07-06-2022

IAEA SAFETY STANDARDS

for protecting people and the environment

Step 11:

Review by NUSSC Members

Review Committees: NUSSC (lead), NSGC

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

DS508

DRAFT SAFETY GUIDE

New Safety Guide

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1 The publication of IAEA Safety Standards Series No. SSR-2/1, Safety of Nuclear Power Plants: Design in 2012[1], and its subsequent revision in 2016 as 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 application of the concept of defence in depth as follows:

a) Including design extension conditions among the plant states to be considered in the design;
b) Ensuring by design that plant event sequences that could lead to an early radioactive release or a large radioactive release[2] have been 'practically eliminated'[3];
c) Including design features to enable the use of non-permanent equipment for power supply and cooling.

1.2 The incorporation of these aspects into designs of new nuclear power plants will affect the necessary safety assessment. IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment of Facilities and Activities [3] establishes requirements for performing the safety assessment for all types of facility and activity, including assessment of defence in depth. Specific requirements for safety assessment and safety analysis of nuclear power plants are established in SSR-2/1 (Rev. 1) [1].

OBJECTIVE

1.3 The objective of this Safety Guide is to provide recommendations for the design of new nuclear power plants on the application of selected requirements in SSR-2/1 (Rev. 1) [1] related to defence in depth and the practical elimination of plant event sequences that could lead to an early radioactive release or a large radioactive release. This Safety Guide also provides recommendations in relation to design aspects of defence in depth, in particular on those aspects associated with design extension conditions.

1.4 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 of nuclear power plants, and in the provision of technical support for nuclear power plants, as well as by regulatory bodies.

SCOPE

1.5 This Safety Guide applies primarily to new land based stationary nuclear power plants with water cooled reactors, designed for electricity generation or for other heat production

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

[2] 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 [1, 2].

[3] See definition of the practical elimination term in the definitions of this safety guide.

applications (such as district heating or desalination) (see para 1.6 of SSR-2/1 (Rev. 1) [1]). It is recognized that for reactors cooled by other media or reactors based on innovative design concepts, some of the recommendations in this Safety Guide might not be applicable or fully applicable, or judgement might be needed in their application.

1.6 For nuclear power plants designed in accordance with earlier standards, this Safety Guide might also be useful when evaluating potential safety enhancements of such designs, for example, as part of the periodic safety review of the plant.

1.7 The scope of this Safety Guide is focused on the implementation and assessment of the design safety measures described in para. 1.1. These measures play an important role in the application of the concept of defence in depth, which constitutes the primary means of both preventing and mitigating the consequences of accidents, in accordance with Principle 8 of IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [4].

1.8 As described in para. 2.13 of SSR-2/1 (Rev. 1) [1], defence in depth at nuclear power plants comprises five levels. Plant states considered in the design correspond to one or more levels of defence in depth. This Safety Guide is structured in terms of the design of safety provisions[4] necessary for each plant state, rather than for each level of defence in depth. In this way, the significance and importance of design extension conditions for the safety approach is emphasized.

1.9 This Safety Guide considers the assessment of the degree of independence between levels of defence in depth and, in a general manner, the assessment of independence of structures, systems and components implemented at different defence-in-depth levels. However, factors that could cause dependence between structures, systems and components, such as environmental factors, operational or human factors, and external or internal hazards, are not addressed in detail in this Safety Guide.

1.10 The Safety Guide does not provide specific recommendations for the design of particular safety features for design extension conditions or for any other plant state considered in the design. Such recommendations are provided in Safety Guides for the design of various types of plant system, such as IAEA Safety Standards Series Nos SSG-56, Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants [5], SSG-53, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants [6], SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [7], and SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [8].

1.11 This Safety Guide does not consider the specific safety analyses to be carried out for different plant states, as these are addressed in IAEA Safety Standards Series, SSG-2 (Rev. 1), Deterministic Safety Analysis for Nuclear Power Plants [9], SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [10], and SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear

[4] “Design safety provisions” is considered in this safety guide as the design solutions applied to structures, systems and components to ensure their required level of safety.

Power Plants [11], as appropriate. However, this Safety Guide takes into account the recommendations provided in these publications.

STRUCTURE

1.12 Section 2 sets out the requirements in SSR-2/1 (Rev. 1) [1] that govern the approach to design of nuclear power plants relating to prevention of radiological consequences, on which the recommendations in this Safety Guide are based. Section 3 provides recommendations on the implementation and assessment of design extension conditions within the concept of defence in depth, and on independence of the levels of defence in depth. Section 4 provides recommendations on the application of the concept of practical elimination of plant event sequences that could lead to an early radioactive release or a large radioactive release. Section 5 provides recommendations on the implementation of design provisions for enabling the use of non-permanent equipment for power supply and cooling.

1.13 Annex I provides examples of cases of practical elimination that may differ between the different Member States. Annex II provides some considerations for the application of recommendations included in this Safety Guide to nuclear power plants designed to earlier standards.

2. DESIGN APPROACH CONSIDERING THE RADIOLOGICAL CONSEQUENCES OF ACCIDENTS

2.1 This Safety Guide is focused on the design features in a nuclear power plant for the protection of the public and the environment in accident conditions, which should be assessed regarding compliance with a number of requirements in SSR-2/1 (Rev. 1) [1]. These requirements pertain to the general plant design and particularly on the capability of the plant to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures.

2.2 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.**"

2.3 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."

2.4 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."

2.5 Further requirements on criteria and objectives relating to radiological consequences of different plant states considered in the design, including accident conditions, are also established in 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 design extension conditions).
- "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 design extension conditions).

2.6 As indicated in para. 2.10 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."[5]

2.7 In accordance with para. 2.13 of SSR-2/1 (Rev. 1) [1]:

> "…The safety objective in the case of a severe accident is 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 is avoided or minimized".

2.8 Harmful radiological consequences to the public can arise only from the occurrence of uncontrolled accidents. Recommendations on radiation protection in the 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 [13], and recommendations for protection of the public and the environment are provided in IAEA Safety Standards Series No. GSG-8, Radiation Protection of the Public and the Environment [14].

[5] The establishment of off-site protective actions belongs to level 5 of defence 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 [12].

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

OVERALL IMPLEMENTATION OF DEFENCE IN DEPTH

3.1 The concept of defence in depth for the design of nuclear power plants is described in paras 2.12-2.14 of SSR-2/1 (Rev. 1) [1]. As stated in para. 2.14 of SSR-2/1(Rev. 1) [1]:

> “A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations. The number of barriers that will be necessary will depend upon the initial source term, considering the amount and isotopic composition of radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures.”

3.2 Requirement 7 of SSR-2/1 (Rev. 1) [1] on the application of defence in depth in the design of nuclear power plants states that:

> **“The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable”.**

3.3 Paragraphs 4.9 to 4.13A of SSR-2/1 (Rev. 1) [1] develop this overarching requirement. The specific focus of this Safety Guide is on the reactor core in the reactor pressure vessel and in the spent fuel pool, as the main source of radioactivity with special emphasis on design extension conditions.

3.4 For the safety provisions at each level of defence in depth, the following should be demonstrated:

(a) The performance of the safety provisions implemented at that level to maintain the integrity of the barrier(s);

(b) Adequate reliability of the safety provisions at that level so that it can be assured, with a sufficient level of confidence, that a certain plant condition can be brought under control without the need to implement safety provisions associated with the next level;

(c) The independence, as far as practicable, of the safety provisions at that level, including their physical separation[6], from the safety provisions associated with the previous levels of defence in depth.

3.5 Frequently, for purposes of design safety and operational safety, the various levels of defence in depth are associated with the various plant states considered in the design. The introduction of design extension conditions among the plant states has resulted in different interpretations in different States regarding the correspondence between the plant states

[6] Physical separation is separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof [2].

considered in the design and the levels of defence in depth. Two of these approaches are represented in Table 1. In Approach 1, depicted on the left hand side of Table 1, design extension conditions without significant fuel degradation are associated to level 3 of defence in depth. In this approach, each level has a clear objective that reflects the progression of an accident and the protection of the barriers, i.e. level 3 is implemented to prevent fuel damage and level 4 is implemented to mitigate severe accidents and prevent off-site contamination. Design extension conditions without significant fuel degradation could be understood as those representative event sequences involving either a single initiating event of very low frequency, or an anticipated operational occurrence or infrequent faults of design basis accident combined with multiple failures, which are considered in the design in order to prevent reactor core melt and melting of fuel stored in the spent fuel pool[7]. Therefore, in Approach 1, acceptable limits on predicted radiological consequences for design extension conditions without significant fuel degradation may be the same as or similar to acceptable limits for design basis accidents. Furthermore, the physical phenomena associated with design basis accidents and design extension conditions without significant fuel degradation are similar, although there might be differences in the analysis. In contrast, the physical phenomena associated with design extension conditions with core melt are completely different.

3.6 In Approach 2, depicted on the right hand side of Table 1, design extension conditions without significant fuel degradation and design extension conditions with core melt are grouped together in level 4 of defence in depth. This approach emphasizes the distinction between the set of rules to be applied for design extension conditions and the set of rules to be applied for design basis accidents, both in the design and in the safety assessment.

3.7 Despite their differences, both of these approaches are in compliance with para. 5.29 (a) of SSR-2/1(Rev. 1) [1] and support, the implementation, to the extent practicable, of independence between safety systems and those safety features for the prevention and/or mitigation of events considered in the design extension conditions.

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	Robust design and high quality in construction of normal operation systems, including monitoring and control systems	Operational limits and conditions 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 and/or emergency operating procedures	Level 2

[7] There is consensus that design extension conditions without significant fuel degradation are mainly identified as a result of Level 1 probabilistic safety assessment. Further details of the deterministic selection of event sequences considered in the design extension conditions without significant fuel degradation are provided in para. 3.40 of SSG-2 (Rev. 1) [9].

Level 3	3a	Control of design basis accidents	Safety systems	Emergency operating procedures		Level 3
	3b	Control of design extension conditions to prevent core melting	Safety features for design extension conditions without significant fuel degradation[8]	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 melting[9] Technical support centre	Severe accident management guidelines	4b	
Level 5		Mitigation of radiological consequences of significant releases of radioactive material	On-site and off-site emergency response facilities	On-site and off-site emergency plans and procedures		Level 5

Normal operation and anticipated operational occurrences

3.8 Operational states comprise two sets of plant states: normal operation and anticipated operational occurrences. Modes of normal operation include startup, power operation, shutting down, shutdown, maintenance, testing and refuelling and are defined in the documentation governing the operation of the plant (e.g. the operational limits and conditions[10]). Anticipated operational occurrences are reached either directly by the occurrence of a postulated initiating event or through a failure to prevent abnormal operation and failures.

3.9 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, to maintain the integrity of the first physical barrier for the confinement of radioactive material (i.e. the fuel cladding) and to prevent a significant release of primary coolant, design provisions for operational states should have adequate capabilities to:

(a) Prevent failures or deviations from normal operation by means of robust design and in compliance with proven engineering practices and high quality standards commensurate with the importance of these design provisions to safety;

(b) Detect and intercept deviations from normal operation and return the plant to a state of normal operation;

[8] Such safety features are understood as additional safety features for design extension conditions, or as safety systems with an extended capability to prevent severe accidents (see para. 5.27 of SSR-2/1 (Rev. 1)) [1].

[9] Such safety features are understood as additional safety features for design extension conditions, or as safety systems with an extended capability to mitigate the consequences of severe accidents (see para. 5.27 of SSR-2/1 (Rev. 1)) [1].

[10] In some States, the term 'technical specifications' is used instead of the term 'operational limits and conditions'.

(c) Prevent anticipated operational occurrences, once they start, from escalating into accidents conditions.

3.10 The reliability of safety provisions for anticipated operational occurrences should be such that the frequency of transition to a design basis accident is lower than the highest frequency of postulated initiating events for design basis accidents (usually lower than 10^{-2} per reactor-year) (see Table II–1 of SSG-2 (Rev.1) [9]).

Design basis accidents

3.11 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.**"

3.12 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"

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

> "The design shall be such that for design basis accident conditions, key plant parameters do not exceed the specified design limits. 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 (i.e. safety systems) should be implemented to prevent and mitigate the radiological consequences of design basis accidents by preventing significant fuel damage and maintaining the integrity of the containment (i.e. by preserving the structural integrity of the containment and maintaining its associated systems[11]). The objective of the safety systems is to limit the radiological consequences for the public and the environment to the extent that no off-site protective actions are necessary.

3.14 Accidents conditions are originated from postulated initiating events that are not expected to occur during the lifetime of the plant. The most frequent accidents conditions are categorized as design basis accidents and should have an expected frequency typically below 10^{-2} per reactor-year. Design basis accidents should include both, infrequent and limiting faults as single initiating events due to failure of the first and the second levels of defence in depth. The safety systems should be designed to mitigate all the set of postulated initiating events considered for design basis accidents as challenges to the fulfilment of the safety functions or challenges to the barriers. Safety systems designed to control design basis accidents requiring a prompt and

[11] The containment and its associated systems are described in para. 1.3 of SSG-53 [5].

reliable action should rely on automatic actuation and the need for short term operator actions should be minimized. Safety systems should be designed, constructed and maintained to ensure sufficient reliability. Safety design concepts, such as conservative safety margins and redundancy, should be applied in their design and construction. The environmental conditions considered in their qualification programme should correspond to the loads and adverse environmental conditions induced by design basis accidents, postulated internal and external hazards. Further recommendations on the design of specific safety systems for nuclear power plants are provided in the corresponding Safety Guides [5-8].

Design extension conditions

3.15 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.**"

3.16 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."

3.17 To meet the requirements presented in paras 3.15 and 3.16, two separate categories of design extension conditions should be identified[12]: design extension conditions without significant fuel degradation[13] and design extension conditions with core melting.[14]

Design extension conditions without significant fuel degradation

3.18 A process for the comprehensive identification of design extension conditions without significant fuel degradation should be developed. Paragraphs 3.39 to 3.44 of SSG-2 (Rev. 1) [9] provide recommendations for the identification of design extension conditions without significant fuel degradation.

3.19 In general, the control of design extension conditions without significant fuel degradation should be accomplished by safety features specifically designed and qualified for such

[12] The definition of design extension conditions is provided in SSR-2/1 (Rev.1) Definitions section.

[13] The term 'design extension conditions without significant fuel degradation' comprises situations to be analysed for the fuel in the reactor core and the fuel in the spent fuel pool.

[14] In some States, these categories of design extension conditions are denoted respectively as 'design extension conditions A' (without significant fuel degradation) and 'design extension conditions B' (with core melting).

conditions. Alternatively, design extension conditions without significant fuel degradation can be mitigated by available safety systems provided that these have not been affected by the events that led to the design extension conditions under consideration and that are capable and qualified to operate under the associated environmental conditions. A difference between design basis accidents and design extension conditions without significant fuel degradation is established based on their frequencies of occurrence (see Requirement 13 of SSR-2/1 (Rev.1) [1]). In some States very low frequency initiating events are treated as design extension conditions without significant fuel degradation. In other States, design extension conditions without significant fuel degradation are postulated for complex sequences involving multiple failures, whereas very low frequency postulated single initiating events are treated as design basis accidents.

3.20 The safety analyses of design basis accidents and design extension conditions without significant fuel degradation may share similar safety objectives, namely, to maintain the integrity of barriers and to prevent core damage or damage to the fuel in the spent fuel pool (see paras 7.28 and 7.45 of SSG-2 (Rev. 1) [9]).

3.21 Design basis accidents and design extension conditions without significant fuel degradation are also distinguished in terms of the application of different design requirements, and the use of different acceptable limits or criteria[15] or approaches for performing deterministic safety analysis. Thus, for design extension conditions without significant fuel degradation the following apply:

(a) Less stringent design requirements than for design basis accidents might be applied: for example, safety features for design extension conditions without significant fuel degradation may be assigned to a lower safety class than safety systems; the single failure criterion may be applied at the function level where appropriate (i.e. functional redundancy) but may not be applied at the system level (i.e. no redundancy among systems is applied). The equipment of the safety features and their supporting systems (e.g. cooling system) including I&C systems (e.g. the signal for anticipated transients without scram) are diversified as far as necessary from the design basis accidents safety system when some equipment of these systems may be affected by a common cause failure in the accident condition (e.g. the anticipated transients without scram, the station blackout);

(b) Less conservative assumptions than for design basis accidents, or best estimate methods, are acceptable for the safety analysis (see paras 7.35 to 7.44 and 7.47 to 7.55 of SSG-2 (Rev. 1) [9]);

(c) The requirements for the overall acceptable limits or criteria related to the radiological consequences for design extension conditions are presented in paras 5.31 and 5.31A of SSR-2/1 (Rev.1) [1]. Member States may choose to apply more restrictive acceptable limits or criteria for design extension conditions without significant fuel degradation. For example, some Member States choose to apply identical or similar acceptable limits or criteria for

[15] Acceptable limits related to radiological consequences used in SSR-2/1 (Rev.1) and acceptance criteria related to radiological consequences used in SSG-2 (Rev.1) are equivalent terms.

radiological consequences to those for design basis accidents (see paras 7.32 to 7.33 and 7.46 of SSG-2 (Rev. 1) [9]).

3.22 If it is possible to use available safety systems to respond to design extension conditions without significant fuel degradation, safety analysis is still required to demonstrate their effectiveness: see Requirement 42 of SSR-2/1 (Rev. 1) [1]. The deterministic safety analysis may use less conservative methods and assumptions than for design basis accidents (see 3.21). Nevertheless, there should still be adequate confidence in the results of the safety analysis and the safety margins to avoid cliff edge effects should be demonstrated to be adequate (see paras 7.45 and 7.54 to 7.55 of SSG-2 (Rev. 1) [9]).

3.23 Design basis accidents are required to be analysed in a conservative manner: see para. 5.29 of SSR-2/1 (Rev. 1) [1]. However, design extension conditions without significant fuel degradation have the potential to exceed the established capabilities of safety systems. Therefore, it might be possible to show that some safety systems, with an extended capability in their design, would be capable of, and be qualified for, mitigating the design extension conditions without significant fuel degradation, based on best estimate analyses and on less conservative assumptions than the assumptions used for design basis accidents.

3.24 As for design basis accidents, for design extension conditions without significant fuel degradation, radioactive releases should be minimized as far as reasonably achievable.

3.25 Anticipated operational occurrences and design basis accidents combined with failures in safety systems should be considered as part of the list of design extension conditions without significant fuel degradation; see para. 3.40 of SSG-2 (Rev. 1) [9]. In many plant designs, such conditions include anticipated transient without scram and station blackout (see para 5.8 of SSG-34 [7] for definition of station blackout).

3.26 On the basis of engineering judgement and of deterministic and probabilistic safety assessments, design extension conditions without significant fuel degradation should also be considered to identify safety provisions to be implemented to prevent and reduce the frequency of severe accidents caused by failures of safety systems. Such safety provisions should include, if possible, additional, diverse measures to cope with common cause failures of safety systems.

3.27 Consideration of design extension conditions without significant fuel degradation reinforces the robustness of the design to cope with some complex and unlikely failure sequences and balances the overall risk profile of the plant. Therefore, the reliability of safety systems and safety features for design extension conditions without significant fuel degradation should be sufficiently high to prevent a severe accident by making the escalation to a severe accident very unlikely to occur.

Design extension conditions with core melting

3.28 In accordance with para. 5.9 of SSR-2/1 (Rev. 1) [1], and with consideration of results from research and development, a set of representative accident conditions with core melting should be postulated to provide inputs for the design of the containment and of the safety features ensuring its functionality. This set of representative accident conditions should be considered in the design of safety features for design extension conditions with core melting and should represent bounding cases that envelop other severe accidents with more limited degradation of the core.

3.29 Paragraph 6.68 of SSR-2/1 (Rev. 1) [1] states [footnote omitted]:

> "For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated' and so as to avoid high radiation fields on the site."

Hence, significant fuel degradation in the spent fuel pool should not be postulated as part of this set of design extension conditions; rather it is required to be considered among the conditions to be practically eliminated (see Section 4).

3.30 The accident conditions chosen as design extension conditions with core melting should be justified on the basis of engineering judgement and insights from probabilistic safety analyses: see SSG-53 [6] and SSG-2 (Rev. 1) [9]. A detailed analysis should be performed and documented to identify and characterize accident conditions that could lead to core damage and also challenge or bypass the containment. Relevant accident conditions that could lead to core damage should be postulated as design extension conditions (see para 3.46 and 3.47 of SSG-2 (Rev.1) [9] and para 2.11 of SSG-53 [6]), even though the design provisions taken in accordance with the requirements of SSR-2/1 (Rev. 1) [1] to prevent such accidents will 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 safety features for design extension conditions with core melting: see para. 3.42 of SSG-53 [6].

3.31 The capability and the reliability of the safety features for design extension conditions with core melting should be evaluated to ensure that they are adequate for the safety function that they need to fulfil.

3.32 The challenges to plant safety presented by design extension conditions with core melting, and the extent to which the design may be reasonably expected to mitigate their consequences, should be considered in establishing accident management procedures and guidelines. Recommendations in this regard are provided in IAEA Safety Standards Series No. SSG-54, Accident Management Programmes for Nuclear Power Plants [15]

3.33 The source term inside the containment in a severe accident conditions is such that the radioactive releases from any direct leakage to the environment have to be avoided or minimised. If the reactor containment integrity is intact, the direct radioactive releases are a consequence of the reactor containment leak rate, depending on the reactor containment pressure. Specific measures may be considered. Firstly, the potential for direct radioactive releases from leakages should be minimised by providing a reactor containment leak rate safety limit, as stated in para 4.100 of SSG-53 [6]:

> "At the design stage, a target leak rate should be set that is well below the safety limit leak rate (i.e. well below the leak rate assumed in the assessment of possible radioactive releases arising from accident conditions)".

Moreover, additional potential paths of leakage of radioactive releases (e.g. containment penetrations) may be identified and measures need to be taken to avoid and reduce the impact of those radioactive releases to the environment (e.g. collect and filter such leakages). Secondly as the actual reactor containment leak rate increases by a higher reactor containment pressure[16], this pressure should be controlled. This may be achieved by ensuring and maintaining adequate cooling of the reactor containment atmosphere during the severe accident or by a filtered reactor containment venting system allowing to reduce the radioactive releases. Therefore, unfiltered direct radioactive releases from the reactor containment in a severe accident should remain below the reactor containment leak rate safety limit to allow sufficient time for implementation of off-site protective actions. Beyond this time, releases might exceed the reactor containment leak rate safety limit but should still be well below the acceptable limits for design extension conditions requiring the implementation of off-site protective actions in place. Those radioactive releases should also be well below what is considered as a large radioactive release.

3.34 As stated in paras 3.44 and 3.45 of SSG-53 [6]:

> "Multiple means to control the pressure build-up in accident conditions inside the containment should be implemented and venting (if any [is included in the design] should be used only as a last resort… the use of the venting system should not lead to an early radioactive release or a large radioactive release".

3.35 A safety assessment of the design should be performed with consideration of the progression of severe accident phenomena and their consequences, and the achievement of acceptable end state conditions and should take into account applicable topical issues. More detailed information on the range of physical processes that could occur following core damage is provided in para. 7.66 of SSG-2 (Rev. 1) [9].

ASSESSMENT OF THE IMPLEMENTATION OF DEFENCE IN DEPTH

3.36 The implementation of defence in depth in the design of a nuclear power plant is required to be assessed to ensure that the safety provisions for each level are adequately designed to meet the objectives of that level in terms of prevention, detection, limitation and mitigation. Requirement 13 of GSR Part 4 (Rev. 1) [3] 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.**"

3.37 Paragraphs 4.45–4.48A of GSR Part 4 (Rev. 1) [3] establish additional requirements on assessment of defence in depth.

[16] At some point the pressure inside of the reactor containment may be so high that the reactor containment may start to fail. This is a cliff edge effect to be avoided.

3.38 The performance and reliability of safety provisions for all plant states should be assessed, taking into consideration an applicable set of analysis rules, the level of risk and the safety significance of the safety provisions. The 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 associated with each level of defence in depth is adequate. The assessment should demonstrate that, for each credible initiating event, the risk has been reduced to a level that is as low as reasonably achievable, considering also all consequences of internal hazards and external hazards that could cause the event. The assessment should consider insights from the assessment of engineering aspects and from deterministic safety analysis and probabilistic safety assessment, as appropriate for each different plant state.

3.39 The multiplicity of the levels of defence is not a justification to weaken the effectiveness of some levels by relying on the effectiveness of other levels. In a sound and balanced design, structures, systems and components at each level of defence are characterized by a reliability commensurate with their function and their safety significance, and reasonable safety margins are provided.

3.40 The defence in depth concept should be applied for all sources of radiation present in the nuclear power plant. The following are examples of sources of radiation likely to be present in a nuclear power plant:

- The reactor core;
- Fresh nuclear fuel, irradiated fuel and fuel casks;
- Neutron sources and other radioactive sources;
- Airborne radioactive material in buildings;
- Piping and process equipment containing radioactive material (e.g. the reactor coolant system, reactor cooling systems, auxiliary systems, heating, ventilation and air conditions systems of controlled areas, gas and liquid effluent treatment systems, solid waste treatment systems).

3.41 For sources of radiation other than the reactor core and the nuclear fuel, defence in depth should be implemented in accordance with a graded approach, with account taken of the fact that some levels of defence in depth may not be appropriate for many sources of radiation within the plant. Account should be taken of the risk represented by the amount and type of radioactive material present; the potential for its dispersion owing to its physical and chemical nature; and the possibility of nuclear, chemical or thermal reactions that could occur under normal or abnormal conditions and the kinetics of such reactions. These characteristics will differ for different sources of radiation and will influence the necessary number of levels of defence in depth and the strength of each level.

3.42 The physical barriers included in the design are an important consideration when assessing the adequacy of the implementation of defence in depth. For each identified source of radiation, the physical barriers (including for the reactor core, the reactor coolant pressure boundary and the containment boundary) should be identified and their robustness should be evaluated in accordance with a graded approach. The following aspects should be assessed in the evaluation:

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

(b) Appropriate codes and standards should be used for the design and manufacture or construction of barriers, and proven materials and technologies should be used in the manufacture or construction.

(c) All loads and combinations 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 and calculated and should be shown to be less than the applicable limits.

(d) The number of barriers provided in the design should be justified and the barriers chosen for each plant state should offer the best protection for workers and the public that may be reasonably expected.

(e) Valves, their control equipment and other equipment used in the barriers to prevent radioactive releases should be designed to ensure structural integrity of the barriers in accident conditions.

(f) Any deviation of a barrier from its normal configuration (e.g. 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.

3.43 An analysis of the various mechanisms that could challenge or degrade 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 of such mechanisms or to stop their progression. To the extent that different degradation mechanisms could necessitate different safety provisions, the adequacy and effectiveness of each safety provision should be assessed for each degradation mechanism.

3.44 The adequacy and effectiveness of safety provisions should be assessed by performing deterministic safety analyses modelling the plant response to a given initiating event for different boundary conditions representative of each plant state. Each plant state should be characterized by a type of safety analysis, with an applicable set of analysis rules, level of conservatism and acceptance criteria. Recommendations on conducting deterministic safety analyses for the different plant states are provided in SSG-2 (Rev. 1) [9].

3.45 The performance of safety provisions at each level of defence in depth is assessed through assessment of engineering aspects and deterministic analysis involving the use of validated and verified computer codes and models to demonstrate that acceptance criteria are met and that there are sufficient margins to avoid cliff edge effects. Further recommendations are provided in paras 5.14-5.39 of SSG-2 (Rev. 1) [9].

3.46 The reliability analysis of safety provisions for the different plant states, as indicated in para. 3.39, typically uses probabilistic techniques and takes into account the plant layout and either protective provisions against or qualification for the effects of hazards, and potential commonalities in the design, manufacture, maintenance and testing of redundant and diverse equipment.

3.47 Statements of reliability should be supported by equipment reliability data that is shown to be relevant to the structure, system or component being assessed, as well as supported by test data, the use of proven technologies and engineering practices, and feedback from operating experience. Statements of reliability should also be supported by verification of compliance of the structure, system or component with the applicable set of design requirements. Reliability analyses for different systems or levels of defence in depth can be integrated into a probabilistic safety assessment to evaluate overall plant risk metrics, such as core damage frequency or frequencies of early radioactive releases or large radioactive releases.

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

3.49 The reliability of structures, systems and components for controlling anticipated operational occurrences should be such that they are capable of reducing the number of challenges to safety systems and of contributing to preventing the occurrence of accident conditions.

3.50 The reliability of safety systems should be such that the collective contribution to the core damage frequency of failing to control design basis accidents does not exceed any safety goals of the plant where set (e.g. for new nuclear power plants typically below 10-5 per reactor-year). Design extension conditions without significant fuel degradation should be postulated for specific low frequency event sequences as appropriate to achieve the safety goals.

3.51 Any vulnerabilities that could result in the complete failure of a safety system should be identified and it should be assessed whether such a failure, in combination with a postulated initiating event, could escalate to a core melt accident. For each such combination analysed, if the consequences exceed those acceptable for design basis accidents and might cause a core melt with unacceptable frequency, separate, independent and diverse safety features, which are unlikely to fail by the same common cause, should be implemented (e.g. an alternate AC power supply in case of a total loss of the emergency power supply, or a separate and diverse decay heat removal chain).

3.52 The reliability of safety features for design extension conditions without significant fuel degradation should be such that it can be demonstrated, with a sufficient level of confidence and considering applicable analysis rules (see paras 7.45-7.55 of SSG-2 (Rev. 1) [9]), that the core damage frequency is lower than the established probabilistic targets.

3.53 The capability and reliability of safety features for design extension conditions with core melting should be sufficient to ensure that the integrity of the containment will not be jeopardized during any postulated core melt sequence. However, since the analysis of core melt and its impact on the integrity of the containment is associated with considerable uncertainties, the reliability claimed for such safety features should be considered with caution.

3.54 It should be demonstrated that the reliability of safety systems and safety features for design extension conditions has taken into account the reliability of their supporting systems.

INDEPENDENCE BETWEEN LEVELS OF DEFENCE IN DEPTH

3.55 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."

3.56 Some additional requirements in SSR-2/1 (Rev. 1) [1] contribute to ensuring the independence of the levels of defence in depth. For example, the sharing of structures, systems or components for executing functions in different plant states is one factor that could compromise the independence of the levels of defence in depth. Requirement 21 of SSR-2/1 (Rev. 1) [1] 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.**"

For protection systems and control systems, in particular, Requirement 64 of SSR-2/1 (Rev. 1) states:

> **"Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence."**

Regarding supporting systems and auxiliary systems, 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.**"

3.57 The potential for common cause failures is a second factor that can compromise the independence of the levels of defence in depth. Typical root causes of common cause failures are undetected human errors in design or manufacturing, human errors in the operation or maintenance, inadequate equipment qualification or inadequate protection against internal or external hazards. 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.**”

3.58 Because of these factors, full independence of the levels of defence in depth may be difficult to achieved. The design of a nuclear power plant should consider all potential causes of dependencies and an approach should be implemented to remove them to the extent reasonably practicable. Robust independence should be implemented among systems whose simultaneous failure would result in conditions having harmful effects for people or the environment.

3.59 As far as practicable, the sharing of safety systems or parts of them for executing safety related functions for different plant states should be avoided. However, since this might not be always practical or possible, it should be ensured that within the event sequence that might follow a postulated initiating event, a safety system credited to respond in a given plant state will not have been needed for a preceding plant state. As emphasized in para. 4.13A of SSR/2-1 (Rev. 1) [1]:

> “… 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.”

Therefore, in some reactor designs it is a common practice to allow the use of some safety systems for certain anticipated operational occurrences. For example, the intervention of the reactor protection system might be necessary to shutdown the reactor for some anticipated operational occurrences that cannot be controlled by the limitation system. For most reactor designs, the reactor trip system is a safety system that is also needed for the control of some anticipated operational occurrences.

3.60 The systems needed for different plant states should be functionally isolated from one another in such a way that a malfunction or failure in a system in a given plant state does not propagate affecting another system required in the following plant state. However, practical limitations of the reactor design may in certain situations necessitate exemptions to such functional isolation, although each case should be justified.

3.61 The systems intended for mitigating severe accidents should be functionally and physically separated from the systems intended for other plant states to the extent practicable. However, safety features for design extension conditions with core melting may, for good reasons, also be used for preventing severe core damage if it can be demonstrated that such use will not undermine the ability of these safety features to perform their primary function if conditions do evolve into a severe accident. As an example, a power supply intended for design extension conditions with core melting could be used, if necessary, to power equipment for design extension conditions without significant fuel degradation.

ASSESSMENT OF THE INDEPENDENCE OF THE LEVELS OF DEFENCE IN DEPTH

3.62 Engineering assessment, deterministic and probabilistic methods should be used to assess the independence of the levels of defence in depth. The structures, systems and components needed for each postulated initiating event should be identified, and it should be shown by means of engineering analyses that the structures, systems and components needed for implementing each level of defence in depth are sufficiently independent from those for the other levels. A postulating initiating event is generally a bounding event covering different kinds of initiating failure and so it might be difficult to list all equipment for normal operation that might initially be affected by the postulated initiating event for particular design extension conditions. For this reason, the crediting of systems for normal operation in the safety assessment of design extension conditions should be considered with extreme caution and should be adequately justified. The adequacy of the independence that is achieved for each level of defence in depth should also be assessed by probabilistic analyses.

3.63 The assessment 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 if an accident occurs. The assessment of the independence of the levels of defence in depth should aim to verify that the vulnerabilities for common cause failures between structures, systems and components that are claimed to be independent, have been identified and removed to the extent practicable. Such common cause failure might have originated in the layout, design, manufacture, operation or maintenance. If a functional dependency between structures, systems and components has not been removed, this must be justified in the assessment.

3.64 The assessment should demonstrate that safety systems that are intended to respond first in an accident 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. Following an initiating event, the failures occurring in anticipated operational occurrences should not compromise the capability of safety systems to manage a design basis accident.

3.65 The assessment should demonstrate that a failure of a supporting system is not capable of simultaneously affecting parts of systems for different plant states in a way that the capability to fulfil a safety function is compromised. For this purpose, the assessment should provide evidence that the reliability, redundancy, diversity and independence of supporting systems is commensurate with the significance to safety of the system being supported.

3.66 An assessment should be conducted of the independence of structures, systems and components that might be necessary at different levels of defence in depth to mitigate the consequences of a single hazard or a likely combination of internal or external hazards on the plant. It should be demonstrated that the postulated initiating event and the failures induced in the plant cannot result in common cause failure of the structures, systems and components necessary for mitigation consequence of of the hazard at different levels of defence in depth. In particular, a common cause failure should not affect at the same time the safety functions performed by the safety systems or some safety features for DEC without significant fuel degradation and the safety functions of the necessary safety features for design extension conditions for core melting.

4. PRACTICAL ELIMINATION OF PLANT EVENT SEQUENCES THAT COULD LEAD TO AN EARLY RADIOACTIVE RELEASE OR A LARGE RADIOACTIVE RELEASE

4.1 Paragraph 2.11 of SSR-2/1 (Rev. 1) [1] states [footnote omitted]:

> "Plant event sequences that could result in high radiation doses or in a large radioactive release have to be 'practically eliminated'… An essential objective is that the necessity for off-site protective actions to mitigate radiological consequences be limited or even eliminated in technical terms, although such measures might still be required by the responsible authorities".

4.2 In relation to the fourth level of defence in depth, para. 2.13 of SSR-2/1 (Rev. 1) [1] states [footnotes omitted]:

> "Event sequences that would lead to an early radioactive release or a large radioactive release are required to be 'practically eliminated'."

This requirement is repeated in SSR-2/1 para 5.31.

4.3 Although the term 'early radioactive release' is predominantly used in SSR-2/1 (Rev. 1) [1], the term 'high radiation doses' appears in para. 2.11 and Requirement 5 of SSR-2/1 (Rev. 1) [1]. It should be interpreted to mean such doses as would occur as a result of an early radioactive release, because protective actions could not be effectively implemented in time to prevent them.

4.4 The concept of practical elimination should be applied only to those events or sequences of events that could lead to or involve significant fuel degradation, i.e. a severe accident, for which the confinement of radioactive material cannot be reasonably achieved. The practical elimination of such plant event sequences is required to be ensured by design [1], either ensuring that the plant event sequence is physically impossible (see paras 4.34–4.35) or because the plant event sequence is considered, with a high level of confidence, to be extremely unlikely to arise (see paras 4.36–4.43).

4.5 The concept of practical elimination should be applied as part of the overall safety approach to the design of nuclear power plants, as set out in section 2 of SSR-2/1 (Rev. 1) [1]. As a result of the implementation of the first, second, third and fourth levels of defence in depth, the likelihood of an off-site radioactive release that could potentially result from an accident will be very low. However, it is necessary to verify that there would not be credible plant conditions that could not be effectively mitigated and which could thus lead to unacceptable radiological consequences. This is where the aim of the practical elimination concept lies: to reinforce the implementation of defence in depth at a plant by a focused analysis of those conditions having the potential for unacceptable radiological consequences.

4.6 Practical elimination should not be seen as an alternative to mitigation of the consequences of a severe accident (i.e. implementation of the fourth and fifth levels of defence in depth); rather, the application of practical elimination may lead to the identification of additional provisions which will complement defence in depth in the design. Moreover, the practical elimination of plant event sequences that could lead to an early radioactive release or a large radioactive release does not remove the need for emergency preparedness and response, in accordance with principle 9 of SF-1 [3] and the requirements of GSR Part 7 [12].

4.7 Therefore, as mentioned in para. 4.4, the concept of practical elimination should be applied only in relation to plant event sequences that could lead to an early radioactive release or a large radioactive release, for which reasonably practicable technical means for their mitigation cannot be implemented. Otherwise, the technical means should be considered in the design for the mitigation of the accident consequences at the plant, but this would not constitute the application of the concept of practical elimination.

4.8 SSR-2/1 (Rev. 1) [1] does not provide quantitative acceptance limits or criteria for the radiological consequences of accident conditions, nor for the magnitude of what is to be considered an early radioactive release or a large radioactive release. Independent of the design or specific definitions of the phrases, early radioactive releases or large radioactive releases are those which could challenge defence in depth Level 5 provisions. In some States an early radioactive release is defined for a specific site considering restrictions on implementing off-site protective actions in a timely manner. In some States, acceptable limits on radioactive releases for purposes of radiation protection, and probabilistic criteria or target values for the purpose of demonstrating a low frequency of a core damage accident, have been established, consistent with regulatory requirements or objectives. However, the justification that a plant event sequence has been practically eliminated should rely primarily on a deterministic evaluation of the robustness and independence of design safety provisions and should not solely relied on the compliance with such probabilistic criteria, but supported by the results of probabilistic safety assessments.

4.9 The concept of practical elimination should be applied in a new nuclear power plant from an early stage, when it is more practicable to design and implement additional[17] safety features. The incorporation of such features should be an iterative process, which should use insights from engineering experience, and from deterministic safety analyses and probabilistic safety assessment in a complementary manner.

IDENTIFICATION OF RELEVANT PLANT EVENT SEQUENCES

4.10 The first step in demonstrating the practical elimination of event sequences that could lead to an early radioactive release or a large radioactive release is the identification of such plant event sequences. This identification process is expected to result in a list of plant event sequences, which can be grouped into a smaller set of plant conditions among the severe accidents identified for the plant. The identification process should be justified and supported by relevant information.

[17] Such additional safety features include any design provision that is implemented following an assessment supporting the demonstration of practical elimination of some plant event sequences. Some design provisions will already have been implemented to support other safety objectives and analyses and can also support the demonstration of practical elimination.

4.11 In a severe accident, large quantities of radioactive substances are likely to be present and not confined in the fuel or by the reactor coolant system. In addition, severe accident phenomena can generate large amounts of energy very rapidly. Together, this can make it impossible to ensure the confinement of radioactive material, thus giving rise to unacceptable radiological consequences.

4.12 If a severe accident occurs, it is necessary to ensure that radioactive material released from the nuclear fuel will be confined. In particular, 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 where there is a containment bypass that cannot be isolated, the only way to prevent unacceptable radiological consequences is to prevent the occurrence of such severe accidents. In such cases, it may be necessary to demonstrate practical elimination by proving the physical impossibility of the accident or by proving with a high degree of confidence that such severe accidents would be extremely unlikely. Therefore, the issue when considering whether a particular plant event sequence should be practically eliminated is the potential for the event sequence to lead to a radioactive release greater than the maximum radioactive release allowed in accordance with para 5.31A of SSR-2/1 (Rev.1) [1].

4.13 To help ensure that the demonstration of practical elimination is manageable, the whole set of individual plant event sequences that might lead to an unacceptable radiological consequence should be grouped to form a limited number of bounding cases or types of accident conditions. As an example (see 4.15), the following five general types of plant event sequences should be considered, depending on their applicability for specific designs:

(a) Plant events sequences 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) Uncontrolled reactivity accidents.

(b) Plant event 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) Plant event sequences that could lead to late containment failure, such as:
    (i) Basemat penetration or other damage to the containment integrity during molten corium concrete interaction;
    (ii) Long term loss of containment heat removal (e.g., failure of containment heat removal system);
    (iii) Loss of containment cooling against overtemperature (e.g., failure of containment spray system)
    (iv) Explosion of combustible gases, including hydrogen and carbon monoxide.

(d) Plant event sequences with containment bypass, such as:

(i) A loss of coolant accident with the potential to drive the leakage outside of the containment via supporting systems (i.e. a loss of coolant accident in an interface system)[18];
(ii) Plant event sequences producing a consequential containment bypass (e.g. an induced steam generator tube rupture);
(iii) A plant event sequence with core melt and in which the containment is open[19] (e.g. in the shutdown state).

(e) Significant fuel degradation in a spent fuel pool[20].

4.14 The grouping in para. 4.13 is consistent with the recommendations provided in SSG-53 [6] (see para 3.67) and SSG-2 (Rev. 1) [9] (see para 3.56), and highlights some examples of plant event sequences (e.g. severe accident conditions) for consideration for practical elimination.

4.15 Other criteria for grouping are also possible. To facilitate the grouping proposed, each type of plant event 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 to a radioactive release greater than the maximum radioactive release allowed in accordance with para 5.31A of SSR-2/1 (Rev.1) [1].

4.16 The identification and grouping described in paras 4.13 and 4.15 should combine, when relevant, the following approaches:

(a) A phenomenological (top-down) approach, in which phenomena are considered that might challenge the confinement function before or in the course of a severe accident, in order to define a comprehensive list of plant event sequences, i.e. as listed in para. 4.13;
(b) A sequence-oriented (bottom-up) approach, in which all plant event sequences that could lead to a severe accident are reviewed. For each sequence, any challenge to the confinement function is assessed (this might involve evaluation of the loads on the containment and of possible release routes via leakages and bypasses). The sequence-oriented approach supplements the phenomenological approach with broader screening to identify all relevant plant event sequences.

[18] 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’

[19] In many LWR designs, the technology used for equipment hatches might not be fast enough to ensure re-closure and restoration of the containment integrity before a radioactive release occurs.

[20] Several plant designs 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 involved enable the implementation of on-site or off-site prevention or protective measures. However, this does mean that any occurrence of significant fuel degradation in the spent fuel pool would directly lead to a large radioactive release. Therefore, any plant event sequence with significant degradation of the fuel assemblies stored in the spent fuel pool located outside of the containment has to be considered for practical elimination. If the spent pool is located inside the containment (as in WWER designs) the degradation of the spent fuel does not result in an early radioactive release or large radioactive release. Thus, for those particular designs, the plant event sequence with significant degradation of the fuel assemblies stored in the spent fuel pool might not be needed to be considered for practical elimination.

4.17 All possible normal operating modes of the plant (e.g. start-up, power operation, shutdown, refuelling, maintenance) should be considered in the process of identifying relevant event sequences, including operating modes with an open containment.

4.18 All plant locations and buildings where nuclear fuel is stored should be considered in the process of identifying relevant plant event sequences, including the spent fuel pool.

IDENTIFICATION AND ASSESSMENT OF SAFETY PROVISIONS FOR DEMONSTRATING PRACTICAL ELIMINATION

4.19 The assessment aimed at identifying safety provisions in the form of design and operational features that could be implemented for demonstrating the practical elimination of each relevant plant event sequence should considered the following aspects:

(a) The state of the art in nuclear science and technology, as appropriate;
(b) Experience from the operation of nuclear power plants and from accidents;
(c) Proven technical and industrial feasibility of safety provisions;
(d) The capability of safety provisions to provide sufficient margins for dealing with uncertainties and to avoid cliff edge effects;
(e) Potential drawbacks of safety provisions, which might only become evident after the plant is put into operation (e.g. operational constraints or spurious actuations);
(f) The kinetics of the severe accident phenomena that might threaten the containment integrity or its leaktightness;
(g) Avoiding the need to conduct on-site actions or use off-site personnel or equipment.

4.20 The identification of safety provisions necessitates a comprehensive analysis of the physical phenomena involved, from the deterministic, probabilistic and engineering judgement perspectives, and it might be necessary to further refine the identification of event sequences performed in accordance with the approaches described in para. 4.16.

4.21 The designer should establish a decision making process for determining reasonably practicable safety provisions to achieve practical elimination. Several options for safety provisions should be considered and the rational for selecting the final design of safety provisions should be documented.

4.22 The safety provisions identified to demonstrate the practical elimination of relevant plant event sequences should be associated, on a case by case basis, to the appropriate level of defence in depth or plant state at which the event sequence would need to be interrupted to prevent unacceptable radiological consequences. It should be verified that the appropriate engineering design rules (e.g., fail safe actuation and protection against common cause failures induced by internal and external hazards) and technical requirements for the safety provisions in that level of defence in depth or plant state have been followed. The aim of this verification is to ensure that the safety provisions would achieve their safety function with sufficient margins to account for uncertainties, under the prevailing conditions (e.g., the harsh environmental conditions associated with a severe accident). In applying the engineering design rules and technical requirements, where relevant, appropriate testing should be applied, operational procedures should be followed, and, in operation, surveillance as well as in-service testing and inspection should be conducted. The engineering design rules and technical requirements should be applied at all steps in the development of the safety provisions, from design to operation, including their manufacture, construction or implementation at the plant, and their commissioning and periodic testing.

4.23 Safety provisions for demonstrating practical elimination of some severe accident conditions could include the need of operational provisions as well as design provisions, and as such they could involve the performance of operator actions (e.g. the opening of primary circuit depressurization valves to prevent high-pressure core melt conditions). Requiring operator actions should be minimized and, when unavoidable, a human factor assessment should be part of the justification supporting any claim for high reliability of operator actions. The human factor assessment should address the following:

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

(b) The environment for performing the action (e.g. access to the local area, components to be handled, identification of the location of components, ambient conditions). If local actions are expected to be taken in harsh environmental conditions, this is likely to reduce the reliability for demonstration of practical elimination.

(c) The timescales for performing the actions, including sufficient margin to achieve the expected outcomes.

4.24 Some safety provisions claimed to contribute towards the practical elimination of some plant event sequences could be vulnerable to human errors that might have occurred prior to the onset of the accident. Such human errors could introduce latent risks that might prevent successful operation of a system or component when it is called upon during an event or accident. In such cases, the system or component used to perform the action should be subject to relevant operational provisions (e.g. periodic testing, in-service inspection and surveillance, qualification tests following maintenance and periodic system alignment checks) to limit the risk from human errors of this type.

4.25 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.”

Therefore, certain safety provisions for demonstrating practical elimination should be designed to withstand relevant internal and external hazards (i.e. hazards that consequential to the accident condition or likely to arise concurrently), with appropriate margin.

4.26 Where safety provisions for demonstrating practical elimination rely on support functions, the relevant supporting systems should all be designed to the standards necessary to ensure that they have same level of overall reliability as the safety provisions. The design should use a combination of safety design principles such as redundancy, separation, diversity, and robustness to hazards to achieve the required reliability of the relevant safety function. Alternatively, the safety provisions should be tolerant to the loss of support functions.

DEMONSTRATION OF PRACTICAL ELIMINATION

4.27 The overall effectiveness of the safety provisions identified by the designer to demonstrate practical elimination should be proven through a safety assessment that includes engineering judgement, deterministic analyses and probabilistic assessments. The demonstration of practical elimination should be conducted as part of the design and safety assessment process for the plant, including the necessary inspection and surveillance processes during manufacture, construction, commissioning and operation.

4.28 All safety provisions developed to prevent the plant event sequences in each of the groups in para. 4.13 from occurring should be analysed. None of the phenomena or accident conditions indicated should be overlooked because of their low likelihood of occurrence. Credible research results should be employed to support claims of effectiveness of the safety provisions.

4.29 For each group of plant event sequences considered for practical elimination, an assessment should be performed to demonstrate the effectiveness of the associated safety provisions. Either it should be demonstrated that it is physically impossible for the event sequence to arise (see paras 4.33 and 4.34) or it should be demonstrated, with a high level of confidence, that the event sequence is extremely unlikely to arise (see paras 4.35 to 4.42). The justification of practical elimination of an event sequence should preferably rely on a demonstration of the physical impossibility of its occurrence. If this is not achievable, it should be demonstrated, with a high level of confidence, that it is its extremely unlikely to occur.

4.30 As evident from para. 4.13, the various plant event sequences to be considered for practical elimination are inherently rather different. As a consequence, their practical elimination should be demonstrated on a case by case basis.

4.31 Uncertainties due to limited knowledge of some physical phenomena, in particular severe accident phenomena, should be considered when conducting engineering analyses as well as deterministic safety analyses and probabilistic safety assessment, so that a high level of confidence in the result can be assured.

4.32 Computer codes and calculations used to support the demonstration of practical elimination should be verified and validated and models used should reflect best understanding of the physical phenomena involved so as to provide acceptable prediction of the plant event sequences and the phenomena involved. Section 5 of SSG-2 (Rev. 1) [9] provides recommendations on the use of computer codes for deterministic safety analyses.

Practical elimination of plant event sequences because they would be physically impossible

4.33 Where a claim is made that a plant event sequence can be practically eliminated because it is physically impossible, it should be demonstrated that the inherent safety characteristics of the system or reactor type are such that the plant event sequence cannot, by the laws of nature, occur and that the fundamental safety functions (see Requirement 4 of SSR-2/1 (Rev. 1) [1]) will always be fulfilled.

4.34 In practice, the demonstration of physical impossibility is limited to very specific cases. Demonstration of physical impossibility cannot rely on measures that involve active components or operator actions. An example is the practical elimination of the prompt reactivity accident from the effect of heterogeneous boron dilution. By design, the accident could be considered as eliminated by demonstrating that only a limited volume of non-borated water could be injected, which does not allow that effect to happen. The accident could be also considered as eliminated by demonstrating that sufficient negative reactivity coefficient exists for possible combinations of the reactor power and coolant pressure and temperature, for the core cycle. In this case, a prompt reactivity insertion accident could be considered physically impossible. Another example is the practical elimination of containment failure from post-accident combustible gas (e.g., hydrogen) detonation. By design, excessive containment loads from the effects of gas detonation in the containment building could be considered as eliminated by justifying that a limited amount of material that could generate combustible gas during a severe accident exists. Then, the use of bounding analyses of the maximum gas generated justifying that combustible gas concentration is below the detonation limit could demonstrate physical impossibility.

Practical elimination of plant event sequences considered, with a high level of confidence, to be extremely unlikely to arise

4.35 The demonstration that certain plant sequences are extremely unlikely to occur should rely on the assessment of engineering aspects, deterministic considerations, supported by probabilistic considerations to the extent practicable, taking into account the uncertainties due to the limited knowledge of some physical phenomena. Although probabilistic targets can be set (e.g. frequencies of core damage or of radioactive releases), the demonstration of practical elimination cannot be approached only by probabilistic means. Probabilistic insights should be used in support of deterministic and engineering analyses. Meeting a probabilistic target alone is not a justification to exclude further deterministic and engineering analyses and possible implementation of additional reasonable safety provisions to reduce the risk. Thus, the low probability of occurrence of an accident with core damage is not a reason for discounting further consideration of means to protect the containment against the conditions generated by such an accident. In contrast, design extension conditions with core melting are required to be postulated in the design, in accordance with para 5.30 of SSR-2/1 (Rev. 1) [1].

4.36 The demonstration that a plant event sequence can be practically eliminated should consider the following, as applicable:

(a) An adequate set of safety provisions, including both equipment and organizational provisions;

(b) The robustness of these safety provisions (e.g. adequate margins, adequate reliability, qualification for the operational conditions);

(c) The independence between the stated equipment safety provisions (i.e. an adequate combination of redundancy, physical separation, diversity and functional independence).

4.37 Deterministic analyses of severe accidents should be performed using a realistic approach (see Option 4 in table 1 of SSG-2 (Rev. 1) [9]), to the extent practicable. Because explicit quantification of uncertainties might be impractical owing to the complexity of the phenomena and insufficient experimental data, sensitivity analyses should be performed to demonstrate the robustness of the results and to support the conclusions of the analyses. Sensitivity studies could also be used to confirm the adequacy and representativeness of the selected severe accidents considered for the bounding analysis.

4.38 When probabilistic arguments are used to support a claim that a particular plant event sequence has been practically eliminated, it should be ensured that the cumulative contribution of all the different event sequences considered does not exceed the target frequency for early radioactive releases or large radioactive releases, if such a target has been claimed by the designer or operating organization in the safety assessment of the plant or has been established by the regulatory body.

4.39 The validity of any probabilistic models used should be confirmed for the intended application. Assumptions made in support of this check should be well justified and validated.

4.40 The limitations of uncertainties associated with the models used in demonstration of practical elimination should be identified, taking into account that limitations of probabilistic safety assessment studies are associated with the probabilistic modelling, as well as the supporting deterministic best-estimate studies.

4.41 If the plant event sequence to be practically eliminated is the result of a single initiating event, such as the failure of a large pressure-retaining component[21] in normal operation, the demonstration of practical elimination should rely on the substantiation that a high level of quality is achieved at all stages of the lifetime of the component, i.e. its design, manufacture, implementation, commissioning and operation (including periodic testing and in-service surveillance, if any) so as to prevent the occurrence and propagation of any defect liable to cause the failure of the component. Hence, both the occurrence of the single initiating event (e.g. failure of a large pressure-retaining component) and the consequential event (i.e. uncontrolled reactivity accident) should be considered for practical elimination.

4.42 If the event sequence to be practically eliminated is the result of an event sequence in which the confinement function is degraded before core melt occurs, then it should be demonstrated, with a high degree of confidence, that core melt will be prevented. This means

[21] In some States, this demonstration is associated with other concepts such as ‘incredibility of failure’, ‘break preclusion’, ‘high integrity component’, ‘non-breakable component’, rather than with the concept of practical elimination.

that, at least, the usual levels of defence in depth should be implemented (i.e. for anticipated operational occurrences, design basis accidents and design extension conditions without significant fuel degradation) with enhancements, as necessary, to prevent design extension conditions with core melt.

DOCUMENTATION OF THE APPROACH TO PRACTICAL ELIMINATION

4.43 The safety analysis report of the plant should reflect the measures taken to demonstrate the practical elimination of plant event sequences that could lead to an early radioactive release or a large radioactive release. The safety analysis report should include, either directly or by reference, all elements of the demonstration, including the approach used to identify such event sequences, the design and operational safety provisions implemented to ensure that the possibility of such event sequences arising has been practically eliminated and the corresponding analyses.

5. IMPLEMENTATION OF DESIGN PROVISIONS FOR ENABLING THE USE OF NON-PERMANENT EQUIPMENT FOR POWER SUPPLY AND COOLING

5.1 As an application of Requirement 14 of SSR-2/1 (Rev. 1) [1], the design basis for items important to safety should take into account the most limiting conditions under which they need to operate or maintain their integrity. This includes the conditions resulting from internal and external hazards. In accordance with Requirement 17 of SSR-2/1 (Rev. 1) [1], the effects of internal and external hazards and relevant combinations of hazards are required to be evaluated. For external hazards this is done as part of the site evaluation for the plant (see IAEA Safety Standards Series No. SSR-1. Site Evaluation for Nuclear Installations [16]).

5.2 There have been cases in which some external hazards, such as extreme earthquakes, floods and tsunamis, have exceeded the levels of external hazards considered for the design. Paragraphs 5.21 and 5.21A of SSR-2/1 (Rev. 1) [1] state that adequate margins are required to be provided in the design to protect against external hazards for such cases.[22]

5.3 In addition to these margins and to provide additional resilience against event sequences exceeding those considered for design, such as levels of external hazards exceeding those considered in the design basis, several requirements are established in SSR-2/1 (Rev. 1) [1] regarding the inclusion of features in the design to enable the safe use of non-permanent equipment for the following purposes[23]:

(a) Restoring the necessary electrical power supplies (para. 6.45A of SSR-2/1 (Rev. 1) [1]);
(b) Restoring the capability to remove heat from the containment (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 (para. 6.68 of SSR-2/1 (Rev. 1) [1]).

5.4 The use of non-permanent equipment for other similar purposes, such as the removal of residual heat from the core is not explicitly required, but is not excluded.

5.5 Non-permanent equipment is primarily intended for preventing unacceptable radioactive consequences in the long term phase of accident conditions and after very rare events (e.g. external hazards exceeding the levels considered for the design, derived from the hazard evaluation for the site) for which the capability and availability of design features installed on-site might be affected[24]. The aim of the use of non-permanent equipment is to restore safety functions that have been lost, but it should not be the regular means for coping in the short term phase for design basis accidents or for design extension conditions (see also paras 7.51 and 7.64 of SSG-2 (Rev. 1)).

[22] Some States take a more formal approach to this issue by setting a higher level of hazards that has to be considered in design, although with realistic analysis assumptions and possibly relaxed failure criteria and acceptable limits for purposes of radiation protection.

[23] These requirements in SSR-2/1 (Rev. 1) [1] were the result of feedback from the Fukushima Daiichi accident and the stress tests or similar types of investigation conducted 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].

[24] Further considerations related to non-permanent equipment are provided in SSG-54 [15]

5.6 To meet the SSR-2/1 (Rev.1) requirements recalled in para. 5.2 and 5.3, levels of hazards exceeding those considered for design, i.e. those derived from the hazard evaluation for the site, should be considered and their consequences should be evaluated as part of the defence in depth approach. For natural external hazards, it is not always possible to get sufficient confidence in the frequency of occurrence of a certain level of hazard for the definition of a design basis level and furthermore for higher level. In that case, rather than trying to associate levels to frequencies, the level of natural hazards exceeding the level considered for design should be defined by the addition of a relevant margin. The behaviour of structures, systems and components to loading parameters resulting from these levels should be assessed.

5.7 An evaluation should be conducted to demonstrate that the plant would be able to cope with a external hazard of a severity exceeding the levels considered for the design as follows:

- To a certain extent, on the basis of the demonstration of the margin of a set of structures, systems and components that are necessary to reach a safe state, against the resulting loading of such a situation;
- After the main effects of the hazard have passed, and/or in addition to this, on the basis of the use of non-permanent equipment to restore the necessary safety functions.

5.8 For each relevant scenario involving an external hazard of a level exceeding the level considered for the design, the evaluation should identify limitations on the response capabilities of the plant and a strategy should be defined to cope with these limitations. The evaluation should also identify the various coping provisions, accident management measures and equipment (i.e. fixed or non-permanent equipment stored on the site or off the site) that will be used to restore the safety functions and to reach and maintain a safe state. The 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 levels of natural hazards exceeding those considered for design;

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

(c) The coping strategies to limit and mitigate the consequences of scenarios that could lead to a loss of relevant safety functions;

(d) An estimate of the necessary resources (i.e. human resources, equipment, logistics and communication) to confirm the feasibility of the coping strategies;

(e) A demonstration that the time available before a safety function is lost provides a sufficient margin over the time needed to perform all necessary actions to restore the safety function.

5.9 Some aspects of the use of non-permanent equipment and the associated safety assessment cannot be fully considered in detail at the design stage and should be considered in the commissioning and operation stages. However, specific provisions to ensure radiation protection of operating personnel for the use of non-permanent equipment should be considered at the design stage of new nuclear power plants or during the implementation of modifications, where applicable, for nuclear power plants designed to previous standards.

5.10 The evaluation should consider the possibility that multiple units at the same site could be simultaneously affected by such a level of natural external hazard exceeding those considered for the design.

5.11 The plant response and the coping strategies for natural external hazards exceeding the levels considered for design should be assessed based on a realistic approach and should be supplemented where relevant (e.g. in the case of cliff edge effects) by sensitivity analyses where assumptions in the modelling or where important operator actions are identified as essential factors for the credibility of the strategy.

5.12 The coping strategies should be defined, and the associated coping provisions should be specified and designed taking into account the possible scenarios, in accordance with para. 5.8.

5.13 To make the coping strategies more reliable, an adequate balance should be implemented between fixed equipment and non-permanent equipment. This balance should be defined in accordance with the time for which each coping strategy will need to be implemented (the ‘coping time’), the time for installation of the non-permanent equipment, flexibility of using equipment for different purposes, human reliability, the availability of human resources and the total number of operator actions needed for the whole coping strategy. The use of permanent fixed equipment should be preferred for the implementation of short-term actions.

5.14 The use of non-permanent equipment should be such that the time period needed for the installation and putting into service of the equipment is less than the defined coping time, with a specified margin allowed for time sensitive operator actions. Appropriate time margins should be established for implementing operator actions before the occurrence of a cliff edge effect. This time period should be derived, where possible, on the basis of times recorded during drills, or other approaches for validating operator actions. The ability to deliver and operate non-permanent equipment on time under adverse conditions at the site should also be demonstrated, particularly for events that could involve significant degradation of infrastructure and roads caused by extreme hazards on the site and off the site. Considerations should be given to storing non-permanent equipment at a distance from the units in the case of some extreme hazards.

5.15 To ensure the success and reliability of the coping strategies, the performance 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.

5.16 The appropriateness of the coping strategies and coping provisions, and the feasibility of implementation under environmental conditions caused by external hazards exceeding the levels considered for design and the radiological consequences of the accident should be evaluated.

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, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

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

[4] 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).

[5] 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).

[6] 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).

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

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

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

[10] 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). (A revision of this publication is in preparation.)

[11] 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). (A revision of this publication is in preparation.)

[12] 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).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.13, Vienna (2005). (A revision of this publication is in preparation.)

[14] 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).

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

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSR-1, IAEA, Vienna (2019).

ANNEX I. EXAMPLES OF CASES OF PRACTICAL ELIMINATION

This annex is an illustration of potential examples and should be considered carefully: both list of example and contents of associated articles differ between different Member States.

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 in which reactor cooling would be lost in a short time and a pressure wave or a missile would damage the containment boundary. The safety provisions for defence in depth would not be effective in a such situation and an early radioactive release or large radioactive release could follow. This is a very exceptional type of initiating event for which safety systems and safety features are not designed for its mitigation and therefore it needs to be demonstrated that with high confidence the likelihood of such an initiating event occurring would be so low that it can be excluded, i.e. practically eliminated, from consideration. This is particularly important for the reactor vessel, in which a break would eliminate the capability of holding and cooling the core. In addition, the likelihood of a failure of the pressurizer or the steam generator shell need to be shown to be extremely low, or alternatively it needs to be demonstrated that a failure of the pressurizer or the steam generator shell would not lead to unacceptable consequences for the containment.

I-2. The safety demonstration needs to be especially robust and the corresponding assessment suitably demanding, so that an engineering judgement can be made for the following key aspects of each large component in the reactor coolant system:

(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 operating practices need to be in place to minimize thermal fatigue, stress corrosion, embrittlement, pressurized thermal shock and over-pressurization of the primary circuit;
(f) A continuous leak detection capability during pressurised operation;
(g) Effective in-service inspection and surveillance and chemistry control programmes need to be in place during the manufacture, construction, commissioning and the operation of the equipment, so that any defects or degradation mechanisms are detected and to ensure that equipment properties are preserved over the lifetime of the plant.

I-3. In addition, evidence needs to be provided to demonstrate that the necessary integrity of large components of the reactor coolant system 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 failures of the pressure vessel has to be based on rigorous application of these technical standards. Such technical standards also provide instructions for verification of the state of the pressure vessel during the lifetime of the vessel.

I-5. The practical elimination of failures of large components is thus achieved by the first level of defence in depth and does not rely on the subsequent levels of defence in depth.

I-6. The demonstration, with a high level of confidence, of a low likelihood of failure 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 to be 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 assessments address aspects such as material fracture toughness and weld residual stress, which in turn consider deterministic analysis, engineering judgement and the measurements of monitored values.

FAST REACTIVITY INSERTION ACCIDENT IN A LIGHT WATER REACTOR

I-7. Fast reactivity accidents can be very energetic and have a potential to destroy the fuel, fuel cladding and other barriers. As far as practicable, the prevention of such accidents is to be ensured at the first level of defence in depth by proper design of the reactor coolant system and the core, or at the third level of defence in depth by provision of two diverse, independent means of shutdown.

I-8. The first level of defence in depth may be provided by the core nuclear characteristics (such as the negative reactivity coefficient in light water reactors), which, under all possible combinations of reactor power, neutron absorber concentration, coolant pressure and temperature, suppresses any increase in reactor power during any disturbances and eliminate any uncontrolled reactivity excursion. Therefore, this is a case of demonstration of practical elimination by physical impossibility of the event sequence.

I-9. 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. In this case, the demonstration of practical elimination is because the event sequence is considered physically impossible to occur.

I-10. Therefore, the demonstration of practical elimination relies primarily on impossibility of reactivity excursions through a core design with overall small or negative reactivity coefficients, supported by other design measures to avoid or limit excursions of reactivity, which can be evaluated deterministically and probabilistically as appropriate to demonstrate that the conditions are extremely unlikely to occur.

I-11. A more complex situation could arise however if criticality can be reached during a severe accident. This has been a topic of concern for specific core meltdown scenarios in reactors, for which 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 the control rods have relocated downwards but the fuel rods are still in their original position. This could result in re-criticality of the fuel, likely resulting in the generation of additional heat on a continuing or intermediate basis, depending on the presence of water. This is again an aspect to be analysed by considering the design provisions and severe accident management features together, in order to be able to demonstrate that the plant sequence has been practically eliminated because it is considered, with a high level of confidence, to be extremely unlikely to occur.

DIRECT CONTAINMENT HEATING

I-12. In a pressure vessel reactor, 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 from the hot melt and exothermic chemical reactions. Plant event sequences involving high pressure core melt therefore need to be practically eliminated by design provisions to depressurize the reactor coolant system when a meltdown is found unavoidable, so that the conditions are considered, with a high level of confidence, to be extremely unlikely to occur.

I-13. In a pressurized heavy water reactor, in contrast, direct containment heating due to ejection of the molten corium at high pressure is practically eliminated because pressure tubes would fail rapidly at high fuel temperature. This would depressurize the primary system before significant core melting can occur. This is a case of practical elimination of the event sequence owing to its physical impossibility.

I-14. 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 design provisions in place to ensure, with a high level of confidence, that such small coolant leaks or boiling of the coolant instead would result in 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 any discharge of molten corium from the reactor vessel can take place. In addition, it is important that dynamic loads from depressurization do not cause a threat to the containment structures. Design provisions need to be in place to ensure, with a high level of confidence, that any high pressure core meltdown scenario does not occur.

I-15. Dedicated depressurization systems have been installed in existing plants and designed for new plants. At pressurized water reactors, such systems 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 if the 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 at very low pressures.

I-16. 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 of the systems by operating personnel. In this way, direct containment heating could be demonstrated, with a high level of confidence, to be extremely unlikely to occur, based on a combined deterministic and probabilistic assessment of specific design provisions.

LARGE STEAM EXPLOSION

I-17. 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 might occur in-vessel, during flooding of a degraded core or if a molten core relocates into the lower head filled with water. Such interactions might also occur ex-vessel, if 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 a potentially serious challenge to the integrity of the reactor vessel and/or the containment.

I-18. The conditions of the triggering of a steam explosion and the energy of explosion in various situations have been widely studied in reactor safety research programmes. The risks of steam explosion cannot be fully eliminated for all core meltdown scenarios in which molten core might drop to water.

I-19. For the practical elimination of steam explosions that could damage the integrity of the containment, the preferred method is to avoid the dropping of molten core into water for all conceivable accident scenarios. Such approach is used in some pressurized water 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 boiling water reactors and in some new designs of boiling water reactors, the molten core would drop to a pool below the reactor vessel in all severe accident scenarios and would be solidified and cooled in the pool. In all such circumstances in which the molten core drops to water, it needs to be proven with arguments based on the physical phenomena involved in the respective scenarios that the risk of steam explosion damaging the containment integrity has been practically eliminated owing to the physical impossibility of the event sequence.

EXPLOSION OF COMBUSTIBLE GASES: HYDROGEN AND CARBON MONOXIDE

I-20. Hydrogen combustion is a very energetic phenomenon, and a fast combustion reaction (detonation) involving a sufficient amount of hydrogen would cause a significant threat to the containment integrity. Dedicated means to prevent the generation of hydrogen and its accumulation at critical concentrations, and to eliminate hydrogen detonation, are needed at all nuclear power plants, although different means are preferred for different plant designs.

I-21. In boiling water reactor containments, which are all relatively small, the main means of protection against hydrogen generation and accumulation 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 against hydrogen detonation.

I-22. 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 eliminates excessive local hydrogen concentration, taking into account that the risk of hydrogen detonation increases if steam providing inertization is condensed.

I-23. The consequences of hydrogen combustion will depend on the highest conceivable rate and the total amount of hydrogen generation inside the containment. Some core catchers that are currently installed in nuclear power plants can significantly reduce or even eliminate ex-vessel hydrogen generation in an accident when the molten core has dropped to the catcher, and this could also considerably reduce the total amount of hydrogen generated inside the containment.

I-24. In particular, 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.

I-25. Carbon monoxide can be generated in a severe accident if molten core 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 this chemical reaction is less energetic than hydrogen combustion and the burning velocity is also lower. Therefore, the contribution of carbon monoxide to the risks to the containment integrity has generally received less attention. However, the presence of 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 so as to demonstration the practical elimination of hydrogen combustion. A design provision to minimize the impact of carbon monoxide is the use concrete with low contents of limestone.

LONG TERM LOSS OF CONTAINMENT HEAT REMOVAL

I-26. 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 a severe accident where the core is molten and is generating steam inside the containment, cooling of the containment atmosphere is a preferred means for preventing its overpressure.

I-27. There are several examples, from both existing plants and from new plant designs, of robust dedicated containment cooling systems that are independent of safety systems and might be capable of supporting the demonstration of practical elimination of containment rupture by overpressure.

I-28. An alternative to cooling of the containment is elimination of containment overpressure by means of venting. This is necessary especially in some boiling water reactors, where the size of the containment is small and pressure limitation might be needed for design basis accidents and design extension conditions with core melt. The venting systems in existing plants prevent overpressurization at the cost of some radioactive release involved in the venting, also in the case that the venting is filtered. However these might be acceptable strategies for severe accident management if technically justified given the risk levels and an appropriate assessment of the decontamination factors for the strategy.

I-29. Containment venting avoids a risk to the containment integrity due to overpressurization, but stabilization of the core and the cooling of the containment are still necessary in the longer term.

I-30. 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. Level 2 probabilistic safety assessment can be used to demonstrate the very low probability of plant event sequences that could lead to a large radioactive release, i.e. the practical elimination of long term loss of containment heat removal owing to its being considered, with a high level of confidence, to be extremely unlikely to arise.

CONTAINMENT PENETRATION BY INTERACTION WITH THE MOLTEN CORE

I-31. In 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-32. Alternative means have been developed and verified in extensive severe accident research programmes in this area conducted in several States and also with 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 and cool the molten core as soon as it has penetrated the reactor vessel wall.

I-33. In both approaches, cooling of the molten core generates steam inside the containment, and it is also 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-34. While probabilistic safety assessment can play a role in assessing the reliability of establishing external reactor vessel cooling or the core catcher cooling (if provided), the demonstration of the practical elimination of melt through of the containment boundary relies extensively on deterministic analysis of the design provisions, to demonstrate that such containment penetration can be considered, with a high level of certainty, to be extremely unlike to arise.

SEVERE ACCIDENTS WITH CONTAINMENT BYPASS

I-35. Containment bypass can occur in different ways, such through circuits connected to the reactor coolant system that exit the containment or as a result of defective steam generator tubes (for pressurized water reactors). Severe accident sequences with non-isolated penetrations connecting the containment atmosphere to the outside and severe accident sequences during plant shutdown with the containment open also need to be considered as containment bypass scenarios. Failures of lines exiting the containment and connected to the primary system, including steam generator tube ruptures, are at the same time accident initiators, whereas other open penetrations only constitute a release path in accident conditions. Nevertheless, all these plant event sequences have to be practically eliminated by design provisions such as adequate piping design pressure and isolation mechanisms.

I-36. The safety demonstration for elimination of bypass sequences includes a systematic review of all potential containment bypass sequences and covers all containment penetrations.

I-37. Requirement 56 of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [I–1] establishes the minimum isolation requirements for various kinds of containment penetration. 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 interface systems loss of cooling accidents.

I-38. Based on the implementation of the design requirements or specific national regulations and the in-service inspection and surveillance practices at the plant, 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 to 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 operator actions, other analysis aspects might 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 to a defensible low frequency estimate of the bypass mechanisms associated with each penetration. In addition, the reliability of design provisions for the isolation of bypass paths based upon conventional probabilistic assessments would complement the demonstration that plant event sequences with containment bypass have been practically eliminated.

SIGNIFICANT FUEL DEGRADATION IN THE SPENT FUEL POOL

I-39. Facilities for spent fuel storage need to be designed to ensure that plant event sequences that could lead to an early radioactive release or a large radioactive release 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 involves 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 sufficiently reliable means (e.g. such as applying redundancy, diversity and independence see para. 3.7 of IAEA Safety Standards Series No. SSG-63, Design of Fuel Handling and Storage Systems for Nuclear Power Plants [I-2]) 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-40. Risks for mechanical fuel failures need to be eliminated by the following means:

(a) A design that ensures that heavy lifts (e.g., a transport cask) 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-41. In designs where the spent fuel pool is outside the containment, the uncovering of the fuel would lead to fuel damage and a large radioactive 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. Therefore, it is necessary to ensure by design provisions that the uncovering of spent fuel elements has been practically eliminated.

I-42. In some designs, the spent fuel pool is located inside the containment. In this case, even though spent fuel damage would not lead directly to a large radioactive 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 could eventually lead to a large radioactive release. Therefore, it is also necessary to ensure by design provisions that also in this case 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).

[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Fuel Handling and Storage Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-63, IAEA, Vienna (2020).

ANNEX II.
APPLICATION OF THE CONCEPTS OF DESIGN EXTENSION CONDITIONS AND PRACTICAL ELIMINATIONTO NUCLEAR POWER PLANTS DESIGNED TO EARLIER STANDARDS

II-1. Paragraph 1.3 of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [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 event sequences that could lead to an early radioactive release or a large radioactive release need to be assessed as part of the periodic safety review processes with the objective of further improving the level of safety, where reasonably practicable.

II-2. The concepts of design extension conditions and practical elimination of plant event sequences that could lead to an early radioactive release or a large radioactive release are not new. In fact, the concept of practical elimination was already introduced in the 2004 IAEA Safety Guide for the design of the reactor containment[25], and both concepts might have been applied partially in the design of some existing nuclear power plants, although not necessarily 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 event sequences that could lead to an early radioactive release or a large radioactive release have been addressed also in many designs already, although a specific demonstration of the practical elimination of such plant event sequences has not been carried out.

II-3. In relation to practical elimination, a number of measures might have been taken for instance, for the prevention of a break in the reactor pressure vessel, for fast reactivity insertion accidents or for severe fuel degradation in the spent fuel pool. However, a demonstration that the existing safety provisions are sufficient to claim the practical elimination of such plant event sequences 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.

II-4. However, an accident condition commonly considered as a design extension condition in a new nuclear power plant (e.g. station blackout or anticipated transient without scram), can only be considered a design extension condition for an existing nuclear power plant if safety features have been introduced in the original design of the existing plant to mitigate the

[25] See para. 6.5 of 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), which has been superseded by INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-53, IAEA, Vienna (2019) [II-2].

consequences of this condition. 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 an original design safety feature. Likewise, for anticipated transient without scram, additional design features capable of rendering the reactor subcritical in case of failure in the insertion of control rods would need to be included in the original design. Without such additional design features in the original design, these accident conditions would need to be considered to be beyond the design basis of the plant.

II-5. Generally, it is 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, the feasibility of reasonable safety improvements in relation to design extension conditions and practical elimination would be considered. There can, however, be constraints on installing the same type of design features as commonly implemented in the design of new nuclear power plants, especially for design extension conditions with core melting such as the implementation of the ex-vessel melt retention or in-vessel corium cooling strategies in PWR designs. In the same context, there can be constraints on ensuring the independence of safety provisions relating to the different levels of defence in depth.

II-6. Safety provisions for design extension conditions and also design features for the practical elimination of plant event sequences that could lead to an early radioactive release or a large radioactive release are addressed in several Safety Guides related to the design of plant systems, including SSG-53 [II-2] and IAEA Safety Standards Series Nos SSG-56, Design of the Reactor coolant 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–2] encompasses most of the design features for design extension conditions with core melting, and addresses the plant event sequences to be considered for practical elimination. SSG-53 [II–2] 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 in the design of the prevention and mitigation 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. 3.23 of this Safety Guide, for design extension conditions without significant fuel degradation, for postulated initiating events less frequent than those considered for design basis accidents it can be acceptable 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. For existing nuclear power plants, this is a possibility to demonstrate the capability for mitigation of design extension conditions not originally postulated in the design, such as a multiple rupture of steam generator tubes. Existing nuclear power plants could also extend the capability of safety systems to be capable of mitigation of some design extension conditions, in accordance with paragraph 5.27 of SSR-2/1 Rev/1 [1].

II-8. The consideration of external events of a magnitude exceeding the original design basis derived from the hazard evaluation for the site, as addressed in Section 5, is to be considered. While for new nuclear power plants the mitigation of design extension conditions is generally expected to be accomplished by permanent design features, and the use of non-permanent equipment is intended only 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 might 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 are relevant. Non-permanent equipment that would be necessary to reduce further the consequences of events that cannot be mitigated by the installed plant capabilities needs to be stored and protected to ensure its availability when necessary, with account taken of possible restricted access due to external events (e.g. flooding, damaged roads) and its operability needs to be verified.

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 Containment and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-53, IAEA, Vienna (2019).

[II–3] 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–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).

DEFINITION

Practical elimination

Ensuring by implementing safety provisions in the form of design and operational features that plant event sequences that could lead to an early radioactive release or a large radioactive release are either physically impossible or are considered, with a high level of confidence, to be extremely unlikely to arise.

> ⓘ The concept of practical elimination is applied in relation to plant event sequences for which reasonably practicable technical means for their mitigation cannot be implemented.

> ⓘ Practical elimination is part of a general approach to design safety and is an enhancement of the application of the concept of defence in depth.

CONTRIBUTORS TO DRAFTING AND REVIEW

Buttery, N.	European Nuclear Installations Safety Standards (ENISS)
Courtin, E.	World Nuclear Association (WNA) / Framatome
Dakin, R.	Office for Nuclear Regulation (ONR), UK
Delfini, G.	Authority for Nuclear Safety and Radiation Protection (ANVS), The Netherlands
Ermolaev, A.	VNIIAES, ROSENERGOATOM, Russian Federation
Exley, R.	Office for Nuclear Regulation (ONR), UK
Franovich, M.	US Nuclear Regulatory Commission, USA
Gyepi-Garbrah, S.	Canadian Nuclear Safety Commission (CNSC/CCSN), Canada
Garis, N.	Swedish Radiation Safety Authority, Sweden
Hardwood, C.	Canadian Nuclear Safety Commission (CNSC/CCSN), Canada
Ibrahim, M. A.	Nuclear Power Plants Authority (NPPA), Egypt
Jansen, R.	Authority for Nuclear Safety and Radiation Protection (ANVS), The Netherlands
Järvinen, M.L.	Nuclear Reactor Regulation Department; Radiation and Nuclear Safety Authority (STUK), Finland
Kim, K.T.	Korea Atomic Energy Research Institute (KAERI), Republic of Korea
Koski, S.	Teollisuuden Voima Oyj (TVO), Finland
Lignini, F.M.	World Nuclear Association (WNA) / Framatome
Luis Hernandez, J.	International Atomic Energy Agency
Kral, P.	Nuclear Research Institute Rez, Husinec – Rez, Czech Republic
Rodriguez Mate, C.	Nuclear Safety Authority (ASN) France
Bernard, M.	DIPNN, Electricité de France (EDF), France
Muellner, N. A.	University of Natural Resources and Life Sciences, Institute for Safety and Risk Sciences, Vienna, Austria

Nakajima, T.	Nuclear Regulation Authority (NRA), Japan
Nuenighoff, K.	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Germany
Obenius Mowitz, A.	Swedish Radiation Safety Authority, Sweden
Okano, T.	Nuclear Regulation Authority (NRA), Japan
Poulat, B.	Consultant, France
Ranval, W.	European Nuclear Installations Safety Standards (ENISS)
Rogatov, D.	Scientific and Engineering Centre for Nuclear Radiation and Safety (SEC NRS), Russian Federation
Schwartz, G.R.	Consultant, Canada
Stoppa, G.	Federal Ministry for the Environment, Germany
Tas, F.B.	Nuclear Regulatory Authority (NDK), Turkey
Titus, B.A	US Nuclear Regulatory Commission, USA
Uhrik, P.	Nuclear Regulatory Authority (UJD), Slovak Republic
Virtanen, E.	Radiation and Nuclear Safety Authority (STUK), Finland
Wattelle, E.	Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France
Wong, E.K.Y.	Radiation Protection and Nuclear Science Department, National Environment Agency, Singapore
Yllera, J.	International Atomic Energy Agency