regardless of the approach used, the subject of fundamental importance is the appropriate definition of the rules and criteria to be applied in the design and safety assessment of safety features for DEC and the consistent implementation of requirements for independence of safety provisions for DBA and DEC

SSR-2/1 [1] also requires the independence of safety provisions at different defence in depth levels:

4.13A. “The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems.”

The issue of the independence of the different levels of defence in depth is addressed in detail in Section 6 of this publication.

TABLE 4. LEVELS OF DEFENCE IN DEPTH FOR THE DESIGN OF NEW NUCLEAR POWER PLANTS

Level of defence **Approach 1**	**Objective**	**Essential design means**	**Essential operational means**	**Level of defence** **Approach 2**
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures	Level 1
Level 2	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures	Level 2
Level 3 3a	Control of design basis accidents	Engineered safety features (safety systems)	Emergency operating procedures	Level 3
Level 3 3b	Control of design extension conditions to prevent core melt	Safety features for design extension conditions without core melt	Emergency operating procedures	4a Level 4
Level 4	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melt. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines	4b
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans	Level 5

5. DEFENCE IN DEPTH FOR THE IRRADIATED FUEL WATER POOL STORAGE

The irradiated fuel storage has a potential for high radiation risks. As indicated in SF-1 [2], the primary means for prevention and mitigation of accidents is the application of defence in depth. This section provides consideration on how the defence in depth approach can be applied to the design of the storage systems for irradiated fuel in a NPP, in which the irradiated fuel is contained in a pool of water (SFP) hosted inside the reactor containment or in an adjacent building outside the containment.

As for the reactor, the storage systems for irradiated fuel need to fulfil at all times, for the irradiated fuel, the three fundamental safety functions:

- Maintaining subcriticality of the fuel;
- Removal of decay heat from irradiated fuel;
- Confinement of radioactive substances.

In addition there is the need to shield the radiation of the fuel elements to meet the limits for occupational radiation doses. To this aim a sufficient level of water over the top of the fuel elements is maintained, thus providing thermal inertia in cooling the fuel.

Consistent with the requirements for the reactor, the practical elimination of early and large releases, and avoiding high radiation fields on the site have to be achieved. Requirement 80 of SSR-2/1 [1] provides important aspects for the implementation of defence in depth for the irradiated fuel storage.

Although the irradiated fuel pool is to large extent independent from the reactor, the same design methodology based on a deterministic approach supplemented by probabilistic evaluations and applying a graded approach, can be used for the design and safety verification of the irradiated fuel pool systems.

This implies that operational states (NO and AOOs) and accident conditions (DBAs and, as appropriate, DECs), as well as the associated design limits for these states, need to be defined to establish the design bases for the SSCs of the irradiated fuel storage. Design provisions and measures have to be implemented to eliminate possibilities for high radiation doses and early or large radiological release. The safety features (essential means) for each level of defence in depth are expected to be specified.

5.1 NORMAL OPERATION

During NO the fundamental safety functions and design limits are ensured as follows:

- Subcriticality is ensured with sufficient margins by the physical layout (geometry of the positioning of the fuel elements) complemented, in some cases, by neutron absorbers (in solid bars or solved in water).
- The removal of heat from the fuel is ensured by the submersion under water maintained at an adequate temperature (e.g. 40 ºC) by a dedicated cooling system.
- The confinement of radioactive gases released from the fuel is ensured by the building isolation and the ventilation system that keeps the pressure in the building slightly below the atmospheric pressure, or by the containment building if the pool is inside the containment.

NO is associated with the 1st level of defence in depth. As for the reactor, typical measures for this level are appropriate design codes and materials, high quality control of the manufacture of components and construction, conservative design, adequate provisions for in-service inspection, maintenance and testing, etc. and in particular robust and reliable cooling and purification systems to ensure the satisfactory operation and the prevention of failures and abnormal conditions.

5.2 ANTICIPATED OPERATIONAL OCCURRENCES

Credible failures of equipment or systems, and abnormal operations, both within and outside the storage facility, have to be postulated in order to put in place adequate protective measures to ensure that the consequences will not exceed established limits of water temperature, margins to criticality and radiological releases for AOOs.

Examples of AOOs are:

- LOOP;
- Malfunction of decay heat removal system;
- Leaking in the pool cooling system;
- Malfunctioning of the ventilation system.

AOOs are associated with the 2nd level of defence in depth. As for the reactor, AOOs are expected to occur during the lifetime of the plant. The essential measures to deal with AOOs are emergency power systems for the case of LOOP and procedures to recover failures and malfunctions. The large mass of water in the pool provides a large time for such processes although, when a full core has just been unloaded from the reactor vessel and transferred to the pool, such time is significantly shorter.

5.3 ACCIDENT CONDITIONS

Equipment failures of lower frequency of occurrence than those categorized in AOO are expected also to be identified and postulated, in particular those leading to loss of the pool cooling or coolant, spreading of radioactive materials or approaching to criticality. They fall into the category of accidents, associated with the 3rd level of defence in depth.

In most of the current designs the systems that run during NOs such as the heat removal system and the ventilation systems also have the capability to deal with some postulated abnormal conditions and accidents. The normal heat removal system is generally designed with characteristics similar to safety systems, e.g. redundant design to satisfy the single failure criterion, powered by the on-site emergency AC power system, cooled by a safety heat transfer system, seismically qualified, etc. In fact, SSR-2/1 [1] doesn't require explicitly an additional dedicated system to deal with the loss of the normal cooling system. This is justified by the long time necessary to uncover the top of the fuel in case of loss of cooling because of the large thermal inertia of the water in the pool. Some designs have however, a separate standby cooling system, acting as a backup system, in case the normal cooling system fails.

5.3.1 Single initiating events

Some generic accidents that are initiated by single failure events could be:

- A break of a piping connected to the water of the pool;

- The drop a fuel element during fuel handling.

Essential means to mitigate these accidents are:

- Piping layout and anti-siphoning devices to prevent drainage below the minimum water level required for shielding in case of pipe breaks. Procedures to recover fuel cooling and to keep the fuel always submerged in water.
- The ventilation system.

The concept of DBAs can be applied to the design of systems for the spent fuel storage but some adjustments are necessary. As indicated before systems for NO have some characteristics of safety systems. The ventilation system has the capability to remove and retain the radionuclides released from the fuel assuming that some rods can be damaged, for example, by dropping a fuel element during the fuel handling. The ventilation system has an emergency mode (filtered system) that would be activated for instance if a fuel element is dropped and damaged. This event can be considered as DBA for the ventilation system.

5.3.2 Multiple failure events

Multiple failure events leading to loss of cooling of the SFP also need to be considered and their consequences analysed with account taken of their likelihood.

The essential means to respond to these multiple failures are:

- The backup cooling system, provided in some new designs;
- Procedures to recover the pool cooling and ensuring sufficient water level in the pool.

Depending on the design, the loss of cooling can occur due to a number of multiple failures that could also be considered as DEC for the reactor, such as SBO, or the loss of systems for transferring residual heat to the ultimate heat sink. Taking into account that the time allowed for the recovery of the functions for the pool is much longer, the design bases of safety features for DEC for the reactor might also be appropriate for the DEC considered for the SFP.

All the provisions for the single and multiple failure events would constitute the essential design and operational means of level 3 of defence in depth.

Moreover, the revised SSR-2/1 [1] requires provisions for connecting non-permanent equipment to maintain the water level in the pool to facilitate the accident management in case provisions for DEC would fail.

Accidents with significant fuel degradation in the SFP are considered to be practically eliminated (see Section 7).

Requirement 6.68 of SSR-2/1 [1] does not make a difference between SFPs outside or inside the containment and requires the prevention of fuel uncover, so as to practically eliminate the possibility of early or large releases. Considering that the number of fuel assemblies in a SFP is in general more numerous than in a reactor core, significant damage of the fuel could result in a large source term. Therefore, a large release is possible if confinement is not effective. This means that, in any case, all sequences that could potentially lead to significant fuel degradation have to be practically eliminated.

Therefore, there is no level 4 of defence in depth implemented in the design of the SFP. It is the objective of the safety analysis to demonstrate that the provisions implemented are sufficiently effective to exclude the need for means for the mitigation of fuel melt events. See Section 7 on practical elimination of large or early radioactive release for further explanations.

6. INDEPENDENCE OF LEVELS OF DEFENCE IN DEPTH

Paragraph 3.31 of SF-1 [2] states:

> 3.31. "The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'. Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment."

The paragraph above stresses two main aspects of defence in depth: the multiplicity of level of protection and the independence of these levels. These two aspects have been investigated at the IAEA and translated into safety requirements in SSR-2/1 [1] taking also into consideration the lessons learned from Fukushima Daiichi accident. The correct implementation of the requirements implies that the multiplicity of the levels of defence is not a justification to weaken the efficiency of some levels relying on the efficacy of others. In a sound and balanced design, SSCs of each level of defence are characterized by reliability commensurate to their function and their safety significance.

Regarding the independence, the full independence of the levels of defence in depth cannot be reached, due to several constraints, such as the common exposure to external hazards, the unavoidable sharing of some SSCs, e.g. the containment or the control room and ultimately the operating crew. Therefore since the independence of the levels of defence in depth is a goal that cannot be achieved, it would be more appropriate to speak about reducing the degree of dependence between the levels of defence in depth, but the term independence of defence in depth levels is commonly spread in the international community, including publications of the International Nuclear Safety group, the IAEA, the Western European Nuclear Regulators Association, the OECD Nuclear Energy Agency and others. Therefore, the interpretation and use of the term 'independence of the levels of defence in depth' needs to be understood as the 'degree of independence,' which needs to be at the highest level possible.

Multiple consecutive levels of protection achieve the objective of defence in depth if, following the failure of one level of defence, the subsequent level would not also fail for the same cause (full dependence). For this reason, SSCs serving different levels remains one of the main factors to threaten the overall efficiency of the defence in depth concept.

In general, to which extent the degree of independence of the levels of defence in depth is practically achievable is still an open issue that requires a significant effort to identify practical measures for a satisfactory implementation.

Requirement 7 of SSR-2/1 [1] on application of defence in depth states: "**The levels of defence in depth shall be independent as far as is practicable.**"

Following the review of SSR-2/1 Rev. 0 [1] to reflect the findings from the Fukushima accident in 2011, the following requirement has been added in SSR-2/1 [1]:

> 4.13A. "The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems."

Factors that affect the independence of levels of defence

In preventing the occurrence of PIE and mitigating their consequences at different levels of the defence in depth, it is important that safety provisions implemented at the different levels have reliability commensurate to their function and safety significance.

In order to ensure very low frequencies of sequences resulting in severe accidents or external releases, it is necessary to ensure that the effectiveness of the levels of defence is not diminished by factors that compromise the independence of the levels of defence in depth. These factors are:

- The sharing of systems or parts of them for executing functions belonging to more than one level of defence in depth. Examples of this type of dependences are the use of emergency core cooling pumps for primary coolant make up or the use of common support systems or part of them for NO and PIEs. Other examples can be the common power supply and component cooling water systems.

- The exposure of SSCs of different levels of defence in depth to failures due to common cause (e.g. internal or external hazards).

6.1 PREVENTION OF COMMON CAUSE FAILURES

Requirement 24 of SSR-2/1 [1] states that "**The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.**"

CCFs are relevant when they affect redundant equipment or provisions belonging to different levels of defence.

There is not a unique understanding and use of the term 'common cause' worldwide. Appendix 3 addresses the more general concept of dependent failures, from which CCFs are a subset. Nowadays, the term CCF is not used to designate for instance the failure of several components in a system due to the failure of a support system, e.g. power supply. This would be considered a functional dependence. Appendix 3 provides some insights on the types of dependent failures, including CCFs. It addresses also the root causes of CCFs, the coupling mechanisms and defensive measures that could be adequate for each of them.

Redundant equipment within a system is more exposed to commonalities in design, operational and maintenance practices. Other factors, such as internal or external hazards can affect several plant systems.

Safety systems, in general, rely upon redundancy, functional independence, robust design and physical separation to ensure high reliability. Diversity is usually a measure applied to reduce the likelihood of CCFs between different levels or sublevels (3a and 3b) of defence in depth, for instance turbine driven pumps (or isolation condenser) for AOOs and motor driven pumps for DBAs in some BWR designs.

Functional independence between different levels of defence in depth is an aspect that cannot be taken for granted as it has been a frequent practice to share systems between different levels of defence.

In SSR-2/1 [1] the emphasis is placed on reinforcing the degree of independence between different levels of defence in depth and in particular, the independence of safety features for DECs involving the melting of fuel, and safety systems.

Functional independence, diversity, for instance on instrumentation, power supply or heat sink, as well as stronger safety margins and protection against external hazards, are among the measures to prevent CCFs from stretching through different levels of defence in depth.

6.2 DESIGN FOR EFFECTIVE INDEPENDENCE OF LEVELS OF DEFENCE IN DEPTH

SSR-2/1 [1] stresses the importance of the independence of different levels of defence in depth and requires that the independence is implemented as far as practicable.

As mentioned before, it is recognized that a full independence is not achievable because too many structures, systems and components have to serve more than one level of defence. A typical example is the containment that has relevant safety functions in different levels of defence and cannot reasonably be duplicated or triplicated. However, independence is essential where concurrent failures of two levels would lead to early or large releases with harmful effects to people or to the environment.

Some considerations for the correct implementation of the Requirement 7: Application of Defence in Depth, of SSR-2/1 [1], are given below.

6.2.1 General considerations

- Items belonging to different levels of defence necessary to mitigate the consequences of a given PIE need to be identified;

- Independence between SSCs or safety features needs to be pursued through the identification of all dependences and their elimination to the greatest practicable extent;

- The safety analysis needs to demonstrate that the safety features intended to respond first are not jeopardized by the initiating event.

6.2.2 Specific considerations

- Vulnerabilities which could result in the total failure of the safety systems need to be identified and, if any, combinations with PIEs need to be considered to assess if they could escalate to a core melt accident. Usually, for each combination analysed, if the consequences exceed those acceptable for DBAs, separate, independent and diverse safety features (e.g. AC alternate power supply in case of the total loss of the standby diesel generators, or a separate and diverse decay heat removal chain, etc.) unlikely to fail for the same common cause need to be implemented to strengthen the defence in depth and to prevent core melt.

- Safety features designed to mitigate the consequences of core melt accidents need to be independent from equipment designed to mitigate DBAs.

- Level 3 needs to be independent from levels 1 and 2 as far as reasonably practicable. To avoid challenging excessively levels 3b or 4, the ability of the safety systems to perform their function would not be jeopardized by a postulated single initiating event, or by

failures of systems designed for NO and AOOs. This includes also shared support systems between these levels.

- Safety features for DEC that are designed to backup SSCs implementing safety functions, need to be independent from SSCs postulated to fail in the accident sequence.

- Multiple failures affecting a safety system are expected to be controlled primarily by the safety features implemented in level 3b.

- Systems designed to control AOOs would be independent from systems for NO as far as reasonably practicable. Generally, AOOs are controlled by non-safety systems and ultimately by the reactor trip system. The ability of the reactor trip system to perform its functions would not be jeopardized by a postulated single initiating event or by single equipment failure of systems designed for NO. Multiple failures resulting in the total loss of the reactor trip system are controlled by the diverse safety features implemented in level 3b (e.g. with DAS I&C system). Limitations systems (level 2) usually share components with the control systems. A full independence of these systems might lead to excessive complexity that is not justified by the benefits to safety.

6.2.3 Independence of levels of defence in depth in relation to I&C systems

I&C systems have a relevant role for performing safety functions in all levels of defence in depth. The correspondence between the different functions and the level of defence in depth together with some recommendations to enhance independence of different levels are summarized below:

- Level 1. To this level belong the functions necessary to operate the plant during normal operating modes and to maintain the main plant variables within the specified range.

- Level 2. To this level belong the functions to prevent AOOs from escalating into accident conditions. This level also includes the reactor trip function and the limitation functions. The limitation system is designed to control AOOs without activating the reactor trip as much as possible.

  Limitations functions (level 2) need to be separated from the operational I&C (level 1) to the extent feasible. Separation may not be implemented where it would lead to increase significantly the number of data transfer between these two I&C systems (e.g. between I&C controls and limitations where the controlled equipment is the same).

- Level 3. To this level belong the functions designed to automatically control design basis accidents without exceeding acceptance criteria and the functions designed to bring to and to maintain the reactor in safe shutdown following a DBA.

  Initiation of reactor trips and safety systems need to be processed in a separated and independent I&C system from the I&C systems used for operational states and the I&C systems used for level 3b. Provisions are necessary to ensure that failures of systems classified in a lower safety class will not prevent the reactor protection system (RPS) from performing its intended functions. Back up functions to prevent that combinations of PIEs with CCFs in the I&C systems escalate to a core melt accident belong to level 3b.

- Level 4. I&C systems dedicated to the mitigation and monitoring of a core melt accident need to be separated and independent from any other I&C systems. This requires the independence of their respective DC power sources.

To reduce the volume of data to exchange and communications within I&C systems, in existing designs, some I&C functions may be performed by a single I&C system. That may be the case for some control and limitation functions, or with the RPS which often processes both the reactor trips and the actuation of the safety systems. In that case the physical separation is not implemented but the functions need to be decoupled.

In I&C systems independence is intended to prevent the propagation of failures between redundant channels or from system to system and is achieved by implementing functional independence, communication independence and avoiding interconnections. If independence is not implemented, the data transfer needs to be secured and the shared signals decoupled (e.g. Data transfer between the redundant channels of the RPS are necessary for the voting logic). Physical separation is intended to prevent CCFs due to internal hazards.

6.2.3.1 Considerations on sensors

The efficacy of all four levels depends upon sensor response but this does not imply that all sensors must be independent or diverse. Nevertheless the independence between redundant trains of a safety system, and between systems assigned to different levels of defence in depth, must not be jeopardized by the sensors (e.g. redundant trains within a safety system must not share instrumentation).

The following considerations apply:

- Independence and diversity between the RPS and the Diverse Actuation System (DAS)[10] must not be impaired by sensors to the extent possible.
- Monitoring the key variables for the management of DBAs and DECs without significant fuel degradation would also be possible using sensors different from those used to initiate the operation of the safety systems and DEC safety features respectively. To the extent possible sensors used for the protection and for the monitoring would not fail because of a common cause.
- Monitoring the key variables for the management of core melt accidents need to be to the extent possible performed by dedicated sensors, and in particular it need not be dependent on the DC source used for DBA management. Sharing sensors with other defence in depth levels may be acceptable provided the sensors are qualified for the environmental conditions prevailing in case of a severe accident and an adequate number of redundant sensors are implemented with effective separation and independence. In this case the shared sensors need to provide input to different I&C systems only through appropriate buffering and isolation devices. The I&C backup system (DAS) needs to be separated, independent and diverse from the RPS.
- Sharing sensors between levels 1, 2 and 3a may be acceptable provided an adequate number of redundant sensors are implemented with effective separation and independence. In this case the shared sensors need to provide input to different I&C systems only through appropriate buffering and isolation devices.

[10] Annex III of the IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [13] addresses the topic and the current practices of Member States in detail.

- For the automatic actuation of safety systems or for the monitoring of plant parameters in accident conditions, it is a good practice to rely on different physical parameters to reduce the consequences of failure of sensors due to common causes.

6.2.3.2 Considerations on the use of diverse actuation system (DAS)

The demonstration that I&C systems using software or hardware description language (HDL) are error free is very difficult. Therefore, for new plants it is common practice to postulate CCF in I&C systems that are using the same software or hardware language. In this case protective functions necessary to cope with a failure of the RPS need to be processed by an additional independent and diverse I&C system (DAS).

The design of the DAS is based on the analysis of the consequences of postulated multiple failures that could prevent the initiation of mitigation actions. The analysis needs to consider the likelihood of the combinations of the CCF with PIEs, but usually, the failure of processing the protection signals is considered as the bounding case. In that case, functions based on different signals and on different functional requirements can be credited in the analysis. If the consequences exceed the acceptance criteria established to prevent significant core damage, a backup signal that is not subjected to the same CCF, needs to be generated. Back up signals also need to prevent the initiating event from escalating to a core melt accident. In the estimate of the consequences, the plant response may be modelled with less conservatism than for DBA analyses.

7. THE CONCEPT OF PRACTICAL ELIMINATION

7.1 INTERPRETATION OF THE CONCEPT

The term 'practically eliminated' was originally introduced in the IAEA publications in INSAG-12 [3] in 1999 and then, this term was used, for the first time in the IAEA Safety Standards Series No. NS-G-1.10, Design of Reactor Containment Systems for Nuclear Power Plants [7] which deals with the design of reactor containment systems and it was published in 2004. NS-G-1.10 [7] also includes the following explanation:

> "In this context, the possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise."

This explanation also adopted in SSR-2/1 Rev.1 [1], has not been included in the IAEA Safety Glossary [4].

The 'certain conditions' meant to be addressed in NS-G-1.10 [7] include accident sequences of very low probability involving very energetic phenomena the consequences of which could not be mitigated with implementation of reasonable technical means, and that could lead to early or large radioactive releases due to containment failure or bypass.

The definition above is based on two concepts of different nature. The first concept is of deterministic nature on the consideration of the physical impossibility (in practice limited to very specific cases), and the second concept is of probabilistic nature and implies the use of probabilistic methods to assess that the probability of a condition is very low (extremely unlikely), and the degree of confidence of the probability estimate is very high.

Paragraph 2.11 of SSR-2/1 [1] states that:

> 2.11. "The design for safety of a nuclear power plant applies the safety principle that practical measures must be taken to mitigate the consequences for human life and health and for the environment of nuclear or radiation accidents (Principle 8 of the Fundamental Safety Principles [2]). Plant event sequences that could result in high radiation doses or in a large radioactive release have to be 'practically eliminated' and plant event sequences with a significant frequency of occurrence have to have no, or only minor, potential radiological consequences. An essential objective is that the necessity for off-site protective actions to mitigate radiological consequences be limited or even eliminated in technical terms, although such measures might still be required by the responsible authorities."

The term is also used in the following requirements of SSR-2/1 [1]:

> 4.3. "The design shall be such as to ensure that plant states that could lead to high radiation doses or to a large radioactive release have been 'practically eliminated'."

> 5.27. "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'."

5.31. “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’.”

The concept of ‘practical elimination’ must not be misinterpreted or misused. It is to be considered as part of a general approach to safety and its appropriate application as an enhancement of defence in depth. The ‘practical elimination’ is achieved by prevention of the conditions that could lead to an early radioactive release or a large radioactive release.

As a first step for the implementation of design provisions for the practical elimination of undesired conditions it is necessary to identify what are these conditions and then for each of them specify the design provisions.

The accident sequences that have a potential to lead to early or large releases involve both severe damage of the reactor core and the loss of the containment integrity or containment bypass. Early or large releases could also be caused by severe damage of spent fuel that is in storage or in transfer outside the reactor containment (see Section 5).

There is still discussion in several Member States on the actual conditions for which the practical elimination needs to be pursued. The text below, which is an elaboration of what already included in NS-G-1.10 [7], need only be considered as a contribution to promote the discussion and to achieve consensus:

6.5 “The consideration of severe accidents should be aimed at practically eliminating the following conditions:

- Severe accident conditions that could damage the containment in an early phase as a result of direct containment heating, some steam explosions or large hydrogen detonation;
- Severe accident conditions that could damage the containment in a late phase as a result of basemat melt-through or containment excessive pressure;
- Severe accident conditions with an open containment — notably in shutdown states;
- Severe accident conditions with containment bypass, such as conditions relating to the rupture of a SG tube or an interfacing system LOCA”.

For practical purpose, the cases to be addressed for ‘practical elimination’ could be grouped within the following five categories:

1. Events that could lead to prompt reactor core damage and consequent early containment failure:
    a. Failure of a large component in the reactor coolant system (RCS);
    b. Uncontrolled reactivity accidents.
2. Severe accident phenomena which could lead to early containment failure:
    a. Direct containment heating;
    b. Large steam explosion;
    c. Hydrogen detonation.
3. Severe accident phenomena which could lead to late containment failure:
    a. Molten core concrete interaction (MCCI);
    b. Loss of containment heat removal.
4. Severe accident with containment bypass;
5. Significant fuel degradation in a storage pool.

Some of these categories entail very severe challenges to the integrity of the physical barriers for radionuclide retention and require specific and very strong design and operation provisions for their practical elimination. The practical elimination can be considered as a design process followed by the necessary inspection and surveillance processes during manufacturing, construction, commissioning and operation. The demonstration of practical elimination is based on and assessment of such provisions, that would necessarily include engineering, deterministic and probabilistic judgement.

The technical measures to prevent each of these situations from occurring need to be provided and their effectiveness needs to be analysed. None of the phenomena mentioned above can be overlooked on the arguments on low likelihood but credible research results and dedicated means to eliminate the identified risks are necessary to support the safety claims.

There is a quite wide consensus on the view that the 'practical elimination', even involving probabilistic considerations, always needs to be based on solid design provisions and supported by deterministic assessment and engineering judgement.

Each of the above hypothetical accident conditions is discussed in more detail in Appendix 4.

7.2 SAFETY DEMONSTRATION

7.2.1 Physical impossibility

Where a claim is made that it is 'physically impossible' for the conditions to arise that could lead to an accident condition that needs to be 'practically eliminated', it is necessary to examine the inherent safety characteristics of the system or reactor type to demonstrate that the event cannot, by the laws of nature, occur and that the fundamental safety functions (see Requirement 4 of SSR-2/1 [1] of reactivity control, heat removal and limitation of accidental radioactive releases will be achieved.

7.2.2 Extremely unlikely conditions

Although probabilistic targets can be set, 'practical elimination' from the need for consideration cannot alone be demonstrated by showing the compliance with a general probabilistic value. The achievement of any probabilistic value cannot be considered a justification for not implementing reasonable design or operational measures. The low probability of occurrence of an accident with core melt is not a reason for not protecting the containment against the conditions generated by such accident. Core melt conditions need to be postulated regardless the provisions implemented in the design and the energetic phenomena associated with the core melt need to be prevented to exclude containment failure.

The 'practical elimination' from consideration of accident situations that could lead to large or early releases has to be demonstrated by deterministic considerations supported by probabilistic considerations, taking into account the uncertainties due to the limited knowledge of some physical phenomena.

It is a decision of the regulatory body to establish or not what are acceptable targets to support the demonstration of practical elimination.

For new designs which adopt the latest technological solutions for a strong implementation of defence in depth, it is expected that a large or early release frequency below 10^{-6} per reactor year could be achieved for events of internal origin.

When it is claimed that a particular accident condition of those described above has been practically eliminated making use of probabilistic arguments, it needs to be taken into account that the cumulative contribution of all the different cases must not exceed the target for large or early release frequency established by the regulatory body.

For some external hazards it may not be not practical or even possible to demonstrate that the occurrence of a hazard of such severity that could cause extensive plant damage leading to a large or early radioactive release, and therefore needing to be practically eliminated, is below a threshold of frequency such as 10^{-6}/year.

This shows the limitations of probabilistic methods to claim the demonstration of the 'practical elimination'. For this reason, it is advisable to keep the 'practical elimination' concept for external hazards separate from those associated with internal plant sequences. The design for external hazards is addressed in Section 9.

8. CLIFF EDGE EFFECTS AND SAFETY MARGINS

One important issue in the understanding of the design basis of plant equipment involves the use of safety margins and how they relate to cliff edge effects. In SSR-2/1 [1], the need to include margins in the design is addressed in the following requirements:

> 4.11. "The design: … (b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect."

> 5.21A. "The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site."

SSR-2/1 [1] also requires that the existence and adequacy of the different margins is demonstrated in the safety assessment of the plant:

> 5.73. "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 and early radioactive releases or large radioactive releases."

In this section the concepts 'cliff edge effect' and 'safety margin' are discussed to provide a more detailed understanding of the requirements above. Both terms are closely linked, as sufficient margins will contribute to the robustness of the design and prevent cliff edge effects in all plant states.

8.1 CLIFF EDGE EFFECTS

The concept of 'cliff edge effect' was intensively used after the accident at the Fukushima Daiichi NPP. This publication provides a short discussion to facilitate the interpretation of the requirements of SSR-2/1 [1].

The definition of cliff edge effect in the IAEA Safety Glossary [4] is:

> "In a nuclear power plant, 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."

Hence, cliff edge effects imply consequences of high relevance following a small deviation in a 'plant parameter' [11].The worst case would have a large release as the consequence. Other cliff edge effects would be the failure of a barrier or the occurrence of a severe accident. A physical barrier could fail if the safety functions protecting the barrier fail as a result of the change in the input parameter.

[11] The term plant parameter in the IAEA definition of cliff edge effect, needs to be interpreted in a broad sense, as any plant physical variable, design aspect, equipment condition, magnitude of a hazard, etc., that can influence equipment or plant performance.

It is possible that a cliff edge effect occurs if the deviation in a parameter affects the functionality of a key SSC in the plant, e.g. the containment. In general however, cliff edge effects are more likely to occur when the parameter has the potential to affect the functionality of many SSCs at once (e.g. flooding exceeding the design value). The safety assessment has to prove that there are adequate margins to avoid cliff edge effects. For this purpose, it is not always necessary to determine the magnitude of the deviation of the value of the parameter that could eventually lead to a cliff edge effect.

8.2 SAFETY MARGINS[12]

The terms 'margin' and 'safety margin' are not defined in the IAEA Safety Glossary [4].

SSR-2/1 [1] refers in general to 'margins' and other safety standards such as the IAEA Safety Standards Series No. GSR Part 4, Safety Assessment for Facilities and Activities [15] refer to 'margins' and to 'safety margins' without any specific difference between the two terms. In this publication the terms 'margins' and 'safety margins' are used as synonyms and the definition proposed[13] is derived from the definition of safety margin in the IAEA-TECDOC-1332 [8].

This publication provides a short description of the meaning of the term and the purpose of using the concept of margin for the design of new NPPs as a measure to prevent the occurrence of cliff edge effects.

The safety margin is understood as the result of the conservative assumptions and conservative rules applied for the design that provides the structures, systems and components the capability to safely perform even in situations more severe than those postulated in the design basis without the incurrence of cliff edge effects.

Figure 3 shows in a simplified scheme the concept of margin (safety margin) used in SSR-2/1 [1].

Figure 3 shows that, in general, there are uncertainties on the knowledge of the value of any calculated parameter as well as on the value of the parameter that can produce cliff edge effects. These uncertainties are also reflected on the knowledge of the safety margin. In Figure 3 there is no attempt to define the different components of the margin for which different terms and definitions are used by different Member States.

In general the assessment of safety margins is a complex problem for which several deterministic and probabilistic techniques are available.

Adopting margins in the design of a NPP is a common practice to improve the robustness of the design and providing an effective mean to deal with uncertainties. However, the extension of the design basis with the introduction of DECs has introduced new elements that need to be addressed. In addition, the Fukushima Daiichi accident has reinforced the importance of the effects of external events and, because of the uncertainties associated with their

[12] Detailed discussions on margins for existing reactors are available in documents from IAEA TECDOC-1332 [8] and OECD/NEA [9].
[13] Amended definitions and new definitions proposed for inclusion in the Glossary are collected in Section 12.

determination, also the importance of adequate safety margins to cope even with events of magnitude exceeding the design basis[14] derived from the site evaluation[15].

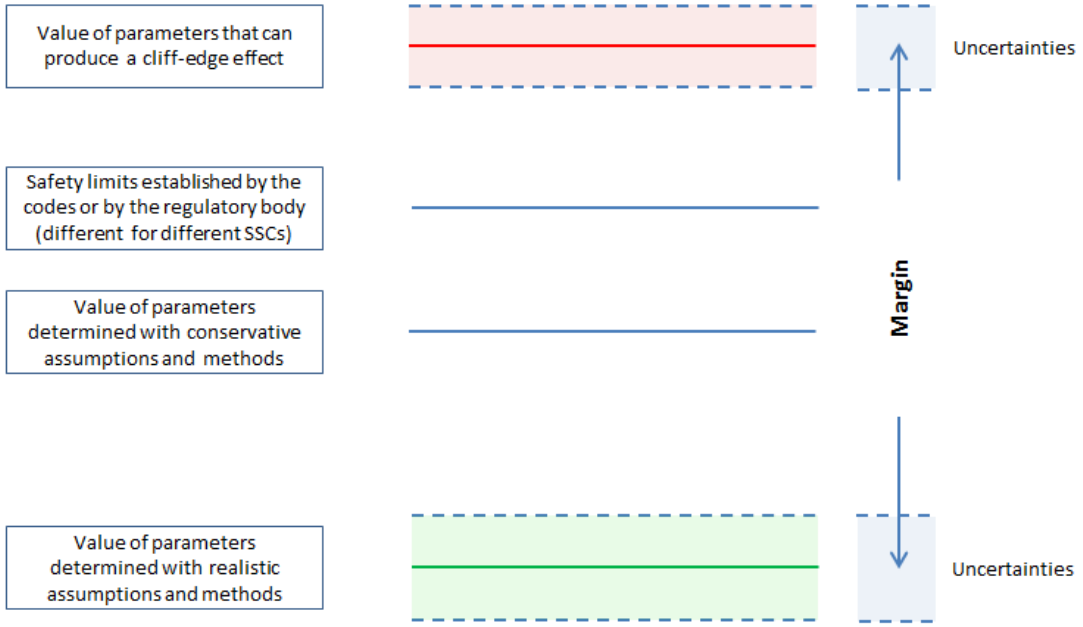

FIG. 3. Margin (safety margin) and cliff edge effects.

8.3 SAFETY MARGINS FOR DESIGN BASIS ACCIDENTS

DBAs are used as boundary conditions to establish the design bases of the safety systems following a conservative approach. The conservative approach implies the use of conservative models, penalizing rules and plant parameters to make sure that the objective are met despite the uncertainties in the modelling of the plant response and in the performances of the equipment.

DBA conditions are calculated taking into account the less favourable initial conditions and equipment performances, and taking into account the single failure affecting the most the global performance of the safety system.

With regard to the design of structures and components, margins result from both the methodology followed to define the loading conditions and compliance with the stress limits defined by the design/manufacturing codes. The methodology to define design loading conditions usually follows a conservative approach assuming the less favourable initial conditions and equipment performances to maximize the loads. Meeting the stress limits established by proven codes is generally a proof for justifying the structural integrity in the different plant states. This proof is generally supplemented by some tests to justify the operability of equipment.

[14] Section 9 provides an interpretation of the requirements of SSR-2/1 [1] for the design for external hazards.
[15] The initial site evaluation may be revised, for instance as part of a periodic safety review, for taking into account knowledge or modelling or the occurrence of an expected event. Therefore, it may be prudent to have a margin available in case the hazard derived from the site evaluation evolves in time.

The possibility of cliff edge effects need to be investigated and necessary margins have to be added to increase the capability of the SSCs and to cope with possible changes during the lifetime of the NPP.

8.4 SAFETY MARGINS FOR DESIGN EXTENSION CONDITIONS

According to SSR-2/1 [1] Requirement 20, the analyses of the DECs may be performed using realistic assumptions. 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.

In the design of equipment for DECs, the loads are often defined in a similar way as for DBA, but using a best estimate approach for determining the accident scenario and the environmental conditions. Stress limits justifying the integrity or operability of equipment may be less conservative than those used for DBAs and would be based on those reasonable expectations for performance of the equipment.

For DECs without significant fuel degradation the uncertainties are likely to be similar to those for DBAs, while for DECs with core melt, the uncertainties are likely to be much larger than those for DBAs. Therefore, in the safety margins there could be a substantial difference between those for DECs without significant fuel degradation and those for DEC with core melt.

9. DESIGN FOR EXTERNAL HAZARDS

In relation to external hazards, SF-1 [2] recognizes the selection of an adequate site for the NPP as an important aspect of the defence in depth. External hazards have the potential to trigger initiating events, to cause failures of equipment needed to mitigate them and also to adversely affect directly or indirectly the barriers to the release of radioactive materials. The site selection and site characterization is not considered explicitly as a level of defence in depth, but is an essential input for the design of SSCs associated with all the levels, including infrastructure that may be required for emergency planning and response. In relation to external hazards the site selection aims at selecting a site that is less prone to natural and human induced external hazards both in terms of intensity and frequency of occurrence. This results in fewer and less severe challenges to the design of plant SSCs.

The design of NPPs includes due consideration of those external events that have been identified in the site evaluation process. All foreseeable external hazards need to be identified and their effects evaluated. The derivation of the design bases of SSCs for external hazard is part of the site evaluation process and the requirements related to this are provided in the IAEA Safety Standards Series No. NS-R-3, Site Evaluation for Nuclear Installations [10]. In particular, NS-R-3 Rev. 1 [10] requires that:

> 2.7. "The hazards associated with external events that are to be considered in the design of the nuclear installation and in its safety assessment shall be determined. For an external event (or a combination of events) the parameters and the values of those parameters that are used to characterize the hazards shall be chosen so that they can be used easily in the design of the installation and in its safety assessment."

There are several alternatives for the derivation of the design basis of plant SSCs for external hazards depending on the hazard and the characteristics of the site region. These alternatives, considered in NS-R-3 [10] and associated Safety Guides include deterministic, probabilistic or hybrid approaches.

In general, the term 'plant design' includes also the plant grade and the plant layout, which are important in relation to external hazards. Site protection measures, on the other hand, include such features as sea walls, pressure barriers, dykes, etc., which may not be part of the plant SSCs but need to be designed and constructed with due consideration that they will be performing safety functions.

As discussed in Section 2, DECs are a specific category of plant states. However external events exceeding the values specified in the design basis derived from the site evaluation and their associated loads are not postulated plant states. For this reason they are not included in the current definition of DECs, which are accident conditions used to introduce in the design of the NPP the consideration of postulated sequences of events typically caused by multiple safety systems failures, failures which may or not be induced by an external event. For external events that exceed the design basis, derived from the site evaluation i.e. the magnitude for which the safety systems are designed to remain functional both during and after the external event, the term 'Beyond Design Basis External Event' (BDBEE) is proposed and used in this publication.

Paragraph 5.21A of SSR-2/1 [1] requires that:

> 5.21A. "The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive

release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site."

SSR-2/1 [1] imposes more demanding requirements for the protection against external natural hazards for equipment ultimately necessary to prevent an early radioactive release or a large radioactive release. The design of these items is expected to be particularly robust and to include margins to withstand loads and conditions generated by natural external hazards exceeding those derived from the site evaluation. This implies that an early radioactive release or a large radioactive release is to be prevented not only for small variations but also for significant variations of the loads and conditions. This has the purpose to ensure that if a severe accident were to occur owing to an external hazard (similar to the case of Fukushima Daiichi NPP[16]) there are appropriate assurances that sufficient mitigatory means would be available to avoid an early or large release. The possibility that a subsequent level of defence in depth (e.g. level 4) may be impaired before the previous one (e.g. level 3), is contrary to the defence in depth logic. The above provision is needed because external hazards may challenge levels of defence in depth without regard to their order.

The implications of the requirement above have not yet been formally addressed in any safety standard of the IAEA, but it is clear that there are some important issues to be addressed and resolved. In particular, it is necessary to compile the list of the equipment ultimately necessary to prevent an early radioactive release or a large radioactive release and then to provide guidance on the external events to include in the design basis of these equipment and on the rules for their design and qualification, and for the assessment of the margins.

9.1 EQUIPMENT ULTIMATELY NECESSARY TO PREVENT AN EARLY RADIOACTIVE RELEASE OR A LARGE RADIOACTIVE RELEASE

SSCs ultimately necessary to prevent an early radioactive release or a large radioactive release refer to equipment of the fourth level of defence in depth and in particular to some of the SSCs necessary to mitigate the consequences of accidents with core melt. A detailed list of these SSCs is design dependent, however, in general they include at least:

- Containment structure;
- Systems necessary to contain the molten core and to remove heat from the containment and transfer heat to the ultimate heat sink in severe accident conditions;
- Systems to prevent hydrogen detonations;
- Alternative power supply (alternative to the emergency power supply);
- Supporting and I&C systems to allow the functionality of the systems above;
- Control room[17].

For instance, if flooding is considered as the external hazard, this would mean that either all the structures hosting the above mentioned systems are located at an elevation higher enough above the beyond design basis flood, or adequate engineered safety features (such as water tight doors etc.) would be in place to protect these structures and ensure that mitigating actions can be maintained.

[16] Note that severe accidents, i.e. DECs, were not part of the plant design envelope

[17] The control room is an item for which SSR-2/1 [1] explicitly requires margins for natural hazards more severe than those included in the design basis; SSR-2/1 [1] Requirement 6.40a: *The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.*

9.2 DESIGN FOR NATURAL EXTERNAL HAZARDS EXCEEDING THE DESIGN BASIS VALUES DERIVED FROM THE SITE EVALUATION

It is expected that the frequency of occurrence of a natural hazard significantly more severe than that considered for the design of plant be very low. This gives confidence for the appropriate selection of the design basis hazards.

The compliance with paragraph 5.21A of SSR-2/1 [1] requires that the SSCs ultimately necessary to prevent early or large releases be still operable in case of external natural events exceeding those to be considered for design taking into account the site hazard evaluation.

The following options are available to comply with paragraph 5.21A of SSR-2/1 [1]:

1. To adopt a higher magnitude of the design basis event for the SSCs ultimately necessary to prevent an early radioactive release or a large radioactive release.

2. To demonstrate, following a best estimate approach that values of parameters for which cliff edge effects would occur are not reached because of adequate safety margin. For this purpose, the demonstration needs to include the determination of the severity of the event and the probability at which the cliff edge effect would occur.

The approach to be followed will depend on the nature of the hazard and the function of the SSCs and has to be decided by the plant designer and the safety authority.

The probabilities of external hazards exceeding a well-established design basis derived from the site evaluation are very low and generally associated with significant uncertainties. It is important to understand the behaviour of the plant SSCs to levels of the loading parameters associated with BDBEE. How much exceedance is needed to adequately understand this behaviour depends on the aleatory and epistemic uncertainties associated with these parameters, the potential evolution of these parameters through time (non-stationarity), and the tolerance of plant SSCs to increased levels of the external event under consideration.

The safety margins to be taken for the various external hazards depend on certain attributes of these hazards. As already mentioned their potential for causing cliff edge effects and the uncertainties in their assessment play an important part in the margins needed. Other factors that may impact the margin to be considered would involve:

- Possibility of warning – Warning may be in terms of hours or minutes depending on the hazard. However, even when the warning lead time is very short, this may be valuable because it takes a very short time to scram the reactor.
- The maturity of the subject matter and the collective experience of the nuclear community to deal with the specific hazard is also an important factor.
- Potential for combination with other external hazards — when there is a dependence between the two events it is important to understand and consider this dependence.
- Potential for concurrent internal events (fire/flood).
- Extent of the common cause – physical separation possibilities. This is one of the most important attributes of an external event that may lead to a serious challenge to multiple layers of defence in depth (and causing dependences in the defence in depth).

Most experience related to this type of evaluation is on the subject of seismic safety. Practice in low-to-medium seismicity countries considers an increase of about 50% above the design basis seismic levels for evaluating the beyond design basis earthquake. This would mean that

a plant must not get into a core damage situation when the seismic demand is increased to 1.5 times the seismic level 2 (SL-2), the one imposing the most stringent safety requirements in the plant design. This evaluation may make use of a different set of safety and behaviour limit criteria.

Conservative safety margins have to be associated with the design basis evaluation for all external hazards and environmental factors such as air/water temperature, etc. This is because at the levels of 10^{-4}/y corresponding to external event design bases there is a lack of data and the values cannot be based on frequency considerations only. This forces the analyses to be model based and phenomenological, which introduces epistemic uncertainties into the process. Together with the aleatory uncertainties already present in the nature of the hazard, the design basis estimates start becoming driven by uncertainties. This requires ample margins to be considered in design. In addition, hazards beyond the design basis need to be taken into account for the consideration of the cliff edge effects.

Some plant SSCs are designed for the loads originated by accident conditions and external hazards. The eventual margin that is incorporated into the design can be determined from the sizing and the support of the SSC under consideration. As an example, if for the containment structure the governing loads are due to airplane impact, there may be a larger margin in the design for withstanding the loads resulting from an accident, e.g. a LOCA.

The design against external hazards needs to be such that a design basis external hazard does not lead to accident conditions. The evaluation of the design basis external hazards and the associated design aspects need to be conservative including significant safety margins.

Acceptance criteria related to BDBEEs need to be compatible with the DEC criteria. Evaluation of the BDBEEs and the design features associated with the BDBEEs could be based on best-estimate considerations.

10. USE OF NON-PERMANENT EQUIPMENT FOR ACCIDENT MANAGEMENT

SSR-2/1 [1] includes three requirements on use of non-permanent equipment.

> Paragraph 6.28B: "The design shall also include features to enable the safe use of non-permanent equipment for restoring the capability to remove heat from the containment."
>
> Paragraph 6.45A: "The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply."
>
> Paragraph 6.68: "The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation."

The design needs to be such that all conditions considered in the design are taken care of by safety systems and safety features installed at the unit. There must not be any need for additional equipment to comply with the acceptance criteria established for each plant state.

Non-permanent equipment may be considered as complementary 'essential means' to facilitate accident management, i.e. as additional means that may be valuable in situations not covered by DECs.

According to the safety approach of the IAEA, the non-permanent equipment needs to be considered as robustness provisions to cope with conditions exceeding those considered for the design. For such situations, minimizing the radiological release and avoiding long term off-site contamination of large areas are the objectives that need to be achieved.

Credit to the use of non-permanent equipment as an accident management measure may be given only if their installation and putting into service is possible in the time available before unacceptable consequences occur. The ability to deliver the equipment on time needs to be demonstrated also for conditions involving significant degradation of off-site transport infrastructures associated with extreme natural disasters.

The crediting of the use of non-permanent equipment needs to involve comprehensive commissioning tests that are used to verify the procedure for their connection and intended use. This is especially important for the safe connection of the electrical supply. The upkeep of practical skills for installation of non-permanent equipment needs to be ensured in emergency exercises simulating accident conditions.

Moreover, the flexibility to cope with different scenarios brought by the use of non-permanent equipment without increasing the complexity of the design also needs to be considered. The coping time, installation time and flexibility are the key parameters to decide whether complementary equipment needs to be pre-installed at the site or stored in a remote storage facility. The location of non-permanent equipment in places separated from the points where their function is required can be of advantage in the case of some external hazards, which could otherwise affect the non-permanent equipment.

There are already examples of non-permanent power sources (SSR-2/1 [1], paragraph 6.45A) and non-permanent equipment for cooling (SSR-2/1 [1], paragraph 6.28B, 6.68) implemented on existing operating reactors.

11. RELIABILITY OF THE HEAT TRANSFER TO THE ULTIMATE HEAT SINK

The possible 'loss of the ultimate heat sink' has been typically described as one of the important issues of the Fukushima Daiichi accident that would necessitate considerations for safety enhancement.

The IAEA Safety Glossary [4] defines the ultimate heat sink as:

> "A medium into which the transferred *residual heat* can always be accepted, even if all other means of removing the heat have been lost or are insufficient. This medium is normally a body of water or the atmosphere."

Requirement 53 on Heat transfer to an ultimate heat sink of SSR-2/1 [1] requires that "the capability to transfer heat to an ultimate heat sink shall be ensured for all plant states." Requirement 70 on Heat transport systems also addresses the need for removing the heat from systems and components that are required in operational states and accident conditions. Therefore, in this context the heat to be removed is to be understood as the summation of decay heat in both the reactor core and the spent fuel, and the heat to be removed from a number of components important to safety in order to maintain their operability.

Although mechanisms have been identified for the loss of the ultimate heat sink in a strict sense, including for instance the clogging of the plant water intake filters, in a broad sense, the loss of the ultimate heat sink is understood not only as the loss of the ultimate heat sink itself but also as the failure of the SSCs that transfer the heat to the sink.

Depending on the particular plant design, such SSCs for transferring heat to the ultimate heat sink typically include a chain of cooling systems generally known as cooling water and service water systems. More details on these systems are in Appendix 5.

The design bases of SSCs accomplishing the heat transfer to the ultimate heat sink need to be defined with sufficient margins against postulated external hazards and with high levels of reliability. Reliability of the heat transfer function can be ensured by a number of safety provisions, including high quality, redundancy, diversity, physical separation, etc. as appropriate. The reliability of the emergency core cooling system and other safety systems that depend on the heat transfer to the ultimate heat sink will also be always limited by the reliability of the heat transfer systems.

If the loss of the heat transfer chain has been selected as DEC, the safety features to backup the heat transfer chain need to be independent from the systems to remove residual heat used at the 3a level of defence. This may include the need for an alternate ultimate heat sink or connecting point as being currently required in SSR-2/1 [1]. Also, in the light of the foreseeable impact of external hazards on the plant through the cooling function, the requirement of high safety margins at least for some components of the heat removal systems needs to be considered in the design, to ensure that the safety function can be maintained even in case of natural external hazards exceeding those derived from the site evaluation.

12. TERMINOLOGY

The following terms and explanations are proposed for consideration in the preparation or revision of safety standards and so for possible inclusion in the IAEA Safety Glossary [4].

design basis of a structure, system or component (new)

The set of information that identifies conditions, needs and requirements necessary for the design of the structure, system or component including the:

- Functions to be performed by a structure, system or component of a facility;
- Conditions generated by operational states and accident conditions that the structure, system or component has to withstand;
- Conditions generated by internal and external hazards that the structure, system or component has to withstand;
- Acceptance criteria for the necessary capability, reliability, availability and functionality;
- Specific assumptions and design rules.

plant equipment (amended)

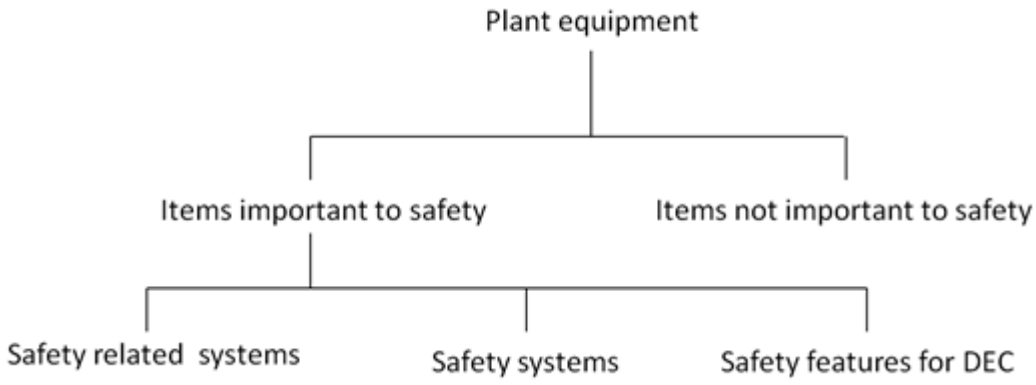

FIG. 4. Plant equipment

margin, safety margin (new)

The difference or ratio in physical units between the limiting value of an assigned parameter the surpassing of which leads to the failure of a structure, system or component, and the actual value of that parameter in the plant.

APPENDIX 1
EXAMPLES OF DESIGN EXTENSION CONDITIONS FOR LWR TECHNOLOGY

1. ANTICIPATED TRANSIENT WITHOUT SCRAM (ATWS)

The reactor trip system, including control rod insertion is fundamental to reactor safety for nuclear power plant (NPP) designs. All transient and accident analyses are predicated on its successful operation to show acceptable consequences. Operating experience from the 1970s suggested that these systems may be susceptible to common cause (multiple) failure that would threaten the safety of the plant.

Although an ATWS event is beyond the plant design envelope for most of the existing plants, new reactors designs include safety features for DEC that reduce the probability of ATWS events or/and mitigate their consequences. Examples of design features to accomplish this objective include alternate scram actuation systems, the use of sensors to detect an ATWS, and diverse and independent reactor shutdown systems.

2. STATION BLACKOUT (SBO)

Numerous studies have shown that a SBO event could be a relevant contributor to the total risk from NPP accidents in some countries. Although this total risk may be small, the relative importance of SBO events was established. This finding and the accumulated Diesel generator failure experience increased the concern about SBO, particularly in plants where the external grid is not very stable.

A SBO is defined in the IAEA Safety Standards Series No. SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [12] as a plant condition with complete loss of all AC power from off-site sources, from the main generator and from standby AC power sources important to safety to the essential and nonessential switchgear buses.

Reactors have to be designed with a realistic ability to withstand and recover from an SBO. In SSR-2/1 [1], the requirements related to SBO are delineated in Requirement 68. The specified duration needs to be based on the probable duration of the SBO.

The reactor core and associated coolant, control, and protection systems, including station batteries and any other necessary support systems, must provide sufficient capacity and capability to ensure that the core is cooled and appropriate containment integrity is maintained in the event of a SBO for the specified duration. The capability for coping with a SBO of specified duration shall be determined by an appropriate coping analysis. Plants are expected to document the baseline assumptions, analyses, and related information used in their coping evaluations.

3. LOSS OF CORE COOLING IN THE RESIDUAL HEAT REMOVAL MODE

The residual heat removal system (RHR) is designed to transfer thermal energy from the core after plant shutdown and maintain the plant in cold shutdown or refuelling conditions for extended periods of time. In several existing NPPs the RHR is a multiple use system with different modes of operation, some of them associated with the emergency core cooling (e.g. , emergency core cooling in recirculation mode and containment spray).

In PWRs, the cooling of the reactor and reactor coolant after shutdown is achieved by dissipating heat through the steam generators (SGs) until the values of pressure and temperature are low enough for the safe operation of the RHR. The RHR is cooled by the heat transfer chain systems that are designed to comply with the single failure criterion and taking into account the less favourable conditions. In cold shutdown conditions or during refuelling with the pressure vessel open, the heat removal through the SGs is not possible. The coping time necessary for restoring the heat removal following a failure of the residual heat removal system (RHR) depends on the reactor coolant temperature, the decay heat rate and the amount of coolant inventory. Decreased primary system inventory, in particular during middle loop operation, can significantly reduce the time available to recover the residual heat removal function prior to possible core uncover occurs. In new reactor designs, the loss of the RHR during shutdown is usually considered as DEC, and specific safety features for alternate residual heat removal are implemented in the design.

Other specific scenarios for the loss of residual heat removal are applicable to BWR or other designs.

4. EXTENDED LOSS OF FUEL POOL COOLING AND INVENTORY

Facilities for spent fuel storage at NPPs shall be designed to ensure that the potential for high radiation doses or radioactive releases to the environment are practically eliminated. Spent fuel pools (SFPs) are designed to maintain a large inventory of coolant to protect and cool the fuel under all plant conditions. SFPs are constructed with thick walls, floor, and stainless steel liner to help maintaining the coolant inventory and protecting fuel from the effects of natural phenomena.

Substantial inventories of irradiated reactor fuel in SFPs could pose safety concerns if there were a loss of coolant inventory or coolant supply. Requirement 20 of SSR-2/1 [1] generally, and Requirement 80 on fuel handling and storage systems specifically, detail the requirements that the design shall prevent the uncovering of fuel assemblies in the SFP so as to practically eliminate the possibility of early or large releases and to avoid high radiation fields on the site. Among the features for this purpose are:

- Providing redundant lines for pool cooling that eliminate possibility of long lasting loss of cooling function, i.e. for time needed to boil-off the water;
- Reliable instrumentation for pool level monitoring;
- Appropriate reliable means to compensate any loses of water inventory.

5. LOSS OF NORMAL ACCESS TO THE ULTIMATE HEAT SINK

The ultimate heat sink for the cooling water systems is that complex of water sources, including necessary retaining structures (e.g. a pond with its dam or a river with its dam) and the canals or conduits connecting the sources with the cooling water intake structure of a NPP. The ultimate heat sink performs two principal safety functions:

1. Dissipation of the residual heat after reactor shutdown and for the SFP;

2. Dissipation of residual heat after an accident.

As required by Requirement 6.19a of SSR-2/1 [1], the DBA design of the ultimate heat sink is very robust with the heat sink safety functions being provided by natural or manmade

features. In some cases, especially when relying on manmade sources, two water sources are prescribed unless the probability of losing one source is extremely low.

Nevertheless, as a result of Fukushima lessons learned, the additional design enhancement of the ultimate heat sink capability is often postulated involving a loss of normal access to the ultimate heat sink. This DEC involves the loss of ability to provide a forced flow of water to key plant systems (i.e., the pumps are unavailable and not restorable as part of a coping strategy). Generally, cooling and makeup water inventories contained in ultimate heat sink systems or structures are available given the different access requirements articulated in paragraph 6.19A of SSR-2-1 Rev. 1 [1] and given that the features are robust with respect to severe natural hazards as required in paragraphs 6.19B and 5.21A.

APPENDIX 2
EXAMPLE OF ACCEPTANCE CRITERIA FOR DIFFERENT PLANT STATES

The demonstration of adequacy of the design to cope with different plant states includes the demonstration of the compliance with the acceptance criteria[18], which are established, following a graded approach, for each plant state. The application of the graded approach leads to acceptance criteria more restrictive for events with higher probability of occurrence.

Acceptance criteria (we need to distinguish acceptance criteria in terms of level of redundancy, system design, behaviour limits for materials, etc. from acceptance criteria for radiological levels) are established in terms of acceptable radiological consequences and in terms of degree of integrity of barriers against releases of radioactive substances (fuel matrix, fuel cladding, reactor coolant pressure boundary (RCPB) or containment) – see Table 5.

High level criteria are typically expressed in terms of discharges or releases of radioactive material to the environment, whole body effective doses, equivalent doses for selected organs or tissues, and radioactivity or contamination levels of ground, water, crops and food items. Derived criteria are typically expressed in terms of surrogate variables determining integrity of barriers, such as pressures, temperatures, stresses, strains, etc.

Since the acceptability of radiological consequences is to a large extent related to off-site emergency response actions, it is reasonable to associate radiological safety objectives or acceptance criteria with emergency action levels (EALs) adopted for emergency measures.

Acceptance criteria for design need to be significantly lower than the EALs adopted for emergency measures.

The target would be to minimize the need for emergency measures

Paragraphs 5.25 and 5.31 of SSR-2/1 [1] provide the hint for a link between the design provisions and the EALs in GSR Part 7 [6] so that quantitative radiological acceptance criteria could be established.

Generic criteria for taking protective actions and other response actions to reduce the risk of stochastic effects in emergency exposure situations are provided in Appendix II of GSR Part 7 [6] as well as in the Annex of the IAEA Safety Standards Series No. GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [14] as follows:

- The generic criterion for sheltering and evacuation is 100 mSv of projected effective dose in the first 7 days.[19]
- The generic criterion for initiating temporary relocation is 100 mSv of projected effective dose in the first year.
- The generic criterion for iodine thyroid blocking is 50 mSv of projected equivalent dose to the thyroid only due to exposure to radioiodine.

[18] These acceptance criteria are to be understood as design targets rather than as regulatory acceptance criteria.
[19] As a less disruptive protective action, sheltering may be implemented at lower doses as long as justified and optimized in accordance with Requirement 5 with due consideration of the reference level in paragraph 4.28(2) of GSR Part 7 [6]. The reference level is typically set in the range 20–100 mSv of effective dose, acute or annual, and includes dose contributions via all exposure pathways.

TABLE 5. EXAMPLES OF ACCEPTANCE CRITERIA FOR DIFFERENT PLANT STATES

Level of defence	Objective	Associated plant state	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level 1	Prevention of abnormal operation and failures	Normal operation	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are bounded by the general radiation protection limit for the public (1 mSv /year[20] commensurate with typical doses due to natural background), typically in the order of 0.1 mSv/year.
Level 2	Control of abnormal operation and detection of failures	Anticipated operational occurrence	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are similar as for normal operation, limiting the impact per event and for the period of 1 year following the event (0.1 mSv/y)
Level 3a	Control of design basis accidents (DBAs)	Design basis accident	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel	No or only minor radiological impact beyond immediate vicinity of the plant, without the need for any off-site emergency actions. Acceptable effective dose limits are typically in the order of few mSv.
Level 3b	Control of DECs without significant fuel degradation (prevention of accident progression into severe accident)	Design extension condition without significant fuel degradation	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel.	The same or similar radiological acceptance criteria as for the most unlikely design basis accidents
Level 4	Control of DECs with core melt (mitigation of consequences of severe accidents)	Design extension condition with core melt (severe accident)	Maintaining containment integrity	Only emergency countermeasures that are of limited scope in terms of area and time are necessary[21]
Level 5	Mitigation of radiological consequences of significant releases	Accident with releases requiring implementation of emergency countermeasures	Containment integrity severely impacted, or containment disabled or bypassed	Off-site radiological impact necessitating emergency countermeasures

[20] See. GSR Part 3, Schedule III-3 [14].

[21] SSG-34 [12] provides more detailed guidance on interpretation of the limited scope of radiological consequences.

APPENDIX 3
DEPENDENT FAILURES

In the context of the design and safety assessment of a nuclear power plant (NPP) it is of particular relevance to minimize or eliminate the degree of dependence[22] between the occurrence of PIEs and the failure of the equipment or human actions designed to mitigate it, between failures of redundant system trains carrying mitigating functions and between failures of equipment associated with different levels of defence in depth, in particular between levels 3 and 4. Other dependent failures also need to be taken into consideration if possible, but their safety significance is much lower for instance in the case that they relate to non-redundant equipment.

For reducing the likelihood of these types of dependent failures, it is important to understand the different types of dependences and how are they treated in the plant safety assessment as well as the types of root causes and the defence measures that can be used in design and operation to prevent them. The analysis and classification of these types of dependences is useful in addition to establish a coherent terminology regarding the different kind of dependent failures.

PSA is particularly useful tool to address dependent failures, starting from the fact that all basic events postulated in PSA models are considered as statistically independent. To be able to make this assumption, the level of detail of the models needs to be sufficient to model all kind of sources of dependence explicitly. These sources of dependence can be categorized in the following categories:

1) *Functional dependences*

These are dependences of a component on its support systems, e.g. power supply, cooling, instrumentation, etc. The component becomes functionally unavailable or eventually fails (e.g. due to overheating) because of a support system failure. Such dependences cannot be eliminated as they are needed for the operation of the system. However, it is of importance for safety that redundant trains rely on different trains of support systems. This is established as a requirement for safety systems. It is necessary to ensure that swing trains in cooling system used in some design to support different trains of front line systems, don't introduce dependences of redundant trains on a common train of supply in a support system.

To this category belong also some subtle dependences on non-connected support systems, typically the ventilation or air conditioning system if it is needed for the functionality of the equipment, at least in the long term.

---

[22] Two events of any kind, A and B, as for instance failures of a component or a system in a nuclear power plant, are statistically independent if and only if:
$Probability\ (A \cap B) = Probability\ (A) \cdot Probability\ (B)$

Otherwise the two events are dependent and
$Probability\ (A \cap B) = Probability\ (A) \cdot Probability\ (B|A) = Probability\ (B) \cdot Probability\ (A|B)$

If $Probability\ (A \cap B) = Probability\ (A)$
or $Probability\ (A \cap B) = Probability\ (B)$
then the two events are fully dependent.

For three or more events, the condition of independence needs to be met by any double, triple, … combination of the events under consideration.

2) *Dependences through system interfaces*

In some designs some systems are connected to common lines of piping or tanks for delivering of flow or water supply, without constituting a functional dependence as discussed in the previous section. Similarities can exist in electrical systems regarding power buses. Thus the failure of a common line of piping or a valve, or the need to perform maintenance in the area of the interface may lead to a diversion of flow or render parts of different systems inoperable, normally of a single train. As example could be a common refuelling water storage tank (RWST) to high and low pressure emergency core cooling and containment spray with all these systems sharing a common line for each train. In this example, none of these systems is a support system of the other but a failure or maintenance in the interface area affects all of them. In some cases this kind of interface may exist with the same system

3) *Dependences between PIEs and mitigating systems*

Provisions need to be taken in the design such as physical separation, protections against dynamic effects, anti-whip equipment qualification, electrical protections, etc. to prevent or minimize the effects of the initiation events on plant SSCs. Notwithstanding some initiating events by their own nature may impair or diminish the reliability of equipment that could be called upon for its mitigation. This is the case for the LOOP, loss of some power buses inducing reactor scram or the loss of the main condenser. The design needs to be in such cases sufficiently robust to shut down the plant safely with the remaining equipment.

4) *Multifunction of systems and components*

Plant designs use some common systems or equipment for different functions that are often associated with different levels of defence in depth for the purpose of plant economy or design limitations. This is the case for the reactor scram system, for which it is practically not feasible to have separate systems for levels 2 and 3 or the use of parts of the emergency core cooling systems in the CVCS or the RHR system.

5) *Operation errors*

These are dependences in the performance of different plant equipment due to the actions of the operating crew. These actions are affected by both operational aspects, e.g. procedures, operator training, and design aspects, e.g. adequacy of instrumentation and man machine interface.

6) *Common cause failures*

CCFs are used to designate failures of two or more redundant[23] components of the same kind due to a number of different causes excluding those indicated before, that can take place simultaneously or close enough in time[24] for the redundant components to fail to fulfil their required function following a PIE. The cause of CCFs can be grouped as:

- Errors in design, manufacturing and construction;
- Errors or inadequate practices during maintenance, surveillance or inspection;

[23] Common cause failures of non-redundant components are not especially relevant as they are expected to be much less frequent than independent failures causing the same effect.
[24] Common cause failures can be latent or remain undetected until a given triggering condition takes place or the components are required to enter into function.

- Environmental or external factors resulting in conditions exceeding the margins of the design;
- Impact of internal or external hazards.

Behind most of these causes a human component can be identified. In fact, the real root causes of CCFs might not be evident and need in depth investigations. Frequently proximate causes of the failure are identified in the short term. They can lead to actual CCFs or incipient failures or degraded failure conditions, that if not timely identified may lead to CCFs. Finally ageing could be considered as an unavoidable common cause root cause affecting a wide range of components in the long term, for which adequate measures must be put in place.

In NUREG/CR-5460[25] an elaborated analysis of how root causes of CCFs linked by coupling mechanisms can lead to CCFs if defensive mechanisms are not in place or are inefficient, is presented. A synthesis of this analysis is presented here for helping to understand the development of CCFs and establishing the adequate design provisions in the design to ensure effective independence of the defence in depth levels an adequate reliability of the safety functions required at each level.

Wherever equal or similar components used in the design to provide redundancy, or more generally combination of failures of equal or similar components may allow the progression of a PIE, such kind of components are required to be considered for the analysis of susceptibility to CCFs. However, this general criterion may lead to an arduous work if no additional considerations are taken into account to reduce the groups of components that could realistically be affected by CCFs. Thus, is not practical to consider that a CCF could affect for instance check valves of the same size and manufacturer in the plant, although a design or manufacturing error could indeed affect to all of them. The consideration of coupling mechanisms, such as, accomplishing the same function, operating under similar conditions, undergoing the same testing procedure or being in the same location, play an important role on establishing the group of components that are more or less susceptible to a CCF and require or not further analysis. In addition, it is considered that CCFs of active equipment would be predominant over CCFs of passive systems. The latter are therefore analysed in less detail in general.

The causes of CCFs can be originated in the preoperational phase of the plant. This includes a series of cause in the design specification, manufacturing, construction, installation and commissioning. They can also be related to the plant operation, e.g. how components are maintained or calibrated, or to environmental causes, e.g. corrosion, effect of heat, steam or water impingement.

In the context of this publication, associated to the application of SSR-2/1 [1], root causes as well as coupling mechanisms and defensive measures related to the plant design are the focus of importance. Therefore, for CCFs rooted in the preoperational phase of the plant the applicable defensive mechanisms can be:

Diversity

Two principal kinds of diversity are normally defined: (1) Functional diversity or use of components based on different operating principles or variables measured and (2) Technical diversity or use of components of different manufacturing or physical characteristics. Diverse

[25] US Nuclear Regulatory Commission, *A Cause-Defense Approach to the Understanding and Analysis of Common-cause Failures,* NUREG/CR-5460, SAND89-2368, March 1990.

equipment provides also redundancy, i.e. they fulfil the single failure criterion. Diversity is a specific measure aimed at preventing CCFs and other dependent failures although not efficient for every specific cause.

Regulations in some countries include requirements for diversity. Functional diversity is for instance required in the generation of signals of the reactor protection system (RPS). Functional diversity is stronger than technical diversity although not always feasible. In addition technical diversity goes against the goal of design standardization and entails additional maintenance and testing practices. Functional diversity implies in practice technical diversity.

Proven design and construction

The use of proven engineering practice is a pillar of the first level of defence in depth and equally applicable to systems involved in other levels.

Physical separation

Physical separation of redundant trains and components is efficient against CCFs and other dependent failures originated by harsh environmental conditions and the effects of several hazards, as well as the direct impact of mechanical or electrical failures of one train on the redundant train.

Earthquakes, fires and floods among other hazards have the potential to fail or degrade the condition of many plant SSCs at once. Moreover some of these hazards can induce other hazards as it happened in the Fukushima accident. Physical separation, adequate plant layout and design robustness are at the core of the defensive measures to reduce the impact of natural hazards, in addition to adequate safety margins and protective measures as well as good operational practices

Of particular importance is the adequate separation of cable routings of different electrical and instrumentation divisions. A full physical separation of trains might not be feasible in all plant areas. Physical separation can be accomplished either by full separations of trains through qualified barriers, the installation of protections on one train's relevant equipment and the separation by sufficient distance. The first option gives in general the highest protection

Self-testing equipment and self-announcement of failures

By an immediate detection and indication of a failed condition in stand by components, it is possible to undertake fast corrective actions for increasing the availability of the component and the systems. This applies also to the early detection of CCFs. This principle is applied extensively in the RPS design.

Regular maintenance and inspection and testing

Adequate testing and inspection programmes reduce the probability of failures, allow an the early detection of inspection failures and if a proper analysis of failures or findings in component conditions is carried out, including subsequent testing or inspections of redundant components if deemed necessary, it contributes to the early detection of CCFs. In addition the implementation of a staggered testing or maintenance policy versus a sequential one reduces the likelihood of human related CCFs.

Redundancy

Redundancy can also be efficient against several root causes of CCFs, since they don't normally lead to simultaneous failures, particularly if the components don't have the same operation regime, e.g. it usual to have one pump running and one pump in standby in cooling systems during plant operation. Hence, the occurrence of a CCF in one component can be still be compensated by the functioning of the redundant components. If adequate instrumentation to detect failures is available and an analysis of the causes of failures is performed, degradations in the redundant component can be identified before an actual CCF occurs in it.

Diversity, in particular functional diversity is of value against errors during design, manufacturing and construction. Technical diversity is less efficient as it may not prevent potential error in the formulation of the component design basis and specifications.

Proven design and construction as well as adequate quality control processes, including design review, inspection and testing from manufacturing to commissioning are another two important defensive mechanisms to prevent CCFs originated in the pre-operational phase of the plant.

With regard to environmental related causes of CCFs, such factors can be originated within the system, e.g. due to the physicochemical properties of the system fluids or to external environmental effects. Environmental effects could be fast or slow acting. For slow acting effects, appropriate policy and practice for surveillance and maintenance may be efficient. For fast developing environmental effects physical separation is the most efficient defensive mechanism.

Equipment diversity may also help is as much as diverse equipment may be differently susceptible to slow acting internal or external environmental common cause stressors.

APPENDIX 4
ACCIDENT CONDITIONS TO BE CONSIDERED FOR 'PRACTICAL ELIMINATION'

1. FAILURE OF A LARGE COMPONENT IN THE REACTOR COOLANT SYSTEM

A sudden mechanical failure of a single large component in the reactor coolant system (RCS) could initiate an event where reactor cooling would be lost in a short time and a pressure wave or a missile would damage the containment boundary. The defence in depth provisions would not be effective in such situation and an early large radioactive release would follow. This is a very exceptional type of initiating event for which safety systems and safety features are not designed for their mitigation and therefore it needs to be demonstrated that their likelihood would be certainly so low that they can be excluded, i.e. 'practically eliminated', from consideration. This is essential at least for the reactor vessel, which break would eliminate the capability of holding and cooling the core but also the likelihood of pressurizer and steam generator (SG) shell failure need to be shown to be extremely low, or alternatively it needs to be demonstrated that a failure of pressurizer or SG would not lead to unacceptable consequences to the containment.

The safety demonstration needs to be especially robust and the corresponding assessment suitably demanding, in order that an engineering judgement can be made for the following key requirements:

- The most suitable composition of materials needs to be selected;
- The metal component or structure needs to be as defect-free as possible;
- The metal component or structure needs to be tolerant of defects;
- The mechanisms of growth of defects are known;
- Design provisions and suitable operation practice are in place to minimize thermal fatigue, stress corrosion, embrittlement, pressurized thermal shock, over-pressurization of the primary circuit, etc.;
- An effective in service inspection and surveillance programme is in place during the manufacturing and the operation of the equipment to detect any defect or degradation mechanisms and to ensure that the equipment properties are preserved over the lifetime of the plant.

In addition, evidence needs to be provided to demonstrate that the necessary level of integrity will be maintained for the most demanding situations.

Several sets of well established technical standards, for instance the ASME Boiler and Pressure Vessel Code and equivalent codes used in other countries, are today available for ensuring reliability of large pressure vessels, and the demonstration of 'practical elimination' of vessel failures can be based on rigorous application of those standards. The technical standards also provide instructions for verification of the state of pressure vessels during the plant lifetime.

The practical elimination of failures of large components is thus achieved by the essential means of the defence in depth level 1 without relying on the subsequent levels of defence in depth.

The demonstration of low failure likelihood with a high confidence level could be supplemented by a probabilistic fracture mechanics assessment, which is today a widely recognized and commonly used technique. Probabilistic assessment in the demonstration of practical elimination, and specially in this case, is not restricted to the use of Boolean reliability models, e.g. fault trees or event trees, or failure rates derived from the statistical analysis of observed catastrophic failures. Probabilistic fracture mechanics includes assessments of material fracture toughness, weld residual stress, etc. which in turn considers deterministic analysis, engineering judgement and the measurements of monitored values as well.

2. UNCONTROLLED REACTIVITY ACCIDENTS

Reactivity accidents can be very energetic and have a potential to destroy the fuel and other barriers. The prevention of such accidents needs to be ensured at the defence in depth level 1 by proper reactor design. The main protection is provided by negative reactivity coefficient with all possible combinations of the reactor power and coolant pressure and temperature, thus suppressing reactor power increase during any disturbances and eliminating the reactivity hazards with help of laws of nature (demonstration of practical elimination by impossibility of the conditions).

An uncontrolled reactivity excursion could potentially be caused by sudden insertion of a cold or un-borated water plug into a reactor core. Nevertheless, all potential risks of sudden changes in the coolant properties must be identified and prevented by design provisions.

The demonstration of practical elimination relies primarily on impossibility of reactivity excursions through a core design with overall negative reactivity coefficients supported by other design measures to avoid insertions of reactivity, e.g. injection of water with low boron concentration in the core that can be evaluated deterministically and probabilistically as appropriate.

More complex situations could arise however if criticality can be reached during severe accidents. This has been a topic of concern in specific core melt-down scenarios in reactors where the control rod material has a lower melting point and eutectic formation temperature than the fuel rods. A potential hazardous scenario might occur if reactor vessel would be re-flooded with un-borated water in a situation when control rods have relocated downwards but the fuel rods are still in their original position. This is again an aspect to be analysed considering the design provisions and severe accident management features together, to reach a plausible conclusion that the condition has been practically eliminated.

3. DIRECT CONTAINMENT HEATING

Core meltdown in high pressure could cause a violent discharge of molten corium material into the containment atmosphere and this would result in direct containment heating by chemical reaction. High pressure core melt situations must therefore be eliminated by design provisions to depressurize the RCS when a meltdown is found unavoidable.

Any high pressure core meltdown scenario would evidently be initiated by a small coolant leak or boiling of the coolant and release of steam through a safety or relief valve. In such

situations it must be a design objective to convert the high pressure core melt to a low pressure core melt sequence with a high reliability so that high pressure core melt situations can be practically eliminated. The depressurization must be such that very low pressure can be achieved before a discharge of molten core from the reactor vessel can take place. On the other hand, dynamic loads from depressurization must not cause a threat to the essential containment structures.

Dedicated depressurization systems have been installed in existing plants and designed for new plants. At PWR plants they are based on simple and robust devices and straightforward operator actions that eliminate the risk of erroneous automatic depressurization but provide adequate time to act when need arises. At BWR plants the existing steam relief systems generally provide means for depressurization, with possibly some modifications in valve controls to ensure reliable valve opening and open valve position also in very low pressures.

A deterministic analysis is necessary to demonstrate the effectiveness of the depressurization system in preventing direct containment heating. Traditional PSA techniques are adequate to demonstrate a high reliability of the depressurization systems including the operator initiation. In this way, the practical elimination of direct containment heating could be demonstrated based on a combined deterministic and probabilistic assessment of specific design provisions.

4. LARGE STEAM EXPLOSION

The interaction of the reactor core melt with water, known as fuel-coolant interaction (FCI), is a complex technical issue involving a number of thermal-hydraulic and chemical phenomena. FCI may occur in-vessel, during flooding of a degraded core or when a molten core relocates into the lower head filled with water. They may also occur ex-vessel, when molten core debris is ejected into a flooded reactor cavity after the vessel failure. Each of the scenarios may lead to an energetic FCI, commonly known as ‘steam explosion’, which represents potentially serious challenge to the reactor vessel and/or containment integrity.

The conditions of steam explosion triggering and the energy of explosion in various situations have been widely studied in reactor safety research programs. Although non-triggered steam explosion seem to be very unlikely, the risks of steam explosion cannot be fully eliminated in all core meltdown scenarios where molten corium may be dropped to water.

For eliminating steam explosions that could damage the containment barrier, the preferred method is to avoid dropping of molten core to water in any conceivable accident scenarios. Such approach is used in some PWR type reactors: existing small reactors where reliability of external cooling of the molten core has been proven and in some new reactors with a separate core catcher. In some existing and in some new designed BWR type reactors the molten core would in all severe accident scenarios drop to a pool below the reactor vessel and be solidified and cooled in the pool. In any such circumstances where corium drops to water, it must be proven with arguments based on the physical phenomena involved in the respective scenarios that risks from steam explosion to the containment integrity have been practically eliminated. The role of PSA in this demonstration, if there is one at all, is very limited.

5. HYDROGEN DETONATION

Hydrogen combustion is very energetic phenomenon, and a fast combustion reaction (detonation) involving sufficient amount of hydrogen would cause a significant threat to the containment integrity. Dedicated means to eliminate hydrogen detonation are needed at all

nuclear power plants (NPPs), although different means are preferred for different plant designs.

In BWR containments that are all relatively small, the main protective mean is filling of the containment with inert nitrogen gas during power operation. In large PWR containments the current practice is to use passive catalytic recombiners or other devices that control the rate of the oxygen and hydrogen recombination.

It is also necessary to ensure and confirm with analysis and tests that circulation of gases and steam inside the containment provides proper conditions for hydrogen recombination and eliminate too high local hydrogen concentrations. Furthermore, the risk of hydrogen detonation increases if steam providing inertization is condensed.

An uncertainty that needs additional attention and further research relates to the highest conceivable rate and the total amount of hydrogen generation inside the containment. Some of the current core catchers can significantly reduce or even eliminate the ex-vessel hydrogen generation in the accident phase when the corium has dropped to the catcher, and this could bring major reduction also to the total amount of hydrogen generated inside the containment.

The design provisions for preventing hydrogen detonation need to be assessed in other to demonstrate the practical elimination of this phenomenon. This assessment also includes the consideration of hydrogen propagation and mixing inside the containment. This is of particular importance in case of MCCI when the amount of hydrogen exceeds the capacity of recombination due to lack of oxygen in the containment.

6. LOSS OF CONTAINMENT HEAT REMOVAL

In a situation where core decay heat cannot be removed by heat transfer systems to outside of the containment and further to the ultimate heat sink, or in severe accident where the core is molten and is generating steam inside the containment, cooling of the containment atmosphere is a preferred mean for preventing its overpressure.

Several examples are found today from both existing plants and from new plant designs of robust dedicated containment cooling systems that are independent of other safety systems and are considered to practically eliminate the risk of containment rupture by overpressure.

An alternative to cooling is to eliminate the containment overpressure by venting. This is necessary especially in BWR type reactors where the size of the containment is small and pressure limitation may be needed both in the DBA as well as in accidents with core melt. The existing venting systems prevent overpressurization at the cost of some radioactive release involved in the venting, also in the event that the venting is filtered.

Containment venting avoids some peaks of pressure threatening the containment integrity, but the stabilization of the core and the cooling of the containment are still necessary in the longer term.

The safety demonstration needs to be based on the capability and reliability of the specific measures implemented in the design to cope with the severe accident phenomena. A PSA level 2 analysis can be used to demonstrate the very low probability (practical elimination) of large releases.

7. MOLTEN CORE CONCRETE INTERACTION

In the event of a severe accident in which the core has melted through the reactor vessel, it is possible that containment integrity could be breached if the molten core is not sufficiently cooled. In addition, interactions between the core debris and concrete can generate large quantities of additional hydrogen and other non-condensable gases, which could contribute to eventual overpressure failure of the containment.

Alternative means have been developed and verified in extensive severe reactor accident research programs conducted nationally and in international co-operation.

The means suggested today include

- Keeping of the molten core inside the reactor vessel by cooling the vessel from outside;
- Installing a dedicated system or device that would catch the molten corium as soon as it has penetrated the reactor vessel wall.

In all of these approaches cooling of the corium generates steam inside the containment and it is necessary to provide a separate dedicated system for heat removal from the containment, as discussed below.

While PSA can play a role on assessing the reliability of establishing external reactor vessel cooling or the core catcher cooling (if provided), the demonstration of the practical elimination of containment boundary melt through relies extensively on deterministic analysis of the design provisions.

8. SEVERE ACCIDENTS WITH CONTAINMENT BYPASS

Containment bypass can occur in different ways, such through circuits connected to the RCS that exit the containment or defective SGs tubes (for PWRs). Accident sequences with non-isolated penetrations connecting the containment atmosphere to the outside as well as accident sequences during plant shutdown with containment open also need to be considered as containment bypass scenarios. All these conditions have to be ‘practically eliminated’ by design provisions such as adequate piping design pressure and isolation mechanisms.

It has to be taken into account that failures of lines exiting the containment and connected to the primary system, including SG ruptures are at the same time accident initiators, whereas other open penetrations just constitute a release path in accident conditions.

The safety demonstration for elimination of bypass sequences needs to include a systematic review of all potential containment bypass sequences and cover all containment penetrations.

Requirement 56 in SSR-2/1 [1] establishes the minimum isolation requirements for various kinds of containment penetrations. The requirement addresses aspects of leak-tightness and leak detection, redundancy and automatic actuations as appropriate. Specific provisions are given also for interfacing failures in the RCS. National regulations address in more detail what are the applicable provisions for containment isolations and prevention of containment bypass or interfacing LOCAs.

Based on the implementation of the design requirements or specific country regulations and the in-service inspection and surveillance practices, the analysis has to assess the frequency of bypassing mechanisms. This analysis, although of probabilistic nature, it needs to combine

aspects of engineering judgement and deterministic analysis in the probabilistic calculations, and always be based upon the redundancy and robustness of the design, the application of relevant design rules, e.g. fail safe actuation, as well as the pertinent inspection provisions and operational practices, similar to the previous cases. While the analysis of isolation of containment penetrations or SGs is amenable to conventional fault tree and event tree analyses with due consideration of failures in power supplies, isolation signals and human actions, other analysis aspects may require the use of other probabilistic methods together with deterministic methods and engineering judgement to demonstrate the practical elimination of containment bypass.

This would lead on one hand to a defensible low frequency estimate of the bypass mechanisms associated to each penetration based. On the other hand, the reliability of design provisions for the isolation of bypass paths based upon conventional probabilistic analysis would complement the demonstration that the containment pass has been practically eliminated.

9. SIGNIFICANT FUEL DEGRADATION IN STORAGE POOL

Facilities for spent fuel storage shall be designed to ensure that the potential for high radiation doses or radioactive releases to the environment are practically eliminated. To this aim, it is necessary to ensure that spent fuel stored in a pool is always kept covered by an adequate layer of water. This requires inter alia

- A pool structure that is designed against all conceivable internal and external hazards that could damage its integrity;
- Avoiding siphoning of water out of the pool;
- Providing redundant lines for pool cooling that eliminate possibility of long lasting loss of cooling function, i.e. for time needed to boil off the water;
- Reliable instrumentation for pool level monitoring;
- Appropriate reliable means to compensate for any losses of water inventory.

Risks for mechanical fuel failures need to be eliminated by

- Design that ensures avoiding heavy lifts moving above the spent fuel stored in the pool;
- Structures that eliminate the possibility of heavy lifts dropping on the top of the fuel.

In designs where the spent fuel pool (SFP) is outside the containment, the uncovering of the fuel would lead to fuel damage and a large release could not be prevented. Means to evacuate the hydrogen would prevent explosions that could cause further destruction to the pool and prevent a later reflooding and cooling of the fuel.

In some designs, the SFP is located inside the containment. In this case, even though the spent fuel damage would not lead directly to a large release, the amount of hydrogen generated by a large number of fuel elements, the easy penetration of the pool liner by the corium without a fuel catcher, among other harsh effects would eventually lead to a large release. Therefore, it is also necessary to ensure by design provisions that also in this case that the uncovering of spent fuel elements has been ‘practically eliminated’.

APPENDIX 5
CHAIN TO TRANSFER HEAT FROM ITEMS IMPORTANT TO SAFETY TO THE ULTIMATE HEAT SINK

For the removal of heat from items important to safety a common denomination is essential service water system (ESWS) for an open cooling circuit transferring the heat to the ultimate heat sink and component cooling water system (CCWS) for an intermediate closed loop system, which transfers heat from the majority of the items important to safety to the ESWS in order to reduce the probability of radiological releases to the environment. Some designs, however, don't avail of the CCWS as intermediate closed loop. This is for instance the case of many operating BWRs. Some plant designs have different heat transfer systems for items important to safety than for the rest. If this is not the case, Requirement 70 of SSR-2/1 [1] also requires that the isolation of the cooling circuits serving items that are not essential for safety has to be ensured.

Components typically cooled by the CCWS in existing PWRs are: the RHR heat exchangers, the spent fuel pool (SFP) water cooling system, containment systems (e.g. fan-coolers), electrical pump motors of safety systems, heating ventilation and air conditioning (HVAC) systems of safety important areas, as well as the thermal barriers of the main coolant pump (MCP) seals and the non-regenerative heat exchanger of the let-down line of the chemical and volume control system (CVCS) of the reactor coolant system (RCS). The ESWS in typical PWRs cools the heat exchangers of the CCWS and some additional components such as the diesel generators.

It is common in BWR designs, that cooling functions of items important to safety are accomplished directly by the ESWS without an intermediate cooling circuit in many instances. It has to be remarked however, that these are common examples in existing designs but that many plants can deviate in several aspects from the examples. The very often discussed use of air cooled diesel generators in some units of the Fukushima Daiichi plant is just one case. CCWS and ESWS are system denominations used in the following for systems accomplishing the functions just described, although other names are used for similar systems in specific reactor designs.

At power operation the main heat sink is the condenser, and in shutdown conditions, if the condenser is not available, the heat can also be transferred to the atmosphere through steam relief or safety valves in the PWRs, but even in those situations the CCWS and the ESWS continue to be the mechanism to remove heat from SSCs important to safety.

The loss of CCWS or ESWS seems to be a more credible mechanism for the failure of heat transfer in shutdown conditions to the ultimate heat sink, rather than the loss of ultimate heat sink itself. Some components and structures of the ESWS are particularly exposed to the impact of external hazards (e.g. flooding, clogging by debris or algae) as it was confirmed in the Fukushima accident. The reinforced safety requirements for the heat transfer to the ultimate heat sink call for the provision of an alternative ultimate heat sink or a different access to it[26]. This means to ensure appropriate margins in the design of CCWS and ESWS, and in particular for the parts of the ESWS interfacing with the ultimate heat sink, to ensure

[26] SSR-2/1 [1] paragraph 6.19A: Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink. Paragraph 6.19B: The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.

that external hazards that affect the plant through the ultimate heat sink, e.g. external flooding, cannot render the ESWS unavailable.

Where tsunamis are a hazard to be considered, a temporary withdraw of sea waters before the arrival of tsunami waves is also a phenomenon to be considered in the design of the water intake for the ESWS. A possible long lasting drought (and consequential loss of the ultimate heat sink) could be caused by dam failure downstream. In addition, pipe failures of a system like the ESWS in case of an earthquake, bear the potential for internal flooding of important plant areas. Other external hazards potentially affecting the ultimate heat sink are tornados, liquefaction of the soil and sandstorms.

When is not practical to reinforce this part of the ESWS, the alternative solution considered in SSR-2/1 [1] would mean an additional branch of the ESWS that would allow a different and protected access to the ultimate heat sink or the connection of the ESWS to a different ultimate heat sink. In most cases, the alternate ultimate heat sink would be a closed water repository and water-air cooling devices of sufficient cooling capacity and designed with appropriate seismic margins.

Design and layout of the alternate ultimate heat sink are required to be such that the same natural hazard could not compromise the two ultimate heat sinks simultaneously. The installation of an alternative ultimate heat sink access or an alternative ultimate heat sink entails design provisions in the ESWS to operate safely using different access points or ultimate heat sinks. It could be possible to limit the capacity of the alternative ultimate heat sink to the functional demands of the PIEs that could be caused by the external hazards.

From the typical list of equipment serviced by CCWS or ESWS, it is evident that the loss of one of these systems would very likely lead to a PIE and render inoperable SSCs that would be necessary to respond to the initiating event at levels 2 and eventually 3 of defence in depth. Thus for instance the failure of CCWS, forces a reactor shutdown as result of the failure of the CVCS (malfunction of the non-recuperative heat exchanger in the discharge line) and loss of cooling of the MCP thermal barriers.

In spite of the resistance of the MCP seal and the long thermal inertia in plant SSCSs, the loss of HVAC for rooms and sensitive I&C or electrical equipment together with the loss of spent fuel cooling and the unavailability of emergency core cooling system equipment could eventually result in DECs. The failure of the ESWS could result in similar consequences. Therefore, such common designs of ESWS and CCWS in nuclear power plant (NPP) in operation result in a strong functional dependence between systems required at various levels of defence in depth. For the newest (third) generations of LWRs, it can be expected that the functional dependences introduced by heat transfer systems to the ultimate heat sink will not be so strong. However, the failures of CCWS or ESWS (or systems fulfilling the same functions) are flagged out for their failures to be taken into account as DEC scenarios considered in the design.

ABBREVIATIONS

AOO	anticipated operational occurrence
ASME	American Society of Mechanical Engineers
ATWS	anticipated transient without scram
BDBEE	beyond design basis external event
BWR	boiling water reactor
CVCS	chemical and volume control system
CCWS	components cooling water system
CCF	common cause failure
CDF	core damage frequency
CLI	criteria for limited impact
DC	direct current
DAS	diverse actuation system
DBA	design basis accident
DEC	design extension condition
DNBR	departure from nucleate boiling ratio
EAL	emergency action level
EC	emergency centre
ESWS	essential service water system
EUR	European utility requirements
FCI	fuel-coolant interaction
HDL	hardware description language
HVAC	heating ventilation and air conditioning
I&C	instrumentation and control
LOCA	loss of coolant accident
LOOP	loss of off-site power
LWR	light water reactor

MCCI	molten core concrete interaction
MCP	main coolant pump
MSGTR	multiple steam generator tube ruptures
MSLB	main steam line break
NO	normal operation
OSC	operation support centre
NPP	nuclear power plant
PIE	postulated initiating event
PSA	probabilistic safety assessment
PWR	pressurized water reactor
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RHR	residual heat removal system
RPS	reactor protection system
RWST	refuelling water storage tank
SBO	station blackout
SFP	spent fuel pool
SG	steam generator
SSC	structure, system and component
TSC	technical support centre

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of NUCLEAR POWER PLANTS: Design, IAEA Safety Standards Series No.SSR-2/1, IAEA, Vienna (2016).

[2] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

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

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, IAEA, Vienna (2007).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, INSAG Series No. INSAG-10, IAEA. Vienna (1996).

[6] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.10, IAEA, Vienna (2004).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Margins of Operating Reactors — Analysis of Uncertainties and Implications for Decision Making, IAEA TECDOC-1332, IAEA, Vienna (2003).

[9] NUCLEAR ENERGY AGENCY, Safety Margin Evaluation-SMAP Framework Assessment and Application, NEA/CSNI/R (2011)3, 30 Nov. 2011.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3, IAEA, Vienna (2016).

[11] EUROPEAN UTILITY REQUIREMENTS FOR LWR NUCLEAR POWER PLANTS, Revision D, October 2012. Retrieved from http://www.europeanutilityrequirements.org/Documentation/EURdocument/RevisionD/Volume2.aspx

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34 (2016).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39 (in preparation).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).

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

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

CONTRIBUTORS TO DRAFTING AND REVIEW

Amri, A.	International Atomic Energy Agency
Boyce, T.	US Nuclear Regulatory Commission, USA
Burger D.J.	Ontario Power Generation, Canada
Courtin, E.J.F	Areva NP, France
Gasparini, M.	Consultant, Italy
Geupel, S.	Gesellschaft für Anlagen und Reaktorsicherheit, Germany
Gilbert, L.	Bruce Power, Canada
Gürpinar, A.	Consultant, Turkey
Laaksonen, J.	Rosatom Overseas, Russian Federation
Misak, J.	Nuclear Research Institute Rez, Czech Republic
Nakajima, T.	Nuclear Regulation Authority, Japan
Nuenighoff, K.U.	Gesellschaft für Anlagen und Reaktorsicherheit, Germany
Poulat, B.	International Atomic Energy Agency
Webster, P.	Permanent Mission of Canada to the IAEA, Canada
Yllera, J.	International Atomic Energy Agency

Comments have been provided by: CNSC (Canada), ENISS, IRSN (France), BMUB, GRS (Germany), NRA, JANSI (Japan), KINS (Rep. of Korea), USNRC (USA).

Consultants meetings

Vienna, Austria, 10–14 March 2014, 30 June–2 July 2014, 14–16 April 2015

Working Group Meeting of NUSSC Members

Vienna, Austria, 3 July 2015

IAEA
International Atomic Energy Agency

No. 24

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

BELGIUM
Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC
Suweco CZ, s.r.o.
SESTUPNÁ 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FRANCE
Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 43 43 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY
Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY
Librotrade Ltd., Book Import
Pesti ut 237. 1173 Budapest, HUNGARY
Telephone: +36 1 254-0-269 • Fax: +36 1 254-0-274
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

INDIA
Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://www.bookwellindia.com

ITALY
Libreria Scientifica "AEIOU"
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: http://www.libreriaaeiou.eu

JAPAN
Maruzen-Yushodo Co., Ltd.
10-10, Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: http://maruzen.co.jp

RUSSIAN FEDERATION
Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: http://www.secnrs.ru

UNITED STATES OF AMERICA
Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders for both priced and unpriced publications may be addressed directly to:

IAEA Publishing Section, Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

International Atomic Energy Agency
Vienna
ISBN 978–92–0–104116–6
ISSN 1011–4289