18 September 2020

IAEA SAFETY STANDARDS

for protecting people and the environment

Step 7: First review of the draft safety standard by the RC(s)

New title agreed by the NUSSC Working Group

Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants

DS508

DRAFT SAFETY GUIDE

New Safety Guide

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1 Over the latest decades, IAEA safety standards for nuclear power plant design have been enhanced several times with the aim of providing confidence that the successive generations of nuclear power plants are designed so as to operate efficiently at the highest levels of safety that can be reasonably achieved considering the state of the art practices and techniques in science and technology and taking into account the feedback gained from the nuclear events and operational experience.

1.2 IAEA Safety Standards Series No. SSR-2/1, Safety of Nuclear Power Plants: Design in 2012[1] and its subsequent revision in 2016, SSR-2/1 (Rev. 1) [1] introduced changes to the requirements for the design of nuclear power plants. These changes include measures for strengthening the implementation of the concept of defence in depth by means of the following:

a) Including design extension conditions (DEC);
b) Practically eliminating plant event sequences that could result in early radioactive releases or large radioactive releases;
c) Including design features for enabling the use of non-permanent equipment for power supply and cooling.

The incorporation of these aspects in the new NPP designs requires specific guidance for the design and the necessary safety assessment. Although specific guidance is provided in safety guides for the design of safety features related to these aspects, overarching guidance on their application to the plant design is necessary in a single safety guide.

1.3 IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment of Facilities and Activities, also revised after the Fukushima Dai-ichi accident [2], establishes requirements for safety assessment covering the whole lifetime of all types of facility and activity. Requirements for safety assessment of the design in this publication are not sufficiently detailed for nuclear power plants. However, specific requirements for safety assessment and safety analysis of nuclear power plants are established in SSR-2/1 (Rev. 1) [1], and these need to be considered to address specific aspects of relevance for nuclear power plant design.

OBJECTIVE

1.4 The objective of this Safety Guide is to provide recommendations on the implementation of the requirements in SSR-2/1 (Rev. 1) [1] that are related to defence in depth and practical elimination of event sequences leading to early radioactive releases or large radioactive releases. The recommendations in relation to defence in depth in this Safety Guide are focused on design aspects, in particular on those aspects associated with DEC. This Safety Guide is also aimed at addressing at a high level the safety assessment related to these design aspects.

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

1.5 This Safety Guide is intended for use by organizations involved in the verification, review and assessment of safety of nuclear power plants. It is also intended to be of use to organizations involved in the design, manufacture, construction, modification, and operation, and in the provision of technical support for nuclear power plants, as well as by regulatory bodies.

SCOPE

1.6 The scope of this Safety Guide is focused on the implementation and assessment of the design safety measures described in para. 1.2. These measures play an important role in the implementation of the concept of defence in depth, which constitutes the primary means of preventing accidents and mitigating their consequences should they occur, in accordance with Principle 8 of IAEA Safety Standards Series No. SF-1 Fundamental Safety Principles [3]. As described in para. 2.13 of SSR-2/1(Rev.1) [1], the implementation of defence in depth at nuclear power plants comprises 5 levels. Safety features for DEC as well other safety features that underpin the demonstration of practical elimination of event sequences that can lead to early radioactive releases or large radioactive releases correspond to one or more levels of defence in depth. Therefore, this Safety Guide addresses the implementation or assessment of defence in depth in relation to these aspects.

1.7 A key issue is the independence between levels of defence in depth and in particular in relation to safety features for DEC (especially features for mitigating the consequences of accidents involving the melting of fuel). There are several factors that can be the cause of dependencies between plant structures, systems and components (SSCs) and that are addressed by different means. This Safety Guide considers, in a general manner, the assessment of functional independence of SSCs. Aspects such as environmental factors, operational or human factors, and external or internal hazards, are recognized as relevant, but are not addressed in this Safety Guide.

1.8 This Safety Guide also addresses the reinforcement of safety by including design features for enabling the use of non-permanent equipment for power supply and for cooling, as a result of the lessons learned from the Fukushima Daiichi accident. These features are primarily intended for preventing unacceptable radioactive releases in the event of levels of natural external hazards exceeding the magnitude considered for the design, derived from the hazard evaluation for the site.

1.9 The guide is not intended to provide specific recommendations for the design of safety features for DEC or for any other plant state considered in the design. These are provided in the safety guides for the design of various types of plant system, for instance in IAEA Safety Standards Series Nos SSG-56, Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants [4], SSG-53, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants [5], SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [6], and SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [7].

1.10 This Safety Guide does not consider the specific safety analyses to be carried out for different plant states, as this is addressed in IAEA Safety Standards Series Nos SSG-2 (Rev. 1),

Deterministic Safety Analysis for Nuclear Power Plants [8], SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [9], and SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants [10], as appropriate.

1.11 The recommendations given in this Safety Guide are primarily intended for application to water cooled nuclear power plants designed in accordance with the requirements provided in SSR-2/1 (Rev. 1) [1]. It is recognized that for reactors cooled by other media or based on innovative design concepts, some of the recommendations in this Safety Guide might not be fully applicable, and judgment in their application might be needed.

1.12 For water cooled nuclear power plants in operation designed in accordance with earlier standards, this guide may be also useful when evaluating potential safety enhancements of such designs (for example as part of the periodic safety reassessment of the plant).

STRUCTURE

1.13 This safety guide comprises five sections and two annexes. Section 2 sets the framework for the guidance that is provided in the following sections by describing the requirements in SSR-2/1 (Rev. 1) [1] and GSR Part 4 (Rev. 1) [2] on which guidance is based. It also introduces some relevant concepts and explanations on the topics covered by this Safety Guide. Section 3 provides recommendations on the implementation and assessment of DEC including the aspect of independence between safety provisions at the corresponding levels of defence in depth. Section 4 provides recommendations on the application of the concept of practical elimination of event sequences that could lead to early radioactive releases or large radioactive releases. Section 5 provides recommendations on strategies for the implementation of design provisions for enabling the use of non-permanent equipment for power supply and cooling.

1.14 Annex I provides information on the demonstration of a commonly recognized set of events or plant conditions that need to be demonstrated to have been practically eliminated. Annex II provides some considerations for the application of this Safety Guide to nuclear power plants designed to earlier standards.

2. DESIGN APPROACH TO PREVENT ACCIDENTS WITH HARMFUL CONSEQUENCES

2.1 Principle 8 on prevention and mitigation of accidents in SF-1 [3] states that “All practical efforts must be made to prevent and mitigate nuclear or radiation accidents” and furthermore that “The primary means of preventing and mitigating the consequences of accidents is ‘defence in depth’”.

2.2 The implementation of defence in depth, as described in SF-1 [3], comprises safety measures of various types. This Safety Guide is primarily focused on design measures for nuclear power plants as described in [1] and more specifically on design measures for the mitigation of accidents, including those implemented to facilitate accident management.

2.3 Requirement 5 of SSR-2/1 (Rev. 1) [1] states:

> "**The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable in, and following, accident conditions.**"

2.4 Paragraph 4.3 of SSR-2/1 (Rev. 1) [1] states:

> "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', and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence."

2.5 Furthermore, para. 4.4 of SSR-2/1 (Rev. 1) [1] states:

> "Acceptable limits for purposes of radiation protection associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements."

2.6 The requirements in paras 2.3–2.5 establish the safety approach for the design and specifically establish the need for radiological consequences of accident conditions to be not only below acceptable limits but to be as low as reasonably achievable (ALARA). In addition, it needs to be demonstrated in the design that plant states that could lead to high radiation doses or to a large radioactive release have been 'practically eliminated'. Further requirements in relation to acceptable limits for categories of plant states and more specifically for accident conditions are also specified SSR-2/1 (Rev. 1) [1], namely:

— "Criteria shall be assigned to each plant state, such that frequently occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence" (para. 5.2 of SSR-2/1 (Rev. 1) [1]).
— "A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions" (para. 5.25 of SSR-2/1 (Rev. 1) [1] in relation to design basis accidents).
— "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'" (para. 5.31 of SSR-2/1 (Rev. 1) [1] in relation to DEC).
— "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" (para. 5.31A of SSR-2/1 (Rev. 1) [1] in relation to DEC).

2.7 This Safety Guide is focused on the protection of the public and the environment in accident conditions, which should be assessed by verifying compliance with a number of requirements in SSR-2/1 (Rev. 1) [1] pertaining to the general plant design, as those indicated

above, as well as other requirements for plant specific systems, for instance those related to the containment structure and its systems. As indicated in par 2.11 of SSR 2/1, Rev.1 [1], "Measures are required to be taken to ensure that the radiological consequences of an accident would be mitigated. Such measures include the provision of safety features and safety systems, the establishment of accident management procedures by the operating organization and, possibly, the establishment of off-site protective actions by the appropriate authorities, supported as necessary by the operating organization, to mitigate exposures if an accident occurs"[2].

2.8 In accordance with Requirement 5 of SSR-2/2 (Rev. 1) [1], radioactive releases in accident conditions are required to be below acceptable limits and be as low as reasonably achievable. In addition, the purpose of the fourth level of defence in depth is that off-site contamination is avoided or minimized. To this aim, a limit for the release of radioactive materials or on acceptable limit on effective dose should be specified for each category of accident conditions, and compliance with these limits should be verified. For accidents without significant fuel degradation, the releases are required to be minimized such that off-site protective measures (e.g. sheltering, evacuation) are not necessary. For accident with core melting, the releases are required to be such that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release are required to be 'practically eliminated'. The amount of radioactive releases considered acceptable for DEC with core melting should be significantly lower than the amount characterizing a large release. In addition, the design should be such that no cliff edge effect in the radiological consequences is expected for accidents slightly exceeding the plant design basis.

2.9 For normal operation or anticipated operational occurrences, there is limited uncertainty on plant state frequency and radiological impact, which can be monitored and is supported by many years of operating experience of previous plant designs. For less frequent plant states, i.e. accidents, there are larger uncertainties associated with the demonstration of plant state frequency and radiological consequences.

2.10 Harmful radiological consequences to the public can only arise from the occurrence of accidents. Therefore, the following chapters are devoted to the implementation and assessment of defence in depth and the complementary need for demonstration of practical elimination of accident sequences that can lead to early radioactive releases or large radioactive releases.

2.11 Recommendations on radiation protection in design of nuclear power plants are provided in IAEA Safety Standards Series No. NS-G-1.13, Radiation Protection Aspects of Design for Nuclear Power Plants [12], and recommendations for protection of the public are provided in

[2] The establishment of off-site protective arrangements belongs to the level 5 of in depth and is outside of the scope of this Safety Guide. Requirements regarding such arrangements are established in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [11].

IAEA Safety Standards Series No. GSG-8, Radiation Protection of the Public and the Environment [13].

3. IMPLEMENTATION AND ASSESSMENT OF DESIGN EXTENSION CONDITIONS WITHIN THE CONCEPT OF DEFENCE IN DEPTH

OVERALL IMPLEMENTATION OF DEFENCE IN DEPTH

3.1 This section addresses the overall application of Requirement 7 of SSR-2/1 (Rev. 1) [1] for defence in depth in the design of nuclear power plants, with specific emphasis on design provisions for accident conditions. It also addresses the overall assessment of the implementation of this concept, with specific focus on the reactor core as the main source of radioactivity. For other sources of radiation or potential releases of radioactive materials, the implementation of a defence in depth strategy will depend on the amount and isotopic composition of radionuclides, on the effectiveness and leak tightness of the individual confinement barriers as well as the potential challenges for the integrity of the barriers and the consequences of their failures.

3.2 The concept of defence in depth for the design nuclear power plants is described in para. 2.13 of SSR-2/1 (Rev. 1) [1]. An overall strategy of defence in depth, when properly implemented, achieves the objective that no single technical, human or organizational failure will lead to harm to the public, and that credible combinations of events and failures will lead to no or little harm to the public.

3.3 For the implementation of safety provisions at each level of defence in depth there are three aspects of importance, as follows:

(a) The performance of the safety provisions implemented to meet the acceptance criteria for the integrity of the barrier(s) that should be protected;
(b) The reliability of safety provisions to ensure that a certain plant condition can be brought under control without needing the intervention of the safety provisions implemented for next level, with a sufficient level of confidence;
(c) Adequate independence from the safety provisions implemented at the previous and successive levels of defence in depth.

3.4 An association of the levels of defence in depth with plant states considered in the design is frequently undertaken for design safety and operational safety. The introduction of DEC in the plant design basis has resulted in two different interpretations by States regarding the correspondence between plant states considered in the design and levels of defence in depth. These two approaches are represented in Table 1. Approach 1 (i.e. the association of DEC 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. Radiological acceptable limits for DEC without core melt are the same or similar as for DBA. Also, the physical phenomena in case of DBA and DEC without significant fuel degradation

core are similar, although there are differences in the analysis. In contrast, severe accidents are characterized by completely different physical phenomena. However, approach 2 (i.e. the grouping of DEC without core melt and with core melt in level 4) facilitates the differentiation between the set of rules for design and for safety assessment to be applied for DEC and the rules to be applied to DBA.

Table 1: Levels of Defence in Depth

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

3.5 Normal operation comprises a series of plant operating modes defined in the documentation governing the operation of the plant (such as the Operating Limiting Conditions or the plant Technical Specifications in some States) that range from power operation to reactor refuelling, in which no failures have taken place, and no equipment is unavailable that would prevent the intended accomplishment of the goals of the operational mode. Plant states other than normal operation are reached either directly by the occurrence of postulated initiating events for the applicable modes of operation or through failures in mitigating the consequences of such events in the first place. Their impact on the plant is the main basis for establishing the safety provisions that are necessary at each plant state. For these reasons, this Safety Guide addresses the design safety provisions necessary for each plant state, rather than for each level

of defence. In this way, the significance and importance of design extension conditions for the safety approach is emphasized.

3.6 Paragraph 4.13 of SSR-2/1 (Rev. 1) [1] states:

> "The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant."

Therefore, design provisions for operational states should have adequate capabilities to maintain the integrity of the first barrier for the confinement of radioactive materials (i.e. the fuel cladding) and to prevent a significant release of primary coolant and an evolution to design basis accident conditions, for which the actuation of the engineered safety features (safety systems) is foreseen.

3.7 Consistent with the highest frequency of postulated initiating events for design basis accidents (usually lower than 10^{-2} per reactor-year), the reliability of safety provisions for anticipated operational occurrences should be such that the frequency of transition into an accident condition is significantly lower than this value.

Design Basis Accidents

3.8 Requirement 19 of SSR-2/1 (Rev. 1) [1] states:

> "**A set of accidents that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.**"

3.9 Paragraph 5.24 of SSR-2/1 (Rev. 1) [1] states:

> "Design basis accidents shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control design basis accident conditions"

3.10 Paragraph 5.25 of SSR-2/1 (Rev. 1) [1] states:

> "A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions."

Consequently, specific design provisions (safety systems) should be implemented to mitigate the radiological consequences of DBAs through the prevention of significant fuel damage and damage to the containment boundary in order to limit the radiological consequences to the public and the environment to the extent that no special measures are required for the protection of the public.

3.11 Design basis accidents are postulated events that are not expected to occur during the lifetime of the plant. The most frequent events categorized as DBAs should have an expected frequency below 10^{-2} per reactor-year. The operation of safety systems designed to control DBAs should rely on automatic actuation and should not involve human intervention for a sufficiently long period of time and their reliability should be very high. Safety systems should be designed to ensure their reliable operation under postulated external hazards and prevailing environmental conditions. The reliability of safety systems should be such that (to the extent possible) the collective contribution to the core damage frequency of failing to mitigate DBAs does not exceed the safety goals of the plant (for new nuclear power plants typically below 10^{-5} per reactor-year). If this is not the case, DEC without significant fuel degradation could be postulated for specific low frequency sequences as appropriate to achieve such goals.

3.12 If the design of the containment is such that in the case of the most limiting DBAs the intervention of cooling or pressure reduction systems (e.g. containment spray) is necessary to ensure the integrity of the containment boundary, such systems should be designed, constructed and maintained to ensure a very high reliability, since their failure would not only lead to a severe accident but also jeopardize the subsequent measures for its mitigation. For the same reason, containment isolation provisions in case of DBAs should also be designed to have very high reliability for ensuring that acceptable limits for radiological consequences are not exceeded and sufficient coolant inventory can be maintained. Severe accidents with an open containment constitute one of the plant conditions to be practically eliminated that are addressed in Section 4.

Design extension conditions

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

> "**A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.**"

3.14 Paragraph 5.30 of SSR-2/1 (Rev. 1) [1] states:

> "In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected using engineering judgement and input from probabilistic safety assessments."

3.15 To meet the requirements described in paras 3.13 and 3.14, two separate categories of design extension conditions should be identified: design extension conditions without significant fuel degradation and design extension conditions with core melting.

Design extension conditions without significant fuel degradation

3.16 Design extension conditions without significant fuel degradation should be considered for unlikely yet credible single or multiple failures with the potential for exceeding the capabilities of safety systems designed for the mitigation of DBAs.

3.17 Design extension conditions without significant fuel damage are to a large extent technology and design dependent, but they can be classified in three types [8], as follows:

(a) An initiating event less frequent than those considered for DBAs and that exceeds the capabilities of safety systems for mitigation of DBAs;
(b) An anticipated operational occurrence or frequent design basis accident combined with the failure of a safety system designed for its mitigation, typically due to a common cause failure;
(c) A postulated initiating event associated with the failure of a safety system used for normal operation, e.g. a support system, and is required for the control of the initiating event.

3.18 In general, the mitigation of DEC without significant fuel degradation should be accomplished by specific safety features designed for such conditions. Alternatively, they can be mitigated by available safety systems that have not been affected by the events that led to the DEC under consideration.

3.19 Since the objective in DBA and in DEC without significant fuel degradation is the same, namely to prevent core damage or damage to the fuel in the irradiated fuel storage, the primary difference between these two accidental conditions is the use of different or criteria for design or safety assessment to achieve this objective. Thus, in design extension conditions the following apply:

(a) Less stringent design requirements than for DBA can be applied, for example compliance with the single failure criterion is not required, equipment can have a lower safety class and rigorous reliability measures are allowed;

(b) Less conservative assumptions and criteria, or best estimate methods, are acceptable for the safety analysis.

3.20 The use of available safety systems, when possible, in DEC without significant fuel degradation has the important advantage that safety systems are designed with very stringent reliability criteria. In such cases, the rules for safety analyses [8] use less conservative methods and assumptions but they should still ensure a high confidence in the result (in particular regarding the prevention of cliff edge effects) that cannot be simply achieved by best estimate calculations. If the rules were the same, there would not be a need for differentiation between DBA and DEC.

3.21 As indicated in para. 3.17, DEC without significant fuel degradation have the potential to exceed the capabilities of safety systems designed for the mitigation of DBAs. However, the analysis of DBAs is required to be carried out conservatively to demonstrate compliance with established acceptance criteria. Therefore, for the conditions described in para. 3.12 (a) it may

be possible to show that some safety systems would be capable of (and be qualified for) mitigating the event under consideration, based on best estimate analyses and less conservative assumptions.

3.22 Design extension conditions should be considered for failures of safety systems designed both to cope with anticipated operational occurrences and DBAs. These include in many designs the anticipated transients without scram and station blackout.

3.23 Design extension conditions should also be considered to reduce the frequency of severe accidents caused by failures in the mitigation of some DBAs to acceptable levels by, if possible, the use of additional, diverse measures to cope with common cause failures of safety systems.

3.24 Design extension conditions without significant fuel degradation constitute a reinforcement of the design for some complex and unlikely failure sequences. As some safety systems are designed to cope with various DBAs (e.g. the emergency core cooling is designed for several sizes and locations of loss of cooling accidents or main steam line breaks), safety features for DEC can help to reinforce the capability of the plant for specific sequences improving and balancing the risk profile applying less stringent design or safety assessment criteria than for DBA conditions. The reliability of safety systems should be high enough for DEC without significant fuel degradation to only be postulated exceptionally and to occur with a frequency lower than the most limiting DBAs.

Design extension conditions with core melting

3.25 In accordance with para. 5.30 of SSR-2/1 (Rev. 1) [1], a set of representative accidents with core melting should be used to provide inputs for the design of the containment and of the safety features ensuring its integrity. This set of accidents should be considered in the design of the corresponding safety features for DEC and should be a set of bounding cases that envelop other severe accidents with more limited degradation of the core, or lower loads on the SSCs that fulfil the confinement function.

3.26 The accident conditions chosen should be justified based on engineering judgement and insights from the probabilistic safety analyses: see SSG-53 [5]. A detailed analysis should be performed and documented to identify and characterize accidents that can lead to core damage. For new nuclear power plants, accidents involving core melting are postulated as DEC, irrespective of the fact that the design provisions taken to prevent such conditions make the probability of core damage very low. Aspects that affect the accident progression and that influence the containment response and the source term should be taken into account in the design of the safety features, as indicated in SSG-53 [5].

3.27 The capability and reliability of the safety features to cope with DEC with core melting should be evaluated to ensure that they are adequate for the safety function that they need to fulfil.

3.28 The challenges to plant safety presented by DEC with core melting, and the extent to which the design may be reasonably expected to mitigate their consequences should be

considered in establishing the severe accident management guidelines or guides. Recommendations in this regard are provided in IAEA Safety Standards Series No. SSG-54, Accident Management Programmes for Nuclear Power Plants [14]

3.29 Radioactive releases due to leakage from the containment in a severe accident should remain below the design leakage rate limit for sufficient time to allow implementation of emergency measures. Beyond this time, containment leakages could exceed this limit but still be well below the criterion for a large radioactive release. This may be achieved by provision of adequate filtered containment venting or other design features or alternative measures that could be included in an overall demonstration of adequacy of the containment function.

3.30 A safety assessment of the design should be performed with consideration of the progression of severe accident phenomena and their consequences, and addressing applicable topical issues such as the following:

— Corium stratification and criticality;
— Thermal-chemical interaction between corium, steel components and vessel;
— Heat transfer from corium to vessel or end-shield;
— Combustion of hydrogen and other gases;
— Steam explosion due to molten fuel-coolant interaction;
— Corium-concrete interaction;
— Containment over pressurization
— Containment overtemperature.

More detailed information is provided in SSG-2 (Rev. 1) [8].

ASSESSMENT OF THE IMPLEMENTATION OF THE DEFENCE IN DEPTH CONCEPT

3.31 The concept of defence in depth, as implemented in the design of a nuclear power plant, is required to be assessed to ensure that each level is adequately designed to meet its goals in terms of prevention, detection, limitation and mitigation. Requirement 13 of GSR Part 4 (Rev. 1) [2], states:

> "**It shall be determined in the assessment of defence in depth whether adequate provisions have been made at each of the levels of defence in depth.**"

3.32 Paras 4.45–4.48A of GSR Part 4 (Rev. 1) [2] contain additional requirements on this assessment.

3.33 This section also considers Requirement 7 of SSR-2/1, (Rev. 1) [1] for the application of defence in depth in the design of nuclear power plants. In particular, this section provides recommendations on a top level assessment of the implementation of defence in depth by plant designers and licensees, with specific focus on the levels of defence in depth corresponding to accident conditions.

3.34 The performance and reliability of safety provisions for different plant states should be assessed taking into consideration the level of risk and their safety significance. Such safety

provisions should be designed to maintain the integrity of the barriers to the extent necessary for the relevant plant state, or to mitigate the consequences of postulated failures. The assessment should provide evidence that the performances and reliability of the safety provisions corresponding to each level of defence in depth is adequate. It should demonstrate that, for each credible initiating event, the risk has been reduced as low as reasonably practicable, considering also internal hazards and/or external hazards that could cause the event. The assessment should consider insights from engineering analyses and from deterministic and probabilistic safety analysis, as appropriate for the different plant states. 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 by relying on the efficacy of other levels. In a sound and balanced design, SSCs of each level of defence are characterized by a reliability commensurate to their function and their safety significance.

3.35 The defence in depth strategy in the design of a nuclear power plant should be applied to all radioactive sources that could potentially harm plant personnel or the public, or contaminate the environment, taking into account a graded approach. The following are examples of sources that should be considered:

— Reactor core;

— Fresh fuel, spent fuel and fuel casks;

— Neutron sources and other radioactive sources;

— Airborne activity in buildings;

— Piping and process equipment containing radioactive material (reactor coolant system, reactor cooling systems, auxiliary systems, HVAC of the controlled areas, gas and liquid effluent treatment systems, solid waste treatment systems).

3.36 For each identified source of radiation, the physical barriers (including the boundaries) should be identified and an evaluation of their robustness should be provided. The following aspects should be taken into account in the evaluation:

(a) Each barrier should have been designed with an appropriate margin and the evaluation of robustness of the various barriers should be conducted by applying a graded approach on the basis of the radiation risks or of the safety class of the equipment forming the barrier.

(b) Codes used for the design and manufacturing or construction of barriers should be appropriate, and proven materials and technologies for the manufacturing or construction should be used.

(c) All loads and combination of loads that can apply to the barriers in operational states and accident conditions, including loads caused by the effects of the internal hazards and external hazards considered in the design, should be identified, calculated and be less than the applicable limits. The best estimate of equipment survivability and functionality is appropriate for assessing severe accident performance. For robustness, the limits should be met with adequate margins to cover uncertainties in the calculation and to avoid a cliff edge effect when loads considered for the design are exceeded.

(d) For barriers considered as ultimately necessary to prevent an early radioactive release or a large radioactive release, margins to failure should be assessed to determine if these are adequate to withstand loads caused by natural hazards of a severity exceeding that considered for the design;

(e) The number of barriers provided in the design should be justified. The assessment of defence in depth should examine various barrier options and demonstrate that the barriers chosen for each plant state offer the best protection for workers and the public that may be reasonably expected.

(f) Valves, their control equipment and other equipment that is used in the barrier boundary to prevent radioactive release should have been designed to ensure barrier integrity in accident conditions.

(g) Any deviation of a barrier from its normal configuration (such as open containment to accommodate certain activities when the plant is in a shutdown state) should be justified by demonstrating that adequate protection is maintained in spite of the temporary configuration (or operation) of the barrier.

3.37 An analysis of the various mechanisms that could challenge or degrade the integrity of the barriers or the performance of the safety functions should be carried out in order to assess the adequacy of the safety provisions that are implemented to prevent the occurrence or stop the progression of such mechanisms. To the extent that different degradation mechanisms could necessitate different safety provisions, the adequacy and effectiveness of the safety provisions should be assessed separately for each degradation mechanism.

3.38 The adequacy and effectiveness of safety provisions should be assessed by performing deterministic safety analyses modelling the plant response for different boundary conditions representative of the various anticipated operational occurrences, DBA, DEC without significant fuel degradation and DEC with core melting. Recommendations on conducting deterministic safety analyses for the different plant states are provided in SSG-2 (Rev.1) [8].

3.39 The performance of safety provisions at each level of defence in depth is assessed through engineering assessment and deterministic analysis involving the use of validated and verified analysis codes and models to demonstrate that acceptance criteria are met with sufficient margins.

3.40 The reliability analysis of safety provisions for different plant states, as indicated in para. 3.34, typically uses probabilistic techniques and takes into account the layout and protective provisions against the effects of hazards, and potential commonalities in the design, manufacturing, maintenance and testing between redundant and diverse equipment.

3.41 Statements of reliability should be supported by equipment reliability data which is shown to be relevant to the installation being assessed, as well as to test data, the use of proven technologies and engineering practices, and feedback from operating experience. The reliability should also be supported by verification of compliance of the SSC with the applicable set of

design requirements. Reliability analyses for different systems or levels of defence in depth can be integrated in a probabilistic safety analyses to evaluate overall plant risk metrics, such as core damage frequencies or large early release frequencies.

3.42 It should be verified that diversity has been implemented in the design of systems fulfilling the same fundamental safety function in different plant states if a simultaneous failure of those systems would result in unacceptable damage to the fuel or radiological consequences.

3.43 Equipment for controlling anticipated operational occurrences is aimed at reducing the number of challenges to safety systems. It should be demonstrated that their reliability is such that anticipated operational occurrences only evolve into DBA conditions with a low frequency, well below the highest frequency of postulated initiating events categorized as DBAs.

3.44 The combined reliability of the safety systems designed to mitigate the consequences of a DBA should be sufficient to demonstrate with high confidence, that their probability of failure under the conditions expected for each accident sequence postulated is very low. A failure probability below than 10^{-3} in order of magnitude would be consistent with the strict requirements for reliability imposed to safety systems and supported by operational experience and testing.

3.45 Any vulnerabilities that could result in the complete failure of a safety system should be identified and considered in combination with postulated initiating events 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. an alternate AC power supply in case of the total loss of the emergency power supply, or a separate and diverse decay heat removal chain), which are unlikely to fail due to the same common cause, need to be implemented to strengthen the defence in depth and to prevent core melt.

3.46 Safety features for DEC without significant fuel degradation should be demonstrated to be sufficiently reliable for the accident sequences for which they are intended, in order to contribute to ensuring a core damage frequency below the established probabilistic targets.

3.47 The capacity and reliability of safety features specifically designed to mitigate the consequences of DEC with core melting should be adequate to ensure that the containment integrity will not be jeopardized during any postulated core melt sequence. However, since the analysis of core melt and its impact on containment integrity is surrounded by considerable uncertainties, only a limited reliability can be attributed to those components necessary to ensure the containment integrity after a core melt accident.

3.48 The assessment should include an evaluation of the adequacy and effectiveness of the different accident management strategies defined to cope with extreme scenarios. This evaluation should demonstrate that the likelihood of an accident having unacceptable consequences for people and the environment, and which relies on both fixed and non-permanent equipment to mitigate the consequences of such an accident, is extremely low.

INDEPENDENCE BETWEEN LEVELS OF DEFENCE IN DEPTH

3.49 Paragraph 4.13A of SSR-2/1 (Rev. 1) [1] states:

> "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."

3.50 Independence, as far as practicable, is an essential aspect of the effectiveness in the implementation of defence in depth. Some general plant design requirements in SSR-2/1 (Rev. 1) [1] address aspects contributing to it. Requirement 21 states:

> "**Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.**"

3.51 Requirement 24 of in SSR-2/1 (Rev. 1) [1] states:

> "**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.**"

3.52 Defence in depth is an essential pillar of nuclear power plant safety. It is used to organize the safety related architecture of the plant and to identify, for each plant state, the corresponding safety requirements. To apply the defence in depth principle, it needs to be ensured that, as far as practicable, the failure of a given level does not affect the robustness of the next level. For example, a failure, whether equipment failure or human error, at one level of defence or even combinations of failures at two levels of defence, should not propagate to jeopardise defence in depth at the subsequent levels. Engineering assessment, deterministic and probabilistic methods should be used to assess this independence.

3.53 It is recognized in the IAEA safety standards that full independence of the levels of defence in depth cannot be achieved. This is due to several factors and constraints, such as a potential common exposure to the effects of external hazards and/or internal hazards, an unavoidable sharing of some items important to safety, as well as human factors. The design of a nuclear power plant should consider all potential causes of dependencies and include and implement an approach to remove them to the extent reasonably practicable. Robust independence is essential and should be implemented among systems whose simultaneous failure would result in conditions having harmful effects for people or the environment. For this reason, safety features specifically designed to mitigate the consequences of accidents with degradation or melting of the core should, as far practicable, be independent from safety systems, in accordance with paras 4.13A and 5.29 of SSR-2/1 (Rev. 1) [1].

3.54 In order to ensure a very low frequency of occurrence of sequences resulting in severe accidents or unacceptable releases, it is necessary to demonstrate that the effectiveness of the levels of defence is not reduced by factors that compromise the independence of the levels of defence in depth. These factors are as follows:

(a) The sharing of systems or parts of systems for executing functions for different plant states, for example for normal operation and for design basis accidents.

(b) Common cause failures that can impact different levels of defence in depth. Typical root causes of such failures are undetected human errors in design or manufacturing, human errors in the operation or maintenance, inadequate qualification or protection against internal or external hazards.

3.55 Requirement 69 of SSR-2/1 (Rev. 1) [1] states:

> "**The design of supporting systems and auxiliary systems shall be such as to ensure that the performance of these systems is consistent with the safety significance of the system or component that they serve at the nuclear power plant.**"

Therefore, due consideration needs to be given to the dependence on the auxiliary systems and supporting systems.

3.56 The sharing of systems or parts of them for executing functions for different categories of plant states should be avoided. However, since this might not be always practical or possible, it should be ensured that within the sequence of events that may follow a postulated initiating event, a system credited to respond in a given plant condition should not have been needed for a preceding condition. Thus, complementary safety features designed to mitigate the consequences of DEC without significant fuel degradation should be independent from SSCs postulated as already failed in the sequence. This is especially important when safety systems are credited for the mitigation of DEC.

3.57 The SSCs needed for each postulated initiating event should be identified, and it should be shown by means of engineering analyses that the SSCs needed for implementing any one defence in depth level are sufficiently independent from the other levels. The adequacy of the achieved independence should also be assessed by probabilistic analyses.

3.58 The systems and components used for different plant states should be separated, within the same safety division, from one another by distance or protective structures if there is a possibility for consequential failures arising from a failure of a system or component for another plant state.

3.59 The systems needed for different plant states in accordance with the defence in depth concept should be functionally isolated from one another in such a way that a malfunction or failure in any plant state does not propagate to another. However, practical limitations of design allow exemptions, each of which should be justified. Thus, it is a common practice to use some safety systems for some anticipated operational occurrences. For example, the intervention of

the protection system may be necessary to shut down the reactor for some anticipated operational occurrences that cannot be controlled by the limitation system. For most reactor designs, the reactor trip system is designed as a safety system that is also needed for the control of accidents. In such cases, it should be shown that there is no practicable alternative to use of the safety system to cope with the anticipated operational occurrence, and that the use of the safety system for such an occurrence does not present a significant limitation on the use of the safety system to mitigate a DBA.

3.60 The systems intended for controlling severe accidents should be functionally and physically separated from the systems intended for other plant states. Safety features for DEC with core melting may, for good reasons, also be used for preventing severe core damage if it can be demonstrated that this will not undermine the ability of these systems to perform their primary function if conditions evolve into a severe accident (e.g. an alternate power supply for DEC with core melting could be connected if necessary to equipment for DEC without significant fuel degradation).

3.61 For instrumentation and control systems, it should be demonstrated that defence in depth within the overall instrumentation and control architecture is achieved by means of independent lines of defence, so that the failure of one line of defence is compensated for by the following one. This can be achieved by implementing independence between different levels of defence in depth and independence between redundant functions and by design for reliably. Means of supporting design for reliability and reducing the likelihood of common cause failures in I&C systems are physical separation, electrical isolation, functional independence and independence from the effects of communications errors, and diversity. Further recommendations are provided in SSG-39 [7].

3.62 The assessment of the implementation of defence in depth should demonstrate that independence between successive levels of defence is adequate to limit the progression of deviations from normal operation and to prevent harmful effects to the public and the environment should accidents occur. For this purpose, the assessment of the implementation of the defence in depth should aim to verify that the vulnerabilities for common cause failures, originated in the layout, design, manufacturing, operation and maintenance, between structures, systems and components that are claimed to be independent, have been identified and removed to the extent practicable. In particular, functional dependencies should be removed or justified.

3.63 The assessment should demonstrate that the safety features intended to respond first are not jeopardized by the initiating event. The assessment should demonstrate that the operability of the safety systems is not jeopardized by failures in systems designed for normal operation or anticipated operational occurrences.

3.64 The assessment should demonstrate that a failure of a support service system is not capable of simultaneously affecting redundant parts of a safety system (or a system fulfilling diverse safety functions) and thereby compromising the capability of these systems to fulfil their safety functions, or otherwise adversely affect the independence of safety systems or independence between levels of defence. For this purpose, the assessment should provide

evidence that the reliability, redundancy, diversity and independence of the support service is commensurate with the significance to safety of the system being supported.

3.65 An assessment of independence of SSCs that are necessary to mitigate the consequences of a single or a likely combination of external hazards on the plant should be conducted. It should be demonstrated that the postulated initiating event and the failures induced in the plant cannot result in common cause failure between the SSCs necessary for their mitigation.

4. PRACTICAL ELIMINATION OF EVENT SEQUENCES LEADING TO EARLY RADIOACTIVE RELEASES OR LARGE RADIOACTIVE RELEASES

4.1 The concept of practical elimination is introduced in para. 2.11 of SSR-2/1 (Rev. 1) [1], which states that "Plant event sequences that could result in high radiation doses or in a large radioactive release have to be 'practically eliminated'. This is an objective of the design, but as indicated in this paragraph, off-site protective measures might still be required by the responsible authorities. In relation to defence in depth, para. 2.13 of SSR-2/1 (Rev. 1) [1] also introduces the expectation that event sequences that would lead to an early radioactive release or a large radioactive release will be 'practically eliminated'. The footnotes to the relevant paragraph provide further clarification as follows:

— " An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the" protection of people and of the environment" (Footnote 3 of SSR-2/1 (Rev. 1) [1]).

— "The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise (Footnote 4 of SSR-2/1 (Rev. 1) [1]).

4.2 With regard to design, 'practical elimination' is normally considered to refer only to those events or sequences of events leading to or involving significant fuel degradation, i.e. a 'severe accident', for which the confinement of radioactive materials cannot be reasonably achieved. Those accident sequences have to be considered in the design for 'practical elimination', either by physical impossibility or by being extremely unlikely to occur with a high level of confidence.

4.3 The concept of 'practical elimination' should be considered as part of the overall safety approach for the design of nuclear power plants in accordance with Chapter 2 of SSR-2/1 (Rev. 1) [1]. As a result of the implementation of the four levels of defence in depth, the likelihood of off-site radioactive releases resulting from the failure of the prevention and mitigation of severe accidents should be very low. However, it is necessary to verify that there would not be credible plant conditions that cannot be effectively mitigated and thus lead to unacceptable consequences. This is where the aim of the 'practical elimination' concept lies: to reinforce defence in depth by a focused analysis of those conditions having the potential for 'unacceptable radioactive releases'. Practical elimination should not be seen as an alternative to severe accident mitigation: instead, efficient and reliable provisions should be implemented to mitigate

any core melt sequence, in accordance with the defence in depth concept. However, these provisions may have limited capabilities that could not reasonably cope with some specific severe accident conditions; those are the conditions that should be explicitly identified and practically eliminated.

4.4 The main issue of a severe accident condition is that there is the potential for having both large quantities of radioactive substances available and not confined in the fuel or by the reactor coolant system, together with severe accident phenomena that can potentially generate large amounts of energy and also very rapidly, making it impossible to ensure the containment integrity and thus giving rise to unacceptable releases.

4.5 When a severe accident occurs, it is necessary to ensure that radioactive materials released from the nuclear fuel will be confined. In situations of limited confinement, for example in accidents involving fuel storage or when the containment is open and cannot be closed in time, or there is an containment bypass that cannot be isolated, the only way to prevent unacceptable releases is to avoid the occurrence of a severe accident. In such cases, it may be necessary to demonstrate practical elimination by showing with a high degree of confidence that such severe accidents would be extremely unlikely.

4.6 SSR-2/1 (Rev. 1) [1] does not provide quantitative acceptance criteria for the radiological consequences of accident conditions, or for the magnitude of what is to be considered an early radioactive release (which is site specific as it considers the time restrictions to implement protective measures), or a large radioactive release. Therefore, acceptable limits for radiation protection, as well as probabilistic criteria or target values for the purpose of demonstrating the low frequency of a core damage accident or accident sequences leading to radioactive releases, should be established, consistent with the regulatory requirements.

4.7 When defining these radiological criteria or targets, it is necessary to acknowledge the significant difference in magnitude between the maximum radioactive release and radiological impact that can be generated in case of a successful mitigation of DEC with core melting, and the releases and impacts that are avoided as part of the application of the concept of practical elimination. This also ensures sufficient margins to take into account the uncertainty in analysing complex severe accident phenomena and the performance of the containment. Indeed, radiological criteria for DEC with core melting are defined in order to ensure, with a safety margin, that the radioactive releases would have limited consequences in area and time for people and the environment; therefore, there is a qualitative step between the maximum acceptable releases for DEC with core melting (i.e. in case of successful mitigation) and the magnitude of releases to be considered for the application of the concept of practical elimination. From the probabilistic point of view, event sequences that have been practically eliminated should only represent a very low contribution to the frequency of an early radioactive release or a large radioactive release, when the demonstration can be sustained by probabilistic analysis.

4.8 The first step for demonstrating the practical elimination of plant conditions that can lead to an early radioactive release or a large radioactive release is the identification of severe accident sequences having the potential to give rise to 'unacceptable radioactive releases'. This identification process is expected to result in a list of accident sequences that could be grouped into a small set of plant conditions. The identification process should be justified and supported by relevant information.

4.9 Practical elimination’ is used to confirm that all reasonably practicable design provisions have been implemented, across all levels of defence in depth to ensure that plant conditions for

which a large radioactive release or an early radioactive release could not be prevented, are physically impossible or highly unlikely with a high degree of confidence. Sufficiently robust arguments and evidence are needed to demonstrate the reliability of the lines of defence that are in place. Where further features could be implemented, either for prevention of accidents or for mitigation of the consequences, they should be considered, as far as reasonably practicable.

4.10 As part of the overall safety approach, the 'practical elimination' concept should be applied to a new nuclear power plant at the earliest design stage, when it's more practicable to design and implement additional[3] safety features. The incorporation of such features is an iterative process using insights from engineering experience, and from deterministic safety analyses and probabilistic safety analyses in a complementary manner.

IDENTIFICATION OF POTENTIAL SEVERE ACCIDENT SEQUENCES LEADING TO AN EARLY RADIOACTIVE RELEASE OR A LARGE RADIOACTIVE RELEASE

4.11 The issue when considering whether to practically eliminate a severe accident sequence is the potential for a confinement function failure.

4.12 To help ensure the assessment of practical elimination is manageable, the whole set of individual accident sequences that might lead to an unacceptable radioactive release could be grouped to form a limited number of bounding cases or type of accident conditions. Thus, the following five general types could be considered, which should be assessed for applicability to specific designs:

(a) Events that could lead to prompt reactor core damage and consequent early containment failure, such as:

    (i) Failure of a large pressure-retaining component in the reactor coolant system;

    (ii) Fast reactivity insertion accidents.

(b) Severe accident sequences that could lead to early containment failure, such as:

    (i) Highly energetic direct containment heating;

    (ii) Large steam explosion;

    (iii) Explosion of combustible gases, including hydrogen and carbon monoxide.

(c) Severe accident sequences that could lead to late containment failure such as:

    (i) Basemat penetration or containment bypass during molten core concrete interaction;

    (ii) Long term loss of containment heat removal;

    (iii) Explosion of combustible gases, including hydrogen and carbon monoxide.

(d) Severe accident with containment bypass such as:

[3] 'Additional' is intended here to describe any design provision that is implemented following practical elimination assessment to support the demonstration of 'practical elimination' of some accident sequences, considering that some design provisions already implemented to support other safety objectives and analyses can participate in the demonstration.

(i) Loss of coolant accident with the potential to drive the leakage outside of the containment via supporting systems (interface system-LOCAs). As the containment function might be jeopardised by the initiating event, any escalation to significant fuel degradation has to be analysed and, where relevant, considered for 'practical elimination';

(ii) Containment bypass consequential to severe accident progression (e.g. induced steam generator tube rupture);

(iii) Severe accident in which the containment is open[4] (e.g. shutdown state).

(e) Significant fuel degradation in a storage fuel pool and uncontrolled releases[5].

4.13 The classification and grouping in para. 4.12 is consistent with the recommendations provided in SSG-53 [5] and SSG-2 (Rev. 1) [8], highlighting some examples of severe accident conditions for practical elimination consideration. Other classification or grouping criteria are also possible. Note also that the consequences from the accidents in para. 4.12(c)(i) and 4.12(c)(ii) could be mitigated by the implementation of reasonable technical means. In such cases, for scenarios not retained within the scope of practical elimination, evidence of the effectiveness and an appropriate reliability of the mitigation is necessary. To facilitate the grouping proposed, each type of accident sequence should be analysed to identify the associated combination of failures or associated physical phenomena that are specific to the plant design, and which have the potential to lead both to severe accident sequences and 'unacceptable radioactive releases'. This analysis helps identifying accident sequences that could lead to conditions that need to be 'practically eliminated'.

4.14 The approach described in paras 4.12 and 4.13) combines, when relevant, the following:

(a) A phenomenological (top-down) approach, which considers any phenomena that might challenge the confinement safety function in the course of a severe accident, in order to define a comprehensive list of severe accidents as described in para. 4.12;

(b) A sequence-oriented (bottom-up) approach, which reviews any accident sequence leading to a severe accident. For each sequence, any challenge to the confinement safety function is assessed (this may require evaluation of the loads onto containment and of possible release routes via leakages and bypasses). This supplements the top-down approach with a broader screening to identify any relevant accident sequence.

4.15 All possible normal operating modes of the plant (e.g. start-up, power operation, shutdown, refuelling, maintenance) should be considered in the identification process, including modes with open containment.

[4] Currently, the technology used for equipment hatches is generally not fast enough to ensure re-closure and restoration of the containment integrity. Therefore, any significant rapid fuel degradation mechanism in shutdown operating modes with an open containment should be considered for 'practical elimination'.

[5] Most plant designs in various States locate the spent fuel pool outside of the containment, given the slow kinetics of accidents likely to lead to severe damage of the fuel assemblies stored in the spent fuel pool. The timescales enable the implementation of on-site or off-site prevention or protective measures. This option is considered as the best choice in the decision making process compared to the additional costs and operational constraints if the spent fuel pool were also located in the reactor building. However, this does mean that any occurrence of significant fuel degradation in the pool would directly lead to a large radioactive release. Therefore, any accident sequence with significant degradation of the fuel assemblies stored in the spent fuel pool has to be considered for 'practical elimination'

4.16 All plant locations and buildings where nuclear fuel is stored should be considered in the identification process, including the irradiated fuel storage.

4.17 It may be useful also to classify accident scenarios taking into account the progression from an initiating event to the consequences that need to be avoided. Three type of scenario can be considered:

— Type I: scenarios with an initiating event that leads directly to severe fuel damage and early failure of the confinement function.

— Type II: severe accident scenarios with phenomena that induce early failure of the confinement function.

— Type III: severe accident scenarios that result in late failure of the confinement function.

IDENTIFICATION AND ASSESSMENT OF SAFETY PROVISIONS FOR PRACTICAL ELIMINATION

4.18 The overall objective is to assess if the design is appropriate for preventing the accident sequences identified and grouped in a short list of accident scenarios for practical elimination.

4.19 The assessment aims at identifying design and operational features that could be implemented, either for prevention or for limitation of the consequences of the severe accident condition. In this assessment and later in the demonstration of ‘practical elimination’ of a severe accident condition, the following should be considered:

(a) The state of the art in nuclear science and technology;

(b) The technical and industrial proven feasibility;

(c) The potential drawbacks of additional provisions that might not be seen immediately (e.g. operational constraints);

(d) The kinetic of the adverse phenomena that might threaten the containment or its leaktightness;

(e) The independence of design provisions from the capability for on-site actions or use of off-site staff and equipment.

4.20 The identification of safety provisions necessitates a comprehensive analysis of the physical phenomena involved and it may be necessary to further refine the identification of elementary accident sequences performed in accordance with para. 4.14.

4.21 This identification aims at defining several options to be submitted to the decision making process for establishing reasonably practicable design and operational provisions to achieve practical elimination. This results in a design with a consistent and robust combination of lines of defence in depth.

4.22 The design of provisions for practical elimination should be done on a case-by-case basis and, where relevant, associated to the appropriate level of defence in depth or plant state at which the sequence of events would be interrupted to prevent unacceptable consequences. It

should be verified that the corresponding engineering design rules and technical requirements have been followed to ensure that they would confidently achieve their safety function, under the prevailing conditions, e.g. the harsh environmental conditions associated to a severe accident. In assigning requirements, where relevant, appropriate testing, operational procedures, and in-operation monitoring as well as in-service testing and inspection should be considered. The requirements should be applied at all steps from design to operation, including manufacture, construction or implementation on site, commissioning and periodic testing.

4.23 Design provision and operational provision for practical elimination of some severe accident conditions could require human actions to be performed (e.g. the opening of primary circuit depressurization valves to prevent high-pressure core melt conditions). In this case a human factor assessment should be part of the justification needed to support any claim for high reliability of operator actions. Examples of items the assessment should include as part of the determination of high reliability are as follows:

(a) The availability of information given to operating personnel to perform the action from the control room or locally, and the quality of procedures or guidelines to implement the actions;

(b) The environment for performing the action (e.g. access to local area, components to be handled, identification of components location and ambient conditions). Local actions during a severe accident in hazardous conditions are likely to reduce the necessary reliability for demonstration of practical elimination;

(c) The timescales to perform the action, including sufficient margin to achieve it.

4.24 Design provisions and operational provisions for “practical elimination” of some severe accident might be vulnerable to potential human errors prior to the accident. This type of human error could cause latent risks to be introduced that might prevent successful operation when called upon during an event or accident. In such a case, the SSCs used to deliver the action should be subject to relevant operational provisions to limit the risk from this type of human error (e.g. periodic testing, in-service inspections, commissioning tests following maintenance activities, periodic system alignment checks).

4.25 Some safety provisions ultimately necessary to prevent an early radioactive release or a large radioactive release that support the demonstration of ‘practical elimination’ are designed to withstand relevant (i.e. consequential to the condition or likely to arise concurrently) internal and external hazards, with appropriate margin. Paragraph 5.21A of SSR-2/1 (Rev. 1) [1] states:

> ”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.”

4.26 Where design provisions and operational provisions rely on support functions and systems, the latter are all designed to the standards necessary to ensure the SSCs they support will have same level of separation, diversity, robustness to hazards as the main design provisions, or be tolerant to the loss of support functions.

DEMONSTRATION OF ‘PRACTICAL ELIMINATION’

General Aspects

4.27 The demonstration of practical elimination should be based on the assessment of provisions that would generally include engineering judgement and deterministic and probabilistic analyses. Some of the categories of conditions defined in para. 4.12 for the demonstration of practical elimination entail very severe challenges to the integrity of the physical barriers for radionuclide retention and necessitate specific design and operation provisions for their practical elimination. The demonstration of practical elimination can be considered as part of the design and safety assessment process, including the necessary inspection and surveillance processes during manufacturing, construction, commissioning and operation.

4.28 The measures to prevent the event sequences in each of the categories in para. 4.12 from occurring should be provided and their effectiveness should be analysed. None of the phenomena and plant conditions indicated should be overlooked because of low likelihood, but credible research results and dedicated means to minimize the identified risks are necessary to support the safety claims.

4.29 For each accident sequence considered for ‘practical elimination’, an assessment has to be performed to demonstrate the acceptability of the design or to define additional design provisions to be implemented. It should be demonstrated that it is physically impossible for the condition to arise or for the condition to be extremely unlikely to arise, with a high level of confidence.

4.30 As shown in para. 4.12, the various accident sequences to be considered for ‘practical elimination’ are rather different in essence. As a consequence, demonstrations of ‘practical elimination’ are expected to be provided on a case-by-case basis reflecting this variety.

4.31 Uncertainties due to limited knowledge of some physical phenomena, in particular those resulting from severe accident phenomena, have to be considered when conducting engineering as well as deterministic and probabilistic analyses to ensure a high level of confidence.

4.32 The justification of ‘practical elimination’ should preferably rely on a demonstration of physical impossibility for the accident sequence to occur. If this is not achievable, a demonstration of an extremely low likelihood of occurrence with a high level of confidence should be provided.

4.33 The safety analysis report of the plant should reflect the measures taken to practically eliminate conditions arising that could lead to an early radioactive release or a large radioactive release. The report should include, either directly or by reference, all elements of the demonstration of the acceptability of the design with all relevant design provisions included.

Physical impossibility

4.34 Where a claim is made that a condition that needs to be ‘practically eliminated’ is physically impossible, it is necessary to demonstrate that the inherent safety characteristics of the system or reactor type ensure that the condition cannot, by the laws of nature, occur and that the fundamental safety functions (see Requirement 4 of SSR-2/1 (Rev.1) [1]) are fulfilled.

4.35 In practice, the physical impossibility approach is limited to very specific cases. Demonstration of physical impossibility cannot rely on measures requiring active components or human interactions. Should such a case arise, it would be heavily challenged. An example could be the effect of heterogeneous boron dilution for which the main protection is provided by ensuring a negative reactivity coefficient for all possible combinations of the reactor power and coolant pressure and temperature. In this case, physical impossibility applies only to a prompt reactivity insertion accident.

Extremely unlikely to arise with a high level of confidence

4.36 The expression ‘extremely unlikely’ is by definition a probabilistic notion. Although probabilistic targets can be set (e.g. frequencies of core damage or radioactive releases), the demonstration of practical elimination cannot be approached only probabilistically. Probabilistic insights should be used to support deterministic and engineering analysis for the demonstration of practical elimination. Also, meeting a probabilistic target alone is not a justification to exclude the analysis and possible implementation of additional reasonable design or operational measures to reduce the risk. Thus, a low probability of occurrence of an accident with core damage is not a reason for not protecting the containment against the conditions generated by such accident. In fact, design extension conditions with core melting need to be postulated in the design, in accordance with Requirement 20 of SSR-2/1 (Rev. 1) [1].

4.37 The demonstration of very low likelihood with a high level of confidence should rely on the assessment of engineering aspects, deterministic considerations, supported by probabilistic considerations to the extent possible, taking into account the uncertainties due to the state of knowledge of some physical phenomena. The demonstration for a condition to be ‘practically eliminated’ should consider the following, as applicable:

(a) The several lines of defence consisting of equipment and organisational provisions;

(b) The robustness of these lines of defence (e.g. adequate margins, adequate reliability, qualification against operation conditions);

(c) The independence between these lines of defence (i.e. adequate combination of redundancy and physical separation, diversity, functional independence).

4.38 When ‘practical elimination’ of an accident sequence is supported by deterministic calculations, computer codes and/or analytical calculations should be validated against the specific phenomena. They should reflect best knowledge so as to provide reliable prediction of the accident sequence and the involved phenomena. Analysis of severe accidents should be performed using a realistic approach (see Option 4 in Table 1, Section 2 of SSG-2 (Rev. 1) [8]) to the extent practicable. Because, explicit quantification of uncertainties may be impractical due to the complexity of the phenomena and insufficient experimental data, sensitivity analyses should be performed to demonstrate the robustness of the results and the conclusions of the severe accident analyses.

4.39 The decision whether or not to establish probabilistic targets to support the ‘practical elimination’ of accident sequences that could lead to unacceptable releases, falls under the responsibility of the regulatory body. When it is claimed that a particular accident condition has been practically eliminated on the basis 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 where such as target been established by the regulatory body.

4.40 The validity of the model used should be checked against the dedicated condition to assess. The limitations and uncertainties should be identified, bearing in mind that limitations of probabilistic safety assessment studies are associated with the probabilistic modelling, as well as the supporting deterministic best-estimate studies.

4.41 When the accident sequence to be 'practically eliminated' is the result of a single initiating event such as the failure of a large pressure-retaining component[6], the demonstration should rely on achieving a high level of quality at all stages of the component lifetime: design, manufacturing, implementation, commissioning, operation (periodic testing and in-service monitoring, if any) to prevent the occurrence and propagation of any defect liable to cause the failure of the component. Hence, the occurrence of the initiating event (e.g. failure of a large pressure-retaining component of the facility) or the consequential event (i.e. uncontrolled reactivity accident) needs to be considered for 'practical elimination'.

5. MINIMIZATION OF THE RADIOLOGICAL CONSEQUENCES OF VERY UNLIKELY CONDITIONS EXCEEDING THE PLANT DESIGN BASIS

5.1 The design basis of items important to safety at nuclear power plants is established taking into account the most limiting conditions under which they need to operate or maintain their integrity. However, it is possible, although very unlikely for a well designed nuclear power plant, that some conditions arise that exceed the margins of the design of some SSCs, thus impairing the fulfilment of safety functions. This is particularly important for the case of natural hazards, for which the occurrence of hazards of a magnitude that exceeds the safety margin of the most vulnerable SSC important to safety is generally a matter of probability. There have been cases in which some external natural hazards, such as extreme earthquakes, floods and tsunamis have exceeded the levels considered for the design as a result from the site evaluation. Paragraphs 5.21 and 5.21.A of SSR-2/1 (Rev. 1) [1] require sufficient margins against external hazards for such cases in the design[7].

5.2 SSR-2/1 (Rev. 1) [1] introduced the need to include features to enable the use of non-permanent equipment for the following:

(a) Restoring the necessary electrical power supplies (see para. 6.45A of SSR-2/1 (Rev. 1) [1]);

(b) Restoring the capability to remove heat from the containment (see para. 6.28B of SSR-2/1 (Rev. 1) [1]);

(c) Ensuring sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation (see para. 6.68 of SSR-2/1 (Rev. 1) [1]).

5.3 The use of non-permanent equipment for other similar purposes, e.g. the removal of residual heat from the core is not explicitly required, but not excluded. The aim of the use of such equipment is to restore safety functions that have been lost, but not to be the regular means to achieve these functions in accident conditions. Non-permanent equipment should not be

[6] Note that in some Member States, this demonstration is associated to other concepts such as 'Incredibility of Failure', 'High Integrity Component', 'Non-breakable component', rather than to the 'practical elimination' concept.

[7] Some Member States have a more formal approach to this issue by considering a higher level of hazards which has to be considered in design, although with realistic analysis assumptions and possibly relaxed failure criteria and dose limits.

credited in demonstrating the adequacy of the nuclear power plant design (see para. 7.51 of SSG-2 (Rev. 1) [8].[8]

5.4 In order to approach the implementation of design features for using non-permanent equipment, levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site should be considered and their consequences evaluated as part of the defence in depth approach. This should be done to establish accident management measures to increase the response capability of the nuclear power plant so as to make accidents with harmful radiological consequences very unlikely.

5.5 Particularly for external hazards, it is expected that the frequency of occurrence of a natural hazard significantly exceeding a well-established design basis derived from the site evaluation is very low. However, as such frequencies are generally associated with significant uncertainties, it is very important to understand the behaviour of SSCs to loading parameters resulting from levels of external hazards above the design basis[9].

5.6 For each selected scenario, the evaluation should identify limitations on the plant response capability and should define a strategy to cope with these limitations. In the evaluation, the various coping provisions, accident management measures and equipment (fixed or non-permanent equipment stored on-site or off-site), that will be used to restore the safety functions and to reach and maintain a safe state should be identified. Such an evaluation should include the following:

(a) A robustness analysis of a relevant set of items important to safety to estimate the extent to which those items would be able to withstand natural hazards exceeding their design basis;

(b) An assessment of the extent to which the nuclear power plant would be able to withstand a loss of the safety functions without reaching unacceptable radiological consequences for the public and the environment;

(c) A definition of the coping strategies to limit and mitigate the consequences of the scenarios leading to a loss of key safety functions;

(d) An estimate of the necessary resources in terms of human resources, equipment, logistics and communication to confirm the feasibility of the strategies.

5.7 Some aspects of the use of non-permanent equipment and the associated safety assessment addressed in this Safety Guide cannot be fully considered in detail at the plant design stage and should be considered in more detail during the plant operation. However, where applicable, specific facilities and equipment, should be considered at the final stage of the design of new nuclear power plants. The evaluation should consider the possibility that multiple units at the same site could be simultaneously affected.

---

[8] These requirements in SSR 2/1 (Rev. 1) [1] were the result of the feedback from the Fukushima Daiichi accident and the stress tests or similar types of investigation conducted by Member States thereafter. Therefore, these measures were primarily introduced with the occurrence of extreme external hazards in mind, although it is not explicitly indicated in SSR 2/1 (Rev. 1) [1].

[9] The concept of practical elimination is applied to external hazards within the safety analysis due to the difficulties in providing a safety demonstration based on design features comparable to the full set of cases addressed in Section 4, and it is necessary to ensure in other terms that the risk of early radioactive releases or large radioactive releases as a result from extreme external hazards is very low.

5.8 The plant response and the coping strategy for a level of external hazard exceeding those considered for design should be assessed based on a realistic approach and be supplemented where relevant (e.g. in case of cliff edge effect) by sensitivity analyses where assumptions in the modelling or where important actions by operating personnel are identified as essential factors for the credibility of the strategy.

5.9 The coping strategies should be defined, and the associated coping provisions should be specified and designed taking into account the most unfavourable possible scenario.

5.10 To make the coping strategies more reliable, an adequate balance between fixed equipment and non-permanent equipment should be implemented. This balance should be defined considering the coping time, the time for installation, flexibility of equipment for different purposes, human reliability, human resources and the total number of actions by operating personnel needed for the whole strategy. The use of permanent fixed equipment should be preferred for the implementation of short-term actions. However, use of non-permanent equipment as backup to potentially failed installed equipment, including for short-term actions, may provide innovative and diverse means to further reduce risk and should be considered.

5.11 The use of non-permanent equipment should be credited provided that the time period needed for their installation and putting in service is less than the defined coping time with a specified margin for time sensitive operator actions. Appropriate time margins to implement actions before the occurrence of a cliff edge effect should be established. This time period should be based, where possible, on times recorded during drills, or using other approaches for validating the actions of operating personnel. The ability to deliver and operate non-permanent equipment on time under adverse conditions at the site, and for events involving significant degradation of infrastructures and roads caused by extreme hazards on site and off site, should also be demonstrated. The storage location of non-permanent equipment at distance from the units can be of advantage in the case of some extreme natural hazards.

5.12 If non-permanent equipment is credited, its installation and use should be documented, and comprehensive training, testing and drills should be periodically conducted to maintain proficiency in the use of the equipment and associated procedures. Drills should consider to the extent reasonably possible the conditions of real emergencies.

5.13 Once the strategies are defined and validated, guidance for the operators as well as their technical basis should be established and documented (e.g. in emergency procedures or accident management guidelines).

5.14 To ensure the success and reliability of the strategies, the performances of the necessary coping provisions should be specified, and equipment should be designed and, when relevant, qualified in accordance with appropriate standards to ensure its functionality during and after conditions caused by an extreme external hazard or other extreme conditions taken into consideration.

5.15 The appropriateness of the strategies and coping provisions, and the feasibility of implementation under environmental conditions caused by extreme natural hazards or the radiological consequences of the accident (radiation and releases of radioactive materials) should be evaluated.

5.16 Where there is high confidence of the timely connection and operation of non-permanent equipment, their use could be credited for demonstration of the successful mitigation of an accident to prevent unacceptable radiological consequences.

REFERENCES

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

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

[3] 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).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-56, Vienna (2020).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-53, Vienna (2019).

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

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, Vienna (2016).

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

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, Vienna (2010).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-4, Vienna (2010).

[11] 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).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.13, Vienna (2005).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, UNITED NATIONS ENVIRONMENT PROGRAMME, Radiation Protection of the Public and the Environment, IAEA Safety Standards Series No. GSG-8, Vienna (2018).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-54, Vienna (2019).

ANNEX I. DEMONSTRATION OF PRACTICAL ELIMINATION FOR SPECIFIC COMMON CASES

FAILURE OF A LARGE COMPONENT IN THE REACTOR COOLANT SYSTEM

I-1. A sudden mechanical failure of a single large component in the reactor coolant system 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, in which a break would eliminate the capability of holding and cooling the core. In addition, the likelihood of pressurizer and steam generator shell failure need to be shown to be extremely low, or alternatively it needs to be demonstrated that a failure of the pressurizer or steam generator would not lead to unacceptable consequences to the containment.

I-2. 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 topics:

(a) The most suitable composition of materials needs to be selected;

(b) The metal component or structure needs to be as defect-free as possible;

(c) The metal component or structure needs to be tolerant of defects;

(d) The mechanisms of growth of defects need to be known;

(e) Design provisions and suitable operation practice need to be in place to minimize thermal fatigue, stress corrosion, embrittlement, pressurized thermal shock and over-pressurization of the primary circuit;

(f) An effective in service inspection and surveillance programme needs to be in place during the manufacturing, construction, commissioning 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.

I-3. In addition, evidence needs to be provided to demonstrate that the necessary level of integrity will be maintained for the most demanding situations.

I-4. Several sets of well established technical standards are available for ensuring reliability of large pressure vessels, and the demonstration of 'practical elimination' of vessel failures can be based on rigorous application of these technical standards. The technical standards also provide instructions for verification of the state of pressure vessels during the plant lifetime.

I-5. The practical elimination of failures of large components is thus achieved by the essential means of the first level of defence in depth without relying on the subsequent levels of defence in depth.

I-6. The demonstration of low failure likelihood with a high level of confidence could be supplemented by a probabilistic fracture mechanics assessment, which is a widely recognized and commonly used technique. Probabilistic assessment in the demonstration of practical

elimination, and especially 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.

FAST REACTIVITY INSERTION ACCIDENTS

I-7. 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 first level of defence in depth by proper design of the reactor coolant system and the core. The main protection is provided by an overall negative reactivity coefficient under all possible combinations of reactor power, neutron absorber concentration, coolant pressure and temperature, thus suppressing reactor power increase during any disturbances and eliminating the reactivity hazards with help of the laws of nature (demonstration of practical elimination by impossibility of the conditions).

I-8. An uncontrolled reactivity excursion could potentially be caused by sudden insertion of a cold or under-borated water slug into a reactor core. Nevertheless, all potential risks of sudden changes in the coolant properties need to be identified and prevented by design provisions.

I-9. 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 or limit insertions of reactivity, e.g. injection of water with low boron concentration in the core that can be evaluated deterministically and probabilistically as appropriate to demonstrate that they are extremely unlikely to occur.

I-10. More complex situations could arise however if criticality can be reached during severe accidents. This has been a topic of concern in specific core meltdown scenarios in reactors where the control rod material has a lower melting point and eutectic formation temperature than the fuel rods. A potentially hazardous scenario might occur if the reactor vessel were reflooded 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 by considering the design provisions and severe accident management features together, to reach a plausible conclusion that the condition has been practically eliminated.

DIRECT CONTAINMENT HEATING

I-11. In light water reactors, core meltdown at 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 therefore need to be eliminated by design provisions to depressurize the reactor coolant system when a meltdown is found unavoidable. In pressurized heavy water reactors, direct containment heating due to ejection of the molten core at high pressure is practically eliminated because pressure tubes would fail rapidly at high fuel temperature. This would depressurise the primary system before significant core melting can occur.

I-12. 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. For such situations, there needs to 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 conditions can be practically eliminated. The depressurization needs to 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, it is important that dynamic loads from depressurization do not cause a threat to the essential containment structures.

I-13. Dedicated depressurization systems have been installed in existing plants and designed for new plants. At pressurized water reactors they are based on simple and robust devices and straightforward actions by operating personnel that eliminate the risk of erroneous automatic depressurization but provide adequate time to act when need arises. At boiling water reactors the existing steam relief systems generally provide means for depressurization, with possibly some modifications in valve controls to also ensure reliable valve opening and open valve positions in very low pressures.

I-14. A deterministic analysis is necessary to demonstrate the effectiveness of the depressurization system in preventing direct containment heating. Traditional probabilistic safety assessment techniques are adequate to demonstrate a high reliability of the depressurization systems including the initiation by operating personnel. 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.

LARGE STEAM EXPLOSION

I-15. The interaction of the reactor core melt with water, known as fuel-coolant interaction, is a complex technical issue involving a number of thermal-hydraulic and chemical phenomena. Fuel-coolant interactions 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 might lead to an energetic fuel-coolant interaction, commonly known as ‘steam explosion’, which represents potentially serious challenge to the reactor vessel and/or containment integrity.

I-16. The conditions of the triggering of the steam explosion and the energy of explosion in various situations have been widely studied in reactor safety research programs. Although non-triggered steam explosion seems 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.

I-17. For eliminating steam explosions that could damage the containment barrier, the preferred method is to avoid the dropping of molten core into water in any conceivable accident scenarios. Such approach is used in some pressurized water reactors, such as 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 boiling water 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 needs to 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.

EXPLOSION OF COMBUSTIBLE GASES: HYDROGEN AND CARBON MONOXIDE

I-18. Hydrogen combustion is a 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, although different means are preferred for different plant designs.

I-19. In boiling water reactor containments that are all relatively small, the main means of protection is filling of the containment with inert nitrogen gas during power operation. In large pressurized water reactor containments the current practice is to use passive catalytic recombiners or other devices that control the rate of the oxygen and hydrogen recombination.

I-20. 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 excessive local hydrogen concentrations. Furthermore, the risk of hydrogen detonation increases if steam providing inertization is condensed.

I-21. 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.

I-22. The design provisions for preventing hydrogen detonation need to be assessed in order 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 molten core concrete interaction when the amount of hydrogen exceeds the capacity of recombination due to lack of oxygen in the containment.

I-23. Carbon monoxide can be generated in a severe accident if corium discharged from the reactor vessel interacts with concrete structures. The amount and timing of carbon monoxide generated depend on the particular core melt scenario, the type of concrete and geometric factors. Mixtures of carbon monoxide and air can be also explosive, although the chemical reaction is less energetic than the hydrogen combustion and the burning velocity is also lower. Therefore, the contribution of carbon monoxide to the threats of containment integrity has received less attention. However, carbon monoxide increases the combustible gas inventory in the containment and influences also flammability limits and burning velocities of hydrogen. Therefore, the influence of carbon monoxide needs to be considered. A practical design measure to minimize the impact of carbon monoxide is the use concrete with low contents of limestone.

LONG TERM LOSS OF CONTAINMENT HEAT REMOVAL

I-24. In a situation where core decay heat cannot be removed by heat transfer systems to outside of the containment and further to an 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.

I-25. There are several examples, 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.

I-26. An alternative to cooling is to eliminate the containment overpressure by venting. This is necessary especially in some boiling water reactors where the size of the containment is small and pressure limitation may be needed both in the DBA as well as in DEC with core melt. The existing venting systems prevent overpressurization at the cost of some radioactive release involved in the venting, also in the case that the venting is filtered, which would be the only acceptable type for severe accidents.

I-27. 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.

I-28. 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 level 2 probabilistic safety assessment can be used to demonstrate the very low probability (i.e. practical elimination) of event sequences leading to large releases.

CONTAINMENT PENETRATION BY INTERACTION WITH THE MOLTEN CORE

I-29. 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 combustible gases, hydrogen and carbon monoxide, as well as other non-condensable gases, which could contribute also to eventual overpressure failure of the containment.

I-30. Alternative means have been developed and verified in extensive severe reactor accident research programs in this area conducted nationally and in international co-operation. The means suggested include the following:

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

I-31. In all of these approaches, cooling of the corium generates steam inside the containment, and it is necessary to provide features for heat removal from the containment that are independent, to the extent practicable, of those used in more frequent accidents.

I-32. While probabilistic safety assessment 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.

SEVERE ACCIDENTS WITH CONTAINMENT BYPASS

I-33. Containment bypass can occur in different ways, such through circuits connected to the reactor coolant system that exit the containment or defective steam generator tubes (for pressurized water reactors). Severe accident sequences with non-isolated penetrations connecting the containment atmosphere to the outside as well as severe 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.

I-34. It has to be taken into account that failures of lines exiting the containment and connected to the primary system, including steam generator ruptures, are at the same time accident initiators, whereas other open penetrations only constitute a release path in accident conditions.

I-35. 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.

I-36. Requirement 56 of SSR-2/1 (Rev.1) [I–1] establishes the minimum isolation requirements for various kinds of containment penetrations. The requirement addresses aspects of leaktightness and leak detection, redundancy and automatic actuations, as appropriate. Specific provisions are given also for interfacing failures in the reactor coolant system. National regulations address in more detail what are the applicable provisions for containment isolations and prevention of containment bypass or interfacing los of cooling accidents.

I-37. Based on the implementation of the design requirements or specific national 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, 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 steam generators 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 involve 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 severe accidents with containment bypass have been practically eliminated.

SIGNIFICANT FUEL DEGRADATION IN THE IRRADIATED FUEL STORAGE POOL

I-38. Facilities for spent fuel storage need to be designed to ensure that the potential for high radiation doses or radioactive releases to the environment are practically eliminated. To this end, it is necessary to ensure that spent fuel stored in a pool is always kept covered by an adequate layer of water. This requires the following:

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

I-39. Risks for mechanical fuel failures need to be eliminated by the following means:

(a) A design that ensures that heavy lifts moving above the spent fuel stored in the pool are avoided;
(b) Structures that eliminate the possibility of heavy lifts dropping on the top of the fuel.

I-40. In designs where the spent fuel pool 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 damages and prevent a later reflooding and cooling of the fuel.

I-41. In some designs, the spent fuel pool 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 molten fuel without means to stabilize it, 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’.

REFERENCES TO ANNEX I

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

ANNEX II. APPLICATION TO NUCLEAR POWER PLANTS DESIGNED TO EARLIER STANDARDS

II-1. Paragraph 1.3 of SSR-2/1 (Rev. 1) [II–1] states:

> "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. For the safety analysis of such designs, it is expected that a comparison will be made with the current standards, for example as part of the periodic safety review for the plant, to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements."

This implies that the capability of existing plants to accommodate accident conditions not considered in their current design basis and the practical elimination of plant conditions that can lead to early radioactive releases or to large radioactive releases need to be assessed with the objective of further improving the level of safety.

II-2. The concepts of design extension conditions and practical elimination of event sequences that could lead to early radioactive releases or large radioactive releases are not totally new. In fact, the last concept was already introduced in the former Safety Guide for the design of the reactor containment[10], and both concepts may have been applied partially in the design of some existing nuclear power plants, although not in a systematic way. Over time, design features to cope with conditions such as station blackout or anticipated transients without scram have been introduced in many nuclear power plants. Some plant conditions to be practically eliminated have been addressed also in many designs already, although a specific demonstration in accordance with the concept of practical elimination has not been carried out.

II-3. It is important to note however, that an accident condition commonly considered as a design extension condition in new nuclear power plants (e.g. station blackout or anticipated transients without scram), is only such if safety features have been introduced in the design to mitigate its consequences. Otherwise, it would remain a beyond design basis accident. For the case of station blackout, an alternate power source capable of supplying power in due time to essential loads over a sufficient time period until external or emergency power is recovered would be such a safety feature. For anticipated transients without scram, additional design features are necessary to render the reactor subcritical in case of failure in the insertion of control rods to prevent the failure of the reactor coolant system.

II-4. In relation to practical elimination, a number of measures may have been taken for the practical elimination of some conditions leading to early radioactive releases or large radioactive releases. This includes for instance the prevention of a break in the reactor pressure vessel, fast reactivity insertion accidents or severe fuel degradation in the irradiated fuel storage. However, a demonstration that the existing safety provisions are sufficient to claim the practical elimination of such conditions might not have been conducted, in the way required by IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [II–1] and as recommended in this Safety Guide.

---

[10] 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).

II-5. Generally, it expected that during a periodic safety review or a reassessment of plant safety, or as part of a request for lifetime extension or similar processes, a feasibility of reasonable safety improvements in relation to design extension conditions and practical elimination would be considered. There can, however, be important constraints to install the same type of design features commonly implemented in the design of new nuclear power plants, especially for design extension conditions with core melting. In the same context, the independency of safety provisions related to the different levels of defence in depth will need to be taken into account.

II-6. Safety provisions for design extension conditions and also design features for the practical elimination of conditions leading to early radioactive releases or large radioactive releases are addressed in several Safety Guides related to the design of plant systems, including the IAEA Safety Standards Series Nos: SSG-56, Design of the Reactor coolant and Associated Systems for Nuclear Power Plants [II–2]; SSG-53, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants [II–3]; SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [II–4]; and SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [II–5]. SSG-53 [II–3] encompasses most of the design features for design extension conditions with core melting, and the event sequences to be considered for practical elimination involving severe accidents and needing the integrity of the containment to be maintained. SSG-53 [II–3] also contains an appendix in relation to nuclear power plants designed to earlier standards that provides recommendations for upgrading of the plant design in relation to these aspects.

II-7. Safety systems of existing plants were designed for design basis accidents, without account being taken of the possibility of more severe accidents. However, the conservative deterministic approaches originally followed in the design might have resulted in the capability to withstand some situations more severe than those originally included in the design basis for existing plants. As indicated in para. 3.20, for design extension conditions without significant fuel degradation, it can be acceptable for postulated initiating events less frequent than those considered for DBAs to demonstrate that some safety systems would be capable of and qualified for mitigating the consequences of such events if best estimate analyses and less conservative assumptions are used. This is a possibility for existing nuclear power plants to demonstrate the capability for mitigation as a design extension condition of events not originally postulated in the design, such as the multiple rupture of steam generator tubes.

II-8. The consideration of external events of a magnitude exceeding the original design basis, as it is addressed in Section 5, is a part of the safety reassessment of existing nuclear power plants that needs to be considered. While for new nuclear power plants the mitigation of design extension conditions is expected to be accomplished by permanent design features, and the use of non-permanent equipment is intended for very unlikely external events of a magnitude exceeding the original design basis, for existing nuclear power plants the use of non-permanent equipment with adequate connection features can be the only reasonable improvement in some cases. Relying on non-permanent equipment may be adequate provided there is a justification to demonstrate that the coping time to prevent the loss of the safety function that the equipment is intended to fulfil is long enough to connect and put into service the equipment under the conditions associated with the accident. The recommendations in this regard provided in Section 5 would be relevant. Non-permanent equipment that would be necessary to minimize the consequences of events that cannot be mitigated by the installed plant capabilities needs to be stored and protected to ensure its timely availability when necessary, with account taken of possible restricted access due to external events (e.g. flooding, damaged roads).

REFERENCES TO ANNEX II

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

[II–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-56, IAEA, Vienna (2020).

[II–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-53, IAEA, Vienna (2019).

[II–4] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34, IAEA, Vienna (2016).

[II–5] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

CONTRIBUTORS TO DRAFTING AND REVIEW