22-04-2022

Style Definition: Heading 3,Second level headers: Indent: Left: 0 cm, First line: 0 cm

Style Definition: 4

IAEA SAFETY STANDARDS

for protecting people and the environment

Step 10:

Review by Coordination Committee

Reviewed in NSOC (Asfaw)

Review Committees: NUSSC (lead), NSGC

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

DS508

DRAFT SAFETY GUIDE

New Safety Guide

CONTENTS

Field Code Changed

Field Code Changed

Field Code Changed

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],[1] introduced changes to the requirements for the design of nuclear power plants. (NPP). These changes include measures for strengthening the application implementation of the concept of defence in depth as followsby means of the following:

a) Including design extension conditions among the plant states to be considered in the design; (DEC);

b) Ensuring in the design that Practically eliminating[2] plant event sequences that could lead to anresult in early radioactive release releases or a large radioactive release[3] have been 'practically eliminated'releases[4];

c) Including design features to enablefor enabling the use of non-permanent equipment for power supply and cooling.

c) The incorporation of these aspects into designs of in new nuclear power plants will affect designs requires specific guidance for the design and the necessary safety assessment. Although specific guidance is provided in safety guides for the design of safety features related to these aspects, overarching guidance on their application to the plant design and on their safety assessment is necessary in a single safety guide.

1.2 IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment of Facilities and Activities [3][2] establishes high level requirements for performing the safety assessment for covering the whole lifetime of all types of facility and activity, including assessment of defence in depth. . However, these high level requirements are not sufficiently detailed for ensuring the thorough performance of the safety assessment for nuclear power plants design. Specific requirements for safety assessment and safety analysis of nuclear power plants are established in SSR-2/1 (Rev. 1) [1]. [1], and these need to be considered to address specific aspects of relevance for nuclear power plant design.

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

[2] The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.

[3] 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].

[4] The possibility of event sequences arising may be considered to have been practically eliminated if it would be physically impossible for the event sequence to arise or if these event sequences could be considered with a high level of confidence to be extremely unlikely to arise [1, 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

Commented [AKE1]: In line with SSR-2/1 (Rev. 1), I have changed this to 'application' when talking about the *concept* of DiD DiD. When talking about safety provisions/safety measures, I have left it as 'implementation' (also when talking about DiD as a shorthand for measures)

Commented [AKE2]: I have removed DEC and DBA. They don't appear often enough to warrant their retention (only 64 and 36 times, respectively)

Commented [AKE3]: this is too 'active': you are talking here about what the changes in SSR-2/1 are, not what one is actually doing in a plant

Commented [AKE4]: definitely not 'plant states'? As in para 4.3 of SSR-2/1 (Rev. 1)? (We went through this discussion for SSG-61, but just double checking here. I have made a few changes throughout for consistency)

Commented [AKE5]: I've changed 'result in' to 'lead to' for consistency with SSG-61 too

Commented [AKE6]: changed throughout to singular (because we don't like to talk about plural bad things)

in the footnotes I have added a reference to both SSR-2/1 (Rev.1), which uses this exact language, and also to the 2018 Glossary, from which the footnotes are adapted. You definitely need a reference to the Glossary early on in this SG

Formatted: Normal, Space After: 0 pt, No bullets or numbering

Commented [LHJ7]: The requirements in GSR Part 4 (Rev. 1) are very general or high level if compared to SSR-2/1 (Rev. 1), and without too much detail when considering NPPs.
If not "high level" could be say "general"?

Commented [NM8R7]: By definition, GSR means general safety requirements. No need to specify further here.

Commented [AKE9]: no need to justify the next sentence

Commented [LHJ10R9]: OK, but how do reach this SG, then? Can be mentioned:
However, further guidance is needed to ensure the throughout assessment of the effective implementation of these aspects for nuclear power plants.

Commented [NM11R9]: You do not need an additional sentence here. It is fine as it is. This is only the BACKGROUND section of the publication.

OBJECTIVE

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

Commented [AKE12]: we always use application

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 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. 2. These measures play an important role in the applicationimplementation of the concept of defence in depth for achieving a balance design of NPP, which constitutes the primary means of both preventing accidents and mitigating thetheir consequences of accidentsshould they occur, in accordance with Principle 8 of IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [4].

1.51.8 [3]. As described in para. 2.13 of SSR-2/1 (Rev. 1) [1],[1], the implementation of defence in depth at nuclear power plants comprises five5 levels. Plant states considered in the designSafety features for DEC as well as safety provisions that underpin the demonstration of practical elimination of event sequences that can lead to early radioactive releases or large radioactive releases correspond to one or more levels of defence in depth. This Safety Guide is structured in terms of the design of safety provisions necessary for each plant state, rather than for each levelTherefore, this Safety Guide addresses the implementation and assessment of defence in depth. In this way, the significance and importance of design extension conditions for the safety approach is emphasized. in relation to these aspects.

1.6 This Safety Guide considers the assessmentIn addition to anticipated operational occurrence (AOOs), and design basis accidents (DBAs), design extension conditions (DECs) without significant fuel degradation and DEC with core melting are part of the implementation of the concept of dDefence in Ddepth. There, iIn terms of deterministic safety analyses methods, rules and assumptions to be followed, the IAEA safety guide SSG2 (Rev.1) [4][8] is already providesing relevant guidance to all plant states. However, there is a need to develop guidance about the integration of DEC within the overall implementation of Ddefence in Ddepth. Therefore, this Safety Guide was developed to provide guidance on that aspect.

Commented [AKE13]: I think it is important to have up front exactly the same scope as SSR-2/1 (Rev.1).

Unless you intend a different scope – in which case you should be very clear about that

Commented [AKE14]: is this needed? they might not be in operation yet

Commented [LHJ15R14]: I do not think so. Many MS will be reluctant to accept this paragraph which means they need to apply modifications to meet the objective set with the practical elimination of plant event sequences.

Commented [NM16R14]: ok

Commented [AKE17]: yes?

Commented [AKE18]: this concept is not well established, or used much in this Safety Guide. I suggest not introducing it here

Commented [LHJ19R18]: balance here is related to the means for prevention and mitigation considered in the design, to avoid designers to put all efforts only in the mitigation, such as the use of non-permanent equipment to cope with severe accidents during the medium-term phase of the accident progression and not only for the long-term.

Commented [NM20R18]: I will agree with Katherine that this needs to be deleted. If you keep it, you will need to explain what it means.

Commented [AKE21]: I have taken this from Section 3. It seems to explain why the SG is addressed in terms of plant state rather than level of Did

Commented [AKE22]: this is kind of a repetition of the previous para and the bit about DEC A and DEC B doesn't need to be introduced yet

Commented [AKE23]: SSG-2 is mentioned below, you don't need it here too.

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

Commented [AKE24]: actually, it considers many types of dependence in a general manner. The examples in the next para are examples of CCF, not functional dependence

Commented [AKE25]: this is not part of scope, i.e. it is not explaining something that is left out of the scope. It is moved to Section 5

~~1.8~~1.9 ~~This Safety Guide also addresses the assessment of the design features~~ considered ~~to further strengthen defence in depth by including design features for enabling the use of non-permanent equipment for~~ ensuring additional backup sources such as emergency ~~power supply and for cooling~~ capabilities~~, as a result of the lessons learned from the Fukushima Daiichi accident. These features are primarily intended for preventing unacceptable radioactive releases~~ during the long term phase of accidents conditions and after ~~in the~~ very rare ~~event~~s (e.g., natural external hazards exceeding the magnitude considered for the design, derived from the hazard evaluation for the site), where the capability and availability of design features installed on-site might be affected ~~of levels of natural external hazards exceeding the magnitude considered for the design, derived from the hazard evaluation for the site~~.

1.91.10 The Safety Guide doesguide is not intended to provide specific recommendations for the design of particular safety features for design extension conditionsDEC or for any other plant state considered in the design. Such recommendationsThese are provided in Safety Guidesthe safety guides for the design of various types of plant system, such asfor instance in IAEA Safety Standards Series Nos SSG-56, Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants [5],[4], SSG-53, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants [6],[5], SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [7],[6], and SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [8].[7].

1.101.11 This Safety Guide does not consider the specific safety analyses to be carried out for different plant states, as these arethis is addressed in IAEA Safety Standards Series, Nos SSG-2 (Rev. –1), Deterministic Safety Analysis for Nuclear Power Plants [1],[8], SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [10],[9], and SSG--4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants [11],[10], as appropriate. However, this Safety GuideThis safety guide takes into account however the recommendations providedguidance in these publicationsthem.

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

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

STRUCTURE

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

Commented [AKE26]: there are no GSR Part 4 requirements duplicated in Section 2

Commented [AKE27]: Section 2 doesn't really do that anymore. (Earlier drafts did)

~~1.14~~1.13 Annex I provides examples~~information on the demonstration~~ of cases~~a commonly recognized set~~ of practical elimination.~~events or plant conditions that need to be demonstrated to have been practically eliminated.~~ Annex II provides some considerations for the application of recommendations included in this Safety Guide to nuclear power plants designed to earlier standards when evaluating potential safety enhancements of such designs, for example, as part of the periodic safety reviews.

2. ~~-~~DESIGN APPROACH ~~WHEN~~ 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.

~~2.1~~2.2 Requirement 5 of SSR-2/1 (Rev. 1) [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.**"

~~2.2~~2.3 Paragraph 4.3 of SSR-2/1 (Rev. 1) [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."

~~2.3~~2.4 Furthermore, para. 4.4 of SSR-2/1 (Rev. 1) [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."

~~2.4~~2.5 Further~~The~~ requirements on criteria and objectives relating torecalledrecalled ~~in paras 2.3–2.5 establish the need for~~ radiological consequences of different plant states considered in the design, including accident conditions~~, to be not only below acceptable limits but to be as low as reasonably achievable (ALARA). In addition, it needs to be demonstrated in the design that plant states that could lead to high radiation doses[5] or to a large radioactive release have been 'practically eliminated'. Further requirements for categories of plant states and more specifically for accident conditions~~ are also established~~specified~~ in SSR-2/1 (Rev. 1) [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

[5] Plant states leading to high radiation doses are equivalent to plant states leading to early radioactive release.

Commented [AKE28]: this para is the only para in this section that does not quote requirements, and as such it seems better to have it at the beginning of Section 2, rather than in the middle

Commented [AKE29]: inserted because of IEC comment at CC

Commented [LHJ30R29]: I did the proposal of that text based on the IEC comment, so agree.

Commented [AKE31]: this makes it look like there are requirements for the specific plant systems addressed in this guide, but it's not really the case (and SCOPE also says it's not true). Hence deleted

Commented [LHJ32R31]: Agree, the text was related to the requirements for the general plant design, but there are no recommendations for them here.

Commented [LHJ34R33]: If deleted, we are missing part of the message here which is the ALARA.

Commented [AKE33]: this repeats the paras above, so I deleted this sentence

Commented [NM35R33]: We are not missing anything, because we have the quote in para. 2.2

Commented [AKE36]: you've already quoted para 4.3 of SSR-2/1, so I deleted this sentence

Commented [LHJ37R36]: If deleted the key point made here related to plant event sequences that need to be practically eliminated is missing.

Commented [NM38R36]: It is not missing, it is covered in the quoted paras of SSR-2/1 (Rev. 1). It will be worse to repeat the same things.

to serious consequences shall have a very low frequency of occurrence" (para. 5.2 of SSR-2/1 (Rev. 1) [1][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][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][1][1] in relation to design extension conditionsDEC).

— "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][1][1] in relation to design extension conditionsDEC).

— "The same or similar technical and radiological criteria as those for design basis accidents may be considered for these conditions to the extent practicable. Radioactive releases should be minimized as far as reasonably achievable." (para. 7.46 of SSG-2 (Rev. 1) [8] in relation to DEC).

2.6 This Safety Guide is focused on the protection of the public and the environment in accident conditions, which should be assessed notably regarding compliance with a number of requirements in SSR-2/1 (Rev. 1) [1][1]. These requirements pertain to the general plant design and particularly on its capability to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures, as well as other requirements for plant specific systems, for instance those related to the containment structure and its systems. As indicated in para. 2.10 of SSR-2/1 (Rev. 1) [1]:

> 2.5][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.""[6].

2.7 In accordance with para. 2.13 (4) of SSR-2/1 (Rev. 1) [1]:;

> "…TheTthe 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".

2.6 Harmful radiological consequences to the public can only arise only from the occurrence of uncontrolled accidents. Therefore, the following chapters are devoted to the implementation and assessment of design extension conditions within the concept of defence in depth and the

[6] The establishment of off-site protective actionsarrangements belongs to the 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 [1211].

Field Code Changed

Field Code Changed

Field Code Changed

Commented [LHJ40R39]: OK

Field Code Changed

Commented [AKE39]: deleted because
1) it's not a requirement from SSR-21 (Rev. 1), as the chapeau would suggest
2) it is addressed elsewhere in the text anyway

Formatted: Indent: Left: 1 cm, No bullets or numbering

Commented [AKE41]: this is all just introductory stuff

~~complementary need for demonstration of practical elimination of accident sequences that can lead to early radioactive releases or large radioactive releases.~~

~~2.7~~2.8 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]. ~~[12],~~ 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]. ~~[13].~~

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 paraspara. s 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].]. This section addresses 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."

3.13.2 overall application of Requirement 7 of SSR-2/1 (Rev. 1) [1][1) [1][1) [1]]] on the applicationimplementation of defence in depth in the design of nuclear power plants, which 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".**

3.23.3 ParagraphsSubsequent parasgraphs 4.9 to 4.-13A of SSR-2/1 (Rev. 1) [1] develop this overarching requirement. The specific focus of this Safety Guidesafety guide is on the reactor core as the main source of radioactivity with special emphasis on design extension conditions. As per 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 in terms ofconsidering 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.

3.33.4 For the implementation of safety provisions at each level of defence in depth, the followingthere are three main aspects of importance that should be demonstrated are, as follows:

(a) The performance of the safety provisions implemented at that level to maintainprotect the integrity of the barrier(s) that should be protected;

(b) The Adequate reliability of the safety measures provisions required at that level so that it can be assured,to demonstrate with a sufficient level of confidence, that a certain plant condition can be brought under control without needing the need to implementintervention of the safety provisions associated withimplemented for the next level;

Formatted: Indent: Left: 1 cm

Commented [AKE42]: this is a quote. It is moved up to where this para is first mentioned, rather than swapping back and forth between quotes of various different bits of SSR-2/1 (Rev. 1)

Commented [AKE43]: I think you don't need this.

Commented [LHJ44]: The important point here is not only the implementation of the additional safety features for the next level but the performance.

(c) The independence, as far as applicable, of the safety provisions at that level, including their physical separation[7] ~~and segregation~~, from the safety provisions associated with~~implemented at~~ the previous levels of defence in depth.

3.5 Frequently, for purposes~~An association~~ of design safety and operational safety, the various levels of defence in depth are associated to the various ~~with~~ plant states considered in the design. ~~is frequently undertaken for design safety and operational safety.~~ The introduction of design extension conditions among~~DEC in~~ the plant states~~design basis~~ has resulted into different interpretations in different~~by~~ Member States regarding the correspondence between the plant states considered in the design and the levels of defence in depth. Two~~, two~~ of these approaches~~which~~ are represented in Table 1. In Approach 1, depicted on the left hand side of Table 1, design extension conditions~~approach 1 (i.e. the association of DEC~~ without significant fuel degradation are associated ~~core melt~~ing –to level 3 of defence[8] in depth. In this approach,Table 1~~),~~ each level has a clear objective that reflects~~objectives regarding~~ the progression of an~~the~~ accident and the protection of the barriers, i.e. level 3 is implemented to prevent fuel damage ~~to the reactor core~~ and level 4 is implemented to mitigate severe accidents and prevent~~for preventing~~ off- –site contamination. Design extension conditionsDECDEC without significant fuel degradation could be understood as those representative eventaccident accident sequences involving either a single initiating eventeventsevents of very low frequency, or an anticipated operational occurrence, AOO or frequent design basis accident DBAs combined with multiple failures, which are considered in the design in order to prevent both reactor core melt and melting of fuel stored in the spent fuel pool[9]. Therefore, in Approach~~Radiological a~~Therefore, for approach 1, acceptable limits on predicted radiological consequences for design extension conditions~~DEC~~ without ~~core melt~~ significant fuel degradation ~~are~~ may be the same as or similar to acceptable~~as for DBA~~ limits for design basis accidents. Furthermore~~. Also~~, the physical phenomena associated with design basis accidents and design extension conditions~~in case of DBA and DEC~~ without significant fuel degradation are similar, although there mightmaymay be ~~are~~ differences in the analysis. In contrast, the physical phenomena associated with design extension conditions with core melt ~~severe accidents~~ are ~~characterized by~~ completely different.

3.6 In~~ physical phenomena.~~ Approach 2, depicted on ~~(i.e.~~ the right hand side~~grouping~~ of Table 1, design extension conditions~~DEC~~ without significant fuel degradation and design extension conditions with core melt are grouped together~~and core melt and with core melt~~ in level- 4 of defence in depth. This approach~~)~~ emphasizes the distinction~~differentiation~~ between the set of rules to be applied for DEC and DBA when considering both for their design extension

[7] Physical separation is separation: Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof [2]... (INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: 2018 Edition, Non-serial Publications, 2019.)

[8] "DEC without core melting" corresponds to "DEC without significant fuel degradation" as presented in IAEA Specific Safety Requirements, SSR-2/1(Rev. 1).

[9] There is consensus that design extension conditionsDECDEC without significant fuel degradation are mainly identified as a result of Levellevellevel 1 probabilistic safety assessment. (PSA). Further details of the deterministic selection of eventaccidentaccident sequences considered in the design extension conditionsDECDEC without significant fuel degradation are providedcancan be found in para.paragraph 3.40 of SSG-2 (Rev. 1) [9].).).

Commented [AKE45]: footnote moved to section introducing DEC, para 3.16

Commented [AKE46]: I have made this change throughout, for consistency.

You could add a footnote to explain different usage in different States, if you want

Commented [AKE47]: can we have this sentence containing a plant state, so it's more connected to the Table, instead of the term 'severe accidents'?

Commented [LHJ48R47]: Agree

conditionsand for safety assessment to be applied for DEC and the set of rules to be applied for design basis accidents, both in the design and in the safety assessment.

3.43.7 to DBA. Despite theirthethe differences, both of thesethosethose approaches aresupportsupport, in compliance with para. 5.29 (a) of SSR-2/1(Rev. 1) [1] [1] and support,], the implementation at the design stage, to the extent practicable, of the independence among safety systems, safety features for prevention of severe accidents and safety features for mitigation of events considered in the design extension conditionssevere accidents.

TABLE Table 1: LEVELS OF DEFENCE IN DEPTHLevels of Defence in Depth

Level of defence Approach 1	Objective	Essential design means	Essential operational means	Level of defence Approach 2
Level 1	Prevention of abnormal operation and failures	Conservative Robust design and high quality in construction of normal operation systems, including monitoring and control systems	Operational limits and conditionsconditionsrulesconditionsrules 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
Level 3 3a	Control of design basis accidents	SafetyEngineered safety features (safety systems)	Emergency operating procedures	Level 3
Level 3 3b	Control of design extension conditions to prevent core melting	Safety features[10] for design extension conditions without significant fuel degradation[11] core melting	Emergency operating procedures	4a Level 4
Level 4	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features[12] for design extension conditions with core melting[13].	SevereComplementary emergency operating procedures/ severe accident management guidelines	4b

Commented [AKE49]: I would prefer to use the wording in para 5.29(a) of SSR-2/1 (Rev. 1)

Formatted: Space After: 0 pt, Allow hanging punctuation, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Font Alignment: Auto

Commented [AKE50]: this would be the normal term used in the 'plant equipment' definition in the glossary

[10] Safety features is understood as additional safety features for design extension conditions, or safety systems with an extended capability to prevent severe accidents (paragraph 5.27 of SSR-2/1 (Rev. 1)).

[11] 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].

[12] Safety features is understood as additional safety features for design extension conditions, or safety systems with an extended capability to mitigate severe accidents (paragraph 5.27 of SSR-2/1 (Rev. 1)).

[13] 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].

		Technical support centre~~Support Centre~~		
Level 5	Mitigation of radiological consequences of significant releases of radioactive material~~materials~~	On-site and off-site emergency response facilities	On-site and off-site emergency plans and procedures	Level 5

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

Normal operation~~Operation~~ and anticipated operational occurrences~~Anticipated Operational Occurrences~~

~~3.5~~3.8 Operational states comprise two sets of plant states: normal operation and anticipated operational occurrences. Modes of normal~~Normal~~ operation include startup, power operation, shutting down, shutdown, maintenance, testing and refuelling and are~~comprises a series of plant operating modes~~ defined in the documentation governing the operation of the

Commented [AKE51]: only SAMG is used in our SGs. You could add 'complementary EOPs' in a footnote, but actually this is not the right SG for introducing this term (SSG-54 would have been a better place)

Commented [AKE52]: inserted because of IEC comment at CC

Commented [LHJ53R52]: As agreed

Formatted: Heading 3,Second level headers, Indent: Left: 0 cm, Hanging: 1.5 cm, Space Before: 12 pt

Commented [AKE54]: sentence taken straight from DS497.

I prefer this than talking about a 'series' of modes that 'range from' one to another

plant (e.g.such as the operational limits and conditions[14]).Operational Limits and Conditions or the plant Technical Specifications in some Member States) that range from power operation to reactor refuelling. Plant states other than normal operation are reached either directly by the occurrence of a postulated initiating eventevents for the applicable modes of operation or through a failurefailures in mitigating the consequences of such an eventevents in the first place. Their impact on the plant is the main basis for establishing the safety provisions that are necessary at each plant state. For these reasons, this Safety Guide is oriented by the design of safety provisions necessary for each plant state, rather than for each level of defence. In this way, the significance and importance of design extension conditions for the safety approach is emphasized.

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

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

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

(a)(c) Prevent anticipated operational occurrences, once they start, from evolving into design basis accidents arrest the progression of plant transients (i.e., AOO) once they start, to avoid an evolution to design basis accident conditions, for which the actuation of the engineered safety features, safety systems and the application of emergency operating procedures are foreseen.

3.73.10 The reliability of safety provisions required for anticipated operational occurrences should be such that the frequency of transition tointointo a design basis accident is lower than the value Consistent with of the highest frequency of postulated initiating events for design basis accidents (usually lower than 10^{-2} per reactor-year).), The reliability of safety provisions

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

Commented [AKE55]: footnote taken from DS497

Formatted: Indent: Left: 0 cm, Hanging: 1 cm

Commented [AKE56]: I think you don't need this. What is 'their'?

Commented [LHJ57R56]: design provisions for operational states

Commented [AKE58]: wording from SSG-2 (Rev. 1)

Commented [AKE59]: we don't need this here, it's about the systems needed for DBAs, which are in the next subsection

Commented [LHJ60R59]: No, it is related the role of design provisions for operational states which are designed to prevent the AOO to become DBA, we are not yet in DBA, but preventing them.
I suggest keep it.

~~for anticipated operational occurrences should be such that the frequency of transition into a design basis accident is lower than this value.~~

Design basis accidents~~Basis Accidents~~

~~3.8~~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.**"

~~3.9~~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"

~~3.10~~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 ~~DBAs through the prevention of~~ significant fuel damage and maintaining the integrity of ~~maintain~~ the containment (i.e. by preserving the structural~~functional~~ integrity of the(by ensuring containment structure and maintaining its associated systems[15]). The objective of the safety systems is functions, para. 1.3 of SSG-53 [6]) ~~in order~~ to limit the radiological consequences for~~to~~ the public and the environment to the extent that no additional safety features or off-site protective actions ~~special measures~~ are necessary~~required~~ for the protection of the public.

~~3.11~~3.14 Design basis accidents originated by ~~are~~ postulated ~~events accidents~~initiating events that are not expected to occur during the lifetime of the plant. The most frequent accidents~~events~~ categorized as design basis accidents~~DBAs~~ should have an expected frequency typically below 10^{-2} per reactor-year. Design basis accidents~~DBAs~~ should include both rare and ~~potential~~ single initiating events ~~and also~~as well as ~~-~~frequent single initiating events that failed to be controlled at~~in~~ the second level of defence in depth. The setextentextent of postulated initiating events considered for design basis accidentsinin DBA should cover all challenges to the safety functions and barriers withforfor which the safety systems are designed to cope. Safety with. ~~The operation of safety~~ systems designed to control design basis accidents~~DBAs~~ should rely on automatic actuation and should ~~not~~ avoid the need for ~~involve~~ requiring short term operator

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

Commented [AKE61]: wording here taken from SSG-53

Commented [AKE62]: I think special measures is not a good phrase.

Commented [LHJ63]: In fact it should be
Design basis accidents originated by postulated initiating events that …

Commented [NM64R63]: OK?

Commented [AKE65]: ok?

Is the distinction between
rare single initiating events
and
frequent single initiating events?

Commented [LHJ66R65]: I think rare potential should be kept since it means that those events might happen even with a very low probability.
There is actually a difference between both rare potential events and frequent events. The second comes from AOO which turned wrongly in is management, while the previous is those single IE which are of low frequency.

actions.~~human interventions for a sufficiently long period of time and their reliability should be very high.~~ Safety systems should be designed and constructed (e.g., considering significant conservative margins and sufficient redundancy) as well as maintained to ensure sufficient reliability. Safety design concepts, such as ~~C~~conservative safety margins and redundancy, are required to be applied in their design and construction, and the environmental conditions considered in their a level of reliability (e.g., through qualification programme should correspond toandand/or adequate protection) commensurate with the performance of their intended safety function under the loads and adverse environmental conditions induced by design basis accidents, postulated internal and external hazards~~, postulated internal~~inin-ternal ~~and external hazards~~. Further specific recommendations on therelatedrelated to design of specific safety systems for nuclear power plants are provided in the corresponding Safety Guides [5-8]specific safety guides.~~Safety systems should be designed to ensure their reliable operation under postulated internal and external hazards and prevailing environmental conditions.~~

~~3.12 If the design of the containment is such that in the case of the most limiting DBAs the intervention of cooling or pressure reduction systems (e.g. containment spray) is necessary to ensure the integrity of the containment boundary, such systems should be designed, constructed and maintained to ensure a high reliability, since their failure would not only lead to radioactive releases but also jeopardize the subsequent measures for its mitigation. For the same reason, containment isolation provisions in case of DBAs should also be designed to have very high reliability for ensuring that acceptable limits for radiological consequences are not exceeded and sufficient coolant inventory can be maintained.~~

Design extension conditions

~~3.13~~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.**"

~~3.14~~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."

~~3.15~~3.17 To meet the requirements presented~~described~~ in paras 3.15~~13~~ and 3.16~~14~~, two separate categories of design extension conditions should be identified: design extension

Commented [AKE67]: this is the phrase used in SSG-2 (Rev. 1)

Commented [AKE68]: these are requirements for all items important to safety, I think

Commented [LHJ69R68]: Yes, but then we should mention also diversity, and others. Then text proposed.

Commented [NM70R68]: OK

Commented [AKE71]: I think it confuses to add this. Just keep the focus on DBAs

Commented [LHJ72R71]: The loads are defined by the internal and external hazards. The safety systems should be able to perform their intended function under those loads. I suggest to keep the text

Commented [NM73R71]: It does move the focus from DBAs, but we can keep it.

Commented [AKE74]: ok?

Formatted: Keep with next

conditions without significant fuel degradation[16] and design extension conditions with core melting.[17]

Design extension conditions without significant fuel degradation

3.163.18 A clear process for the comprehensive identification of the design extension conditions without significant fuel degradation to be considered in the design should be developed. The identification of conditions belonging to different plant states is addressed in SSG-2, (Rrev.1) [1][4] [8]. Paragraphs 3.39 to 3.44 of SSG-2 (Rev. 1) [1][9]this guide provide recommendations for the identification of design extension conditions DEC without significant fuel degradation.

3.173.19 In general, the mitigation of design extension conditionsDEC without significant fuel degradation should be accomplished by specific safety features specifically designed and qualified for such conditions. Alternatively, design extension conditions without significant fuel degradationthey can be mitigated by available safety systems that have not been affected by the events that led to the design extension conditionsDEC under consideration and that are capable and qualified to operate under the associatedrelatedrelated DEC environmental conditions. A difference between design basis accidentsDBA and design extension conditionsDEC without significant fuel degradation is established in some Member States in termsconsideration of their frequencies of occurrence.. Very low frequency initiating events are treated as design extension conditionsDEC without significant fuel degradation. In other Member States, design extension conditionsDEC without significant fuel degradation are postulated for complex sequences involving multiple failures, whereas very low frequency postulated initiating events are treated as design basis accidents.DBAs.

3.20 The objective safety analyses of design basis accidentsofinofin DBA and design extension conditionsin DEC without significant fuel degradation share is the similar safetyamesafety objectives, namelynamely, to maintain the integrity of barriers and to prevent core damage or damage to the fuel in the spentirradiated fuel poolstorage (see para paras 7.28 and 7.45 of SSG---2 (Rev. 1) [1]).).). , but they differ in the range of frequencies, in some Member States, or that DEC without significant fuel degradation involve multiple failures in the accomplishment of a safety function.

3.183.21 Design basis accidents and design extensionBoth accident conditions without significant fuel degradation aredifferr also distinguished in termsthe implementation of the application of different design requirements, and in the use of different acceptance criteria, design requirements or approaches for performing safety analysis. Thus, forin design extension conditions without significant fuel degradation the following apply:

(a) Less stringent design requirements than for design basis accidents might be DBA can may be applied:, for example, safety features equipment required for design extension

[16] 'Design extension conditions without significant fuel degradation' are also termed 'design extension conditions without core melting'.

[17] 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).

Commented [AKE75]: don't you think we should add this footnote from SSG-2 (Rev. 1)?

Commented [LHJ76R75]: It was proposed for clarification, I do not think it leads to any contradiction here.

Commented [NM77R75]: I think that both footnotes need to be included.

Commented [YJ78]: Following a WNA proposal

Commented [AKE79]: in all other standards this is called the spent fuel pool. If you want to show that this has another name sometimes, you could add a footnote

Field Code Changed

Commented [AKE80]: correct change?

Formatted: Font: 12 pt

Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 1 cm, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0.63 cm

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: English (United States)

Formatted: English (United States)

conditionsDECDEC, without significant fuel degradation may be assignedareare allowed to have a lower safety class than safety systems;,, ~~compliance with~~ the single failure criterion is applied at the function level (i.e. functional redundancy) but isandand not appliedrequiredrequired at the system level (i.e. no system redundancy among systems is applied);and supporting~~is not required~~), but to the extent practicable, support systems (~~i.e.~~e.g. cooling systemsourcesource) and I&C systems (~~i.e.~~e.g. the signal for anticipated transients without scram signal) may be more diversified than supporting systems and I&C systemswithwith regard to those used for design basis accidentsDBADBA and~~equipment having a lower safety class and less rigorous reliability measures are allowed~~;

(b) Less conservative assumptions ~~and criteria~~ than for design basis accidents~~DBA~~, or best estimate methods, are acceptable for the safety analysis (see para paras 7.35 to 7.44 and 7.47 to 7.55 of SSG-2 (Rev. 1) [1][~~9~~][1][~~4~~][1][~~4~~]);[1][~~4~~][1][~~4~~]);~~:~~

~~(b)~~(c) The acceptable criteria related to the Identical or similar radiological consequences ~~limits as for releases of radioactive material~~ for design extension conditions without significant fuel degradation may be identical or similar to those for design basis accidents~~, but the~~DBADBA, whereas ~~acceptance criteria used for design extension conditions without significant fuel degradation may be~~ may be ~~similar to or less conservative than the acceptance criteria for design basis accidents~~ (see para paras 7.32 to 7.33 and 7.46 of SSG-2 (Rev. 1) [1][~~9~~][1][~~4~~][1][~~4~~]).

~~3.19~~3.22 If~~Where~~ it is possible to use~~utilise~~ available safety systems ~~(provided primarily for DBAs)~~ to respond to design extension conditions~~DEC~~ without significant fuel degradation, safety analysis is still required to demonstrate their effectiveness: see Requirement 42 of SSR-2/1 (Rev. 1) [1]. The safety. ~~This~~ analysis ~~should~~ may use less conservative methods and assumptions than ~~required~~ for design basis accidents~~DBA~~ (otherwise there would be no differentiation between design basis accidents~~DBA~~ and design extension conditions without significant fuel degradation). Nevertheless, there~~DEC).DEC). There~~ should still be high 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 7.54 to 7.55 of SSG---2 (Rev. 1) [1]).

3.23 Design extension conditions ~~As indicated in para. 3.17, DEC~~ without significant fuel degradation have the potential to exceed the established capabilities of safety systems. ~~designed for the mitigation of DBAs.~~ However, design basis accidents are~~the analysis of DBAs is~~ required to be analysed in a conservative manner: see para. 5.29 of SSR-2/1 (Rev. 1) [1].~~carried out conservatively to demonstrate compliance with established acceptance criteria.~~ Therefore, for design extension conditions without significant fuel degradation~~the conditions described in para.~~ paragraphs 3.39 to 3.44 in SSG-2, (Rrev.1) [1][~~4~~] ~~3.17 (a)~~ it might~~may~~ be possible to show that some safety systems, with ~~conservative~~ an extended capability capacity ~~margins~~ embedded in their design, would be capable of, ~~(~~and be qualified for,,),) mitigating the conditions~~event~~ under consideration, based on best estimate analyses and on less conservative assumptions than the assumptions used for design basis accidents.

~~3.20~~3.24 As ~~. As indicated in para. 7.46 of SSG-2 (Rev. 1) [8], the same or similar technical and radiological criteria as those~~ for design basis accidents, ~~F~~for design extension ~~may be~~

Formatted ...

Commented [AKE81]: it's not clear whether 'to the extent practible' fits with the single failure criterion example, or with the diversified support systems example

Commented [AKE82]: is this i.e.? Is it the only relevant support system?

Commented [LHJ83R82]: It is not really the cooling system, it is the cooling source, cooling system might be associated to HVAC, which could be also diversified, but here the example is the cooling source, which is different than for safety systems used for DBA.

Formatted: Font: 12 pt

Commented [AKE84]: is this i.e.? is it the only relevant I&C system?

Commented [LHJ85R84]: It is an example

Commented [NM86R84]: Then e.g. instead of i.e.

Formatted ...

Formatted ...

Formatted ...

Formatted: Font: 12 pt

Commented [AKE87]: is this what is meant by 'radiological limits'?

Commented [LHJ88R87]: It should be "The acceptable criteria related to the radiological consequences…"

Commented [NM89R87]: ok

Commented [AKE90]: below you say that the acceptance criteria are the same as or similar to

Commented [LHJ91R90]: Text deleted to avoid confusion

Commented [NM92R90]: ok

Formatted ...

Formatted: Font: 12 pt

Commented [AKE93]: if you use 'required' in this sentence, you need a confirmation of the source of why it is a requirement

Commented [LHJ94R93]: OK

Commented [AKE95]: ok to delete? it doesn't seem to be a requirement

Field Code Changed

Commented [AKE96]: I don't know if this is the right word, but you do need some word here. It it not that DEC would exceed the *actual* capabilities; only the capabilities that have been determined in the analysis

Commented [AKE97]: I don't think you need this bit to make the argument in this para

Commented [AKE98]: actually, the conditions are only described in 3.40 and 3.41. The other paras in this range describe how to identify them. Better just call them DEC ...

Commented [AKE99]: see 5.27 of SSR-2/1. 'capacity' ...

Commented [AKE100]: new topic=new para. But is ther ...

~~considered for these~~ conditions without significant fuel degradation, radioactive~~to the extent practicable. Radioactive~~ releases should be minimized as far as reasonably achievable.

~~3.21~~3.25 Anticipated operational occurrences and design basis accidents combined with ~~multiple~~ failures in safety systems should be considered as part of the list of design~~Design extension conditions~~DEC without significant fuel degradation; ~~should be considered for failures of safety systems designed both to cope with anticipated operational occurrences and DBAs~~ (see para. 3.40~~1(b)~~41 of SSG-2 (Rev. 1) [9]. In 8]. ~~These include in~~ many plant designs, such conditions include ~~the~~ anticipated transient~~transients~~ without scram and station blackout, i.e. ~~(defined in SSG-34 as~~ loss of the preferred power supply concurrent with a turbine trip and unavailability of all standby AC power supplies (see SSG-34 [7]).~~)~~".

~~3.22~~3.26 ~~Design extension conditions~~DEC without significant fuel degradation should also be considered to identify provisions to be implemented to reduce ~~to acceptable levels~~ the frequency of severe accidents caused by failures of safety systems. Such provisions should include~~in the mitigation of some DBAs to acceptable levels by~~, if possible, ~~the use of~~ additional, diverse measures to cope with common cause failures of safety systems.

~~3.23~~3.27 Consideration of design~~Design extension conditions~~DEC without significant fuel degradation reinforces~~contribute to~~ achieve the fundamental safety objective by~~a reinforce~~ingement of the robustness of the design to cope with ~~for~~ some complex and unlikely failure sequences and balancesbalancingbalancing the overall risk profile of the plant. Therefore, the~~As some safety systems are designed to cope with various DBAs (e.g. the emergency core cooling systems are designed for several sizes and locations of loss of coolant accidents or main steam line breaks), safety features for DEC can help to reinforce the capability of the plant for specific sequences improving and balancing the risk profile: applying less stringent design or safety assessment criteria than for DBA conditions could help to identify reasonably practicable provisions to improve safety. t~~~~The~~ reliability of safety systems and safety features for design extension conditionsrequiredrequired to cope with DEC without significant fuel degradation should be sufficiently high that ~~enough~~, such as the escalation to a severe accident ~~for DEC without~~severe accidents ~~significant fuel degradation to only be postulated~~ is very unlikely to occur.~~exceptionally and to occur with a very low frequency.~~

Design extension conditions with core melting

~~3.24~~3.28 In accordance with para. 5.9 of SSR-2/1 (Rev. 1) [1],~~]~~ and with consideration of ~~R&D~~ results from research and development, a set of representative accident conditions~~accidents~~ 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~~accidents~~ should be considered in the design of ~~the corresponding~~ safety features for design extension conditions with core melting~~DEC~~ and should represent~~be a set of~~ bounding cases that envelop other severe accidents with more limited degradation of the core.

3.29 Paragraph~~In accordance with par.~~ 6.68 of SSR-2/1 (Rev.~~,~~ (R~~rev~~. 1) [1] states [footnote omitted]:

Commented [LHJ101]: What is "acceptable levels the frequency of severe accidents"?
I think the word "acceptable" will be highly controversial here. I would prefer to avoid that.

Commented [NM102R101]: ok

Commented [AKE103]: I think it's better to say failure of an *item* than failure of a *function*

Commented [LHJ104R103]: OK

Commented [AKE105]: it's not that the DEC itself does this, but considering DEC does

Commented [LHJ106R105]: OK

Commented [AKE107]: we hope that everything here contributes to achieving the fundamental safety objective. No need to state it explicitly

Commented [LHJ108R107]: Agree

Commented [LHJ109]: We had a lot of discussions with the adjectives modifying the term "reliability". Here we use "sufficiently" instead of "enough", I hope it will be acceptable for all.

Commented [NM110R109]: Ok

Commented [AKE111]: it's not clear what it's corresponding to. I think you don't need this

Commented [LHJ112R111]: Therefore, we need to specify which DEC we are mentioning here

Commented [NM113R111]: ok

"For], for reactors using a water pool system for fuel storage, it should be demonstrated that 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."

3.25 .Hence, significant fuel degradation in the spentirradiated fuel pool shouldstorage is not be postulated as part of this set of a design extension conditions; rather it is required to be considered among the conditions to be practically eliminated (see Section 5). condition.

3.263.30 The accident conditions chosen as design extension conditions with core melting should be justified based on the basis of engineering judgement and insights from the probabilistic safety analyses: see SSG-53 [65] and SSG-2 (Rev. 1) [9I8]. A detailed analysis should be performed and documented to identify and characterize both accident conditionsaccidents that couldcan lead to core damage and alsoaccident conditions that can also challenge or bypass the containment. All accident conditions that could leadFor nuclear power plants designed according to SSR- 2/1, (Rrev. 1) [1], accidents involving core damage melting should be postulated as design extension conditions, even though DEC, irrespective of the fact that the design provisions taken in accordance with the requirements of SSR-2/1 (Rev. 1) [1] to prevent such accidents will conditions make the probability of core damage very low. Aspects that affect the accident progression and that influence the containment response and the source term should be taken into account in the design of the safety features for design extension conditions with core melting: see para. 3.42 of , as indicated in SSG-53 [65].

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

3.283.32 The challenges to plant safety presented by design extension conditionsDEC with core melting, and the extent to which the design may be reasonably expected to mitigate their consequences, should be considered in establishing procedures and guidelines. Recommendations in this regard are provided in IAEA Safety Standards Series No. SSG-54, Accident Management Programmes for Nuclear Power Plants [1514]

3.33 Radioactive releases from the containment in a severe accident should remain below the safety limit to allow sufficient time for implementation of off-site protective actions. Beyond this time, releases mightcould exceed the safetythis limit but should still be well below the acceptable limits for design extension conditions limit with off-site protective actions in place. Radioactive releases should also and be well below what is considered a large radioactive release. Moreover, as stated in para 4.100 of according to SSG-53 [6]:

"At[5], "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)".

Formatted: No bullets or numbering

Commented [AKE114]: is this what you are saying? is it ok to say it so directly?

Commented [LHJ115R114]: Agree, but it should be specified that we are indicating the DEC with core melting here, since the other set of DEC include the accidents in the spent fuel pool

Commented [AKE116]: this sentence is about two sets of accident conditions, right? (i.e. not accident conditions that can BOTH lead to core damage and challenge the containment)

Commented [LHJ117R116]: It is indeed to identify those accident conditions leading to core damage and that might also have containment bypass. As mentioned in para. 4.13 of this SG. Therefore, I suggest to keep "also" and delete the following text

Commented [NM118R116]: Put 'also' back in and now I think it should be ok with you.

Commented [AKE119]: let's repeat the prhase in the previous sentence, to show the connection

Commented [LHJ120R119]: OK

Commented [AKE121]: maybe it's not a FACT, per se

Commented [LHJ122R121]: OK

Commented [AKE123]: this is an important point and worth having as a separate sentence

This may be achieved by provision of adequate filtered containment venting or other design features or alternative measures.

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

> ~~3.29~~ "Multiple ~~that could be included in an overall demonstration of adequacy of the containment~~ confinement ~~function. If a containment venting system is included in the design, it "should be used only as a last resort" after off-site protective actions have been implemented~~ and~~.~~ ~~"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]"~~." according to SSG-53 [5].~~

~~3.30~~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~~addressing~~ applicable topical issues. More detailed information on the range of physical processes that could occur following core damage is provided in para~~par~~. 7.66 of SSG-2 (Rev. 1) [~~9~~8].

ASSESSMENT OF THE IMPLEMENTATION OF ~~THE~~ DEFENCE IN DEPTH ~~CONCEPT~~

~~3.31~~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~~is~~ adequately designed to meet the objectives of that level~~its goals~~ in terms of prevention, detection, limitation and mitigation. Requirement 13 of GSR Part 4 (Rev. 1) [3]~~2],~~ states:

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

~~3.32~~3.37 Paragraphs~~Paras~~ 4.45–4.48A of GSR Part 4 (Rev. 1) [3] establish~~2] contain~~ additional requirements on ~~this~~ assessment of defence in depth.

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

~~3.34~~3.38 The performance and reliability of safety provisions for all~~different~~ plant states should be assessed, taking into consideration an applicable set of analysis rules, the level of risk and the~~their~~ safety significance of the safety provisions. The~~. Such~~ safety provisions should be designed to maintain the integrity of the barriers to the extent necessary for the relevant plant state, or to mitigate the consequences of postulated failures. The assessment should provide evidence that the performances and reliability of the safety provisions associated with ~~corresponding to~~ each level of defence in depth is adequate. The assessment~~It~~ should demonstrate that, for each ~~credible postulated~~credible initiating event, the risk has been reduced

Commented [AKE124]: I don't think you need this, it just distracts

Commented [AKE125]: deleted based on IEC comment at CC. The rest of the deletions are replaced with the quoted text below

Formatted: Indent: Left: 1 cm, No bullets or numbering

Commented [AKE126]: this quote added following agreement on CC comments

Commented [AKE127]: does it make sense that a safety assessment addresses applicable topical issues? maybe you mean something other than topical issues?

Commented [LHJ128R127]: I agree with the proposal.

Commented [AKE129]: I think it's the safety provisions that are designed, not the level

Commented [AKE130]: yes?

Commented [LHJ131R130]: Postulated IE are analysed on the DBA, credible IE are analysed in PSA, which also covers postulated IE. The safety assessment should cover all, then credible is appropriate.

Commented [NM132R130]: Put 'credible' back in.

to a level that is as low as reasonably achievable~~practicable~~, considering also all consequences of internal hazards and~~/or~~ 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~~analysis~~, as appropriate for each~~the~~ different plant state~~states~~.

~~3.35~~3.39 The~~The correct implementation of the requirements implies that the~~ multiplicity of the levels of defence is not a justification to weaken the effectiveness ~~efficiency~~ of some levels by relying on the effectiveness~~efficacy~~ of other levels. In a sound and balanced design, structures, systems and components at~~SSCs of~~ each level of defence are characterized by a reliability commensurate with~~to~~ their function and their safety significance, and~~providing~~ reasonable safety margins are provided.

~~3.36~~3.40 The defence in depth concept~~strategy in the design of a nuclear power plant~~ should be applied for~~to~~ all ~~radioactive~~ sources of radiation present in the nuclear power plant~~that could potentially harm plant personnel or the public, or contaminate the environment, taking into account a graded approach (see 3.1).~~ The following are examples of sources of radiation likely to ~~that should~~ be present in a nuclear power plant~~considered~~:

- The reactor~~Reactor~~ core;
- Fresh nuclear fuel, irradiated~~spent~~ fuel and fuel casks;
- Neutron sources and other radioactive sources;
- Airborne radioactive material~~activity~~ 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~~HVAC of the~~ controlled areas, gas and liquid effluent treatment systems, solid waste treatment systems).

~~3.37~~3.41 For ~~radioactive~~ sources of radiation other than the reactor core and the nuclear fuel, defence in depth should be implemented in accordance with ~~following~~ a graded approach, with ~~appropriate~~ account taken of the fact that ~~many radioactive sources do not qualify for~~ all five levels of defence in depth will not be appropriate for many sources of radiation within the plant. Account should~~.. For consistent implementation, account needs to~~ be taken of the risk represented by the amount and type of radioactive material present~~; in the nuclear power plant,~~ the potential for its dispersion owing~~due~~ to its~~the~~ physical and chemical nature~~ of these products~~; and the possibility of nuclear, chemical or thermal reactions that could occur under normal or abnormal conditions and the kinetics of such reactions~~events~~. These characteristics will differ for different sources of radiation and will influence the necessary~~required~~ number of levels of defence in depth and the strength of each level~~these levels, de pending on the radioactive source~~.

~~3.38~~3.42 The physical barriers included in the design~~within a facility~~ are an important consideration when assessing the adequacy of the implementation of the defence ~~pth~~ in depth~~. implementation.~~ For each identified source of radiation, the physical barriers (including the reactor coolant pressure boundary and the containment boundary) ~~boundaries)~~ should be identified and ~~an evaluation of their~~ the robustness of their designs should be evaluated in

Commented [AKE133]: I'd prefer to use the wording in para 4.4 of GSR Part 4

Commented [AKE134]: I would use 'effectiveness' in both of these cases. Why 'efficacy'? it's an unusual word, and means something like 'effectiveness in an ideal world'

Commented [AKE135]: radioactive source is a bit misleading for a great big reactor core

Commented [AKE136]: I think you should drop this. It means an assessment should be made straight up as to whether the source is harmful

Commented [AKE137]: lots more about graded approach in the next para, no need to bring it in here

Formatted: Space After: 0 pt

Commented [AKE138]: yes?

Commented [AKE139]: if you're using event as a synonym for accident elsewhere, maybe reactions is better here

Commented [AKE140]: I think boundaries might not be clear, the word 'boundaries' not used in other design standards like this. Can you specify to these 2? Or are there other boundaries? (or delete the bit in brackets?)

Commented [LHJ141R140]: The specifications are good.

Commented [AKE142]: you have graded approach in bullet (a) below

Commented [LHJ143R142]: text added

accordance with~~provided taking into account~~ a graded approach. The following aspects should be assessed~~taken into account~~ in the evaluation:

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

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

(c) All loads and combinations~~combination~~ of loads that can apply to the barriers in operational states and accident conditions, including loads caused by the effects of the internal hazards and external hazards considered in the design, should be identified 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 assessment of defence in depth should demonstrate that the~~ 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 ~~that is~~ used in the barriers~~barrier boundary~~ to prevent radioactive releases ~~to prevent radioactive releases release~~ should be~~have been~~ designed to ensure structural~~barrier~~ integrity of the barriers in accident conditions.

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

~~3.39~~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~~or~~ stop their~~the~~ progression~~. of such mechanisms.~~ To the extent that different degradation mechanisms could necessitate different safety provisions, the adequacy and effectiveness of each~~every~~ safety provision should be assessed for each degradation mechanism.

~~3.40~~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~~, operational occurrences, DBA, DEC without significant fuel degradation and DEC with core melting, which~~ should be characterized by a type of ~~transient~~ safety analysis, with an applicable~~associated~~ set of analysis rules, level of conservatism and acceptance~~safety~~ criteria. Recommendations on conducting deterministic safety analyses for the different plant states are provided in SSG-2 (Rev. 1) [~~8~~9].

~~3.41~~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

Formatted: Space After: 0 pt

Commented [LHJ144]: It is important to assess the barriers regarding the DiD, I do not see why it should be deleted the text.

Commented [AKE145]: ok to delete?

Commented [LHJ146R145]: Agree

Commented [AKE147]: not necessary, I think. we know already from above what the barriers are for

Commented [LHJ148R147]: I do not agree, the text "to prevent radioactive releases" should be there since there are many valves in each system but not all have the function to prevent radioactive release.

Commented [NM149R147]: We put it back to specify the function of the valves.

Formatted: Space After: 6 pt

Commented [AKE150]: OK? broader than safety criteria. See also usage in next para

Commented [LHJ151R150]: Agree

validated and verified computeranalysis codes and models to demonstrate that acceptance criteria are met and that there are sufficient margins to avoid cliff -edge effects. Further recommendations are (further guidance is provided in paras 5.14-5.39 of SSG-2 (Rev. 1) [9].8]).

3.423.46 The reliability analysis of safety provisions for the different plant states, as indicated in para. 3.3934, 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, manufacturemanufacturing, maintenance and testing ofbetween redundant and diverse equipment.

3.433.47 Statements of reliability should be supported by equipment reliability data thatwhich is shown to be relevant to the structure, system or component installation being assessed, as well as supported by to test data, the use of proven technologies and engineering practices, and feedback from operating experience. Statements ofThe reliability should also be supported by verification of compliance of the structure, system or componentSSC 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 analyses assessment to evaluate overall plant risk metrics, such as core damage frequency or frequencies of early radioactive releases or large radioactive releasesearly release frequencies.

3.443.48 It should be verified that adequate diversity has been implemented in the design of systems fulfilling the same fundamentalfundamental 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.

3.453.49 The reliability of structures, systems and componentsEequipment for required for controlling anticipated operational occurrences should be such that they are capable of is aimed at reducing the number of challenges to safety systems and of contributing to preventingpreventprevent the occurrence of design extensionDEC.DEC. It should be demonstrated that their reliability is such that anticipated operational occurrences only evolve into DBA conditions with a low frequency, below the highest frequency of postulated initiating events categorized as DBAs, and the safety systems to manage such a situation are available.

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

3.473.51 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,if in combination with a postulated initiating event,events they could escalate to a core melt accident. Foraccidents. Usually, for each such combination analysed, if the consequences exceed those acceptable for design basis accidentsDBAs, and mightmay cause a core melt with unacceptable frequency, separate, independent and diverse safety features, which are unlikely to fail by the same

Commented [AKE152]: this is the phrase in SSG-2 (Rev. 1)

Commented [LHJ153R152]: Agree

Commented [AKE154]: or plant?

Commented [LHJ155R154]: SSC is better

Commented [AKE156]: supported by…?
or relevant to…?

Commented [LHJ157R156]: "Supported by" is better

Commented [AKE158]: OK?

Commented [LHJ159R158]: Fundamental safety function is more general, since systems can fulfil several safety functions related to one or more fundamental safety functions.
I suggest keeping "fundamental"

Commented [LHJ160]: I agree to add unacceptable but, we need to agree to use " unacceptable radiological consequences" or "unacceptable radioactive releases" or are they equivalent, then it should be mentioned.

Commented [YJ161]: Agreed with France after the meeting

Commented [AKE162]: I've turned this into a straightforward should statement. OK?

Commented [LHJ163R162]: Great, agree.

Formatted: Font color: Auto

common cause, should be implemented (e.g. an alternate AC power supply in case of athe total loss of the emergency power supply, or a separate and diverse decay heat removal chain).), which are unlikely to fail due to the same common cause, need to be implemented to strengthen the defence in depth and to prevent core melt.

3.483.52 Safety features for DEC without significant fuel degradation should be demonstrated to be efficient enough according to the applicable analysis rules to prevent core damage for the accident sequences for which they are intended and sufficiently reliable in order to contribute to ensuring a core damage frequency below the established probabilistic targets.The reliability of safety features considered for design extension conditionsDECDEC without significant fuel degradation should be such that it cancouldcould be demonstrated, with a sufficient level of confidence and considering applicable analysis rules (see paras 7.45-7.55 of SSG-2 (Rev. 1) [1]), that they are capable of preventingtoto prevent core damage with a frequency higher than the established probabilistic targets.

3.493.53 The capability and reliability of safety features for design extension conditionsspecifically designed to mitigate the consequences of DEC with core melting should be sufficientadequate to ensure that the integrity of the containment integrity 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 integrity is associated withsurrounded by considerable uncertainties, the reliability claimed for suchthese safety features should be considered with cautioncautiously in consideration of these uncertainties.

3.503.54 It should be demonstrated that the reliability of safety systems and safety features for design extension conditionsDEC is not limited by the reliability of their supportingits support systems.

INDEPENDENCE BETWEEN LEVELS OF DEFENCE IN DEPTH

3.513.55 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."

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

Commented [AKE164]: this section had a lot of repetition and disordered presentation of ideas. But I hope the changes haven't removed the technical intent

Commented [AKE165]: we don't need to justify why independence is a good thing. It's enough that it's a requirement. Also – it doesn't really add much in the way of technical information about the value of indpeendence

Commented [AKE166]: I have pulled Req 64 and Req 69 up into this beginning part of the section – they're also quoted below and are good supporting requirements

> "**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 24 of in SSR-2/1 (Rev. 1) [1] states:~~ 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.**"

~~3.53~~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.**"

~~3.54 Because of these factors, Defence in depth is an essential pillar of nuclear power plant safety. It is used to organize the safety related architecture of the plant and to identify, for each plant state, the corresponding safety requirements. To apply the defence in depth principle, it needs to be ensured that, as far as practicable, the failure of a given level does not affect the robustness of the next level. For example, a failure, whether equipment failure or human error, at one level of defence, should not propagate to jeopardise defence in depth at the subsequent levels. Engineering assessment, deterministic and probabilistic methods should be used to assess this independence.~~

~~3.55~~3.58 ~~It is recognized in the IAEA safety standards that~~ full independence of the levels of defence in depth cannot be achieved. ~~This is due to several factors and constraints, such as a potential common exposure to the effects of external hazards and/or internal hazards, an unavoidable sharing of some items important to safety, e.g. the containment, as well as human factors.~~ The design of a nuclear power plant should consider all potential causes of dependencies and ~~implement~~ an approach should be implemented to remove them to the extent reasonably practicable. Robust independence ~~is essential and~~ should be implemented among

Formatted: No bullets or numbering

Formatted: Font: Not Bold

Commented [AKE167]: several reasons to delete this: it's not the right place for explaining what DiD is, the terminology (e.g.the word pillar) is not usual for the standards, it repeats ideas from SCOPE

Commented [AKE168]: this sentence is a repetition of para 4.13A, using a should statement

Commented [AKE169]: this sentence just abbreviates what you go into detail on later, hence deleted

Commented [AKE170]: repeated above

systems whose simultaneous failure would result in conditions having harmful effects for people or the environment. For this reason, in paras 4.13A and 5.29 of SSR-2/1 (Rev. 1) [1] it is stated that 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 practicable, be independent of safety systems. It is necessary to demonstrate that the effectiveness of the levels of defence is not reduced by factors that compromise the independence of the levels of defence in depth. These factors include the following:

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

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

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

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

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

3.57 As far as practicable, the sharing of systems or parts of them for executing functions for different categories of plant states should be avoided. However, since this might not be always practical or possible, it should be ensured that within the event sequence of events that mightmay follow a postulated initiating event, a system credited to respond in a given plant state willcondition should not have been needed for a preceding plant state. As emphasized in para. 4.13A of SSR/2-1 (Rev. 1) [1], this condition.condition. This is especially important when safety systems are to be credited for the mitigation of design extension conditions (see para. 3.65).DEC.

3.583.59 The SSCs needed for each postulated initiating event (PIE) should be identified, and it should be shown by means of engineering analyses that the SSCs needed for implementing any one defence in depth level are sufficiently independent from the other levels. It should be taken into account that a PIE is generally a bounding event covering different kinds of initiating failures and it may be difficult to list exactly all the normal operation equipment that may be initially affected by the PIE in a given DEC accident sequence. For this reason, the credit of normal operation systems in the safety assessment of DEC should be considered with extreme caution and adequately justified. The adequacy of the achieved independence should also be assessed by probabilistic analyses.

Commented [AKE171]: don't need to justify why a requirement says what it says

Formatted: No bullets or numbering

Commented [AKE172]: moved up to the early part of this section

3.60 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."**

And Requirement 24 of 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."**

~~3.59~~ Therefore, systems and components within the same safety division[18] and required for different plant states should be protected from one another by physical separation or protective structures, as appropriate, to ensure they can perform their intended function in a situation where it is ~~The systems and components used for different plant states should be separated, within the same safety division, from one another by distance or protective structures if there is a possibility that a failure of a system or component of one safety division impairs the fulfilment of a safety function by the same safety division for another plant state in a situation where it is required.~~

~~3.60~~3.61 The systems needed for different plant states ~~in accordance with the defence in depth concept~~ should be functionally isolated from one another in such a way that a malfunction or failure in any plant state does not propagate to another. However, practical limitations of design necessitate ~~allow~~ exemptions to such functional isolation, ~~,~~ each of which should be justified. Thus, it is a common practice to use some safety systems for certain~~some~~ anticipated operational occurrences. For example, the intervention of the protection system might~~may~~ be necessary to shut down the reactor for some anticipated operational occurrences that cannot be controlled by the limitation system. For most reactor designs, the reactor trip system is a safety system that is also needed for the control of some anticipated operational occurrences.~~AOOS~~.~~AOOS~~. In such cases, it should be shown that there is no practicable alternative to use of the safety system to cope with the anticipated operational occurrence, and that the use of the safety system for such an occurrence does not present a significant limitation on the use of the safety system to mitigate a design basis accident~~DBA~~.

~~3.61~~3.62 The systems intended for mitigating severe accidents should be functionally and physically separated from the systems intended for other plant states. However, safety~~Safety~~ features for design extension conditions~~DEC~~ with core melting may, for good reasons, also be used for preventing severe core damage if it can be demonstrated that such use~~this~~ will not undermine the ability of these safety features~~systems~~ to perform their primary function if

[18] Safety divisions may group redundant safety systems and their support and auxiliary systems. The redundancy concept is applied to safety systems among different divisions to prevent their impairment due to a single failure, since they are required to perform the same intended safety function.

Commented [AKE173]: repetition of earlier quotes

Commented [AKE174]: I am not sure why you need this short para – it just repeats the requirement, and the you have to explain the word 'safety division', which you don't use elsewhere in the text, hence para and footnote deleted

Formatted: Font color: Text 1

Formatted: Font: Bold

Formatted: Font: 12 pt

Formatted: Font: Bold

Formatted: Indent: Left: 0.25 cm, Hanging: 0.63 cm

Formatted: Font: Bold

Formatted: Indent: Left: 1 cm, No bullets or numbering, Don't keep with next, Don't keep lines together

Formatted: No bullets or numbering

Commented [AKE175]: I think necessitate? not allow

Commented [AKE176]: I think the example you are bringing now is the opposite of the recommendation, right?

Commented [LHJ177R176]: Agree

conditions do evolve into a severe accident. As an example, ~~(e.g.~~ a power supply intended for design extension conditions~~DEC~~ with core melting could be used,~~connected~~ if necessary, to power equipment for design extension conditions~~DEC~~ without significant fuel degradation.~~).~~

ASSESSMENT OF THE INDEPENDENCE OF THE LEVELS OF DEFENCE IN DEPTH

3.63 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.

~~3.62~~ The assessment~~For instrumentation and control systems, it should be demonstrated that adequate independency is achieved (see notably requirement 64 of SSR-2/1 rev.1[1]). Further recommendations are provided in SSG-39 [7].~~

~~3.63~~3.64 ~~The assessment of the implementation of defence in depth~~ should demonstrate that independence between successive levels of defence is adequate to limit the progression of deviations from normal operation and to prevent harmful effects to the public and the environment if an accident occurs. The ~~should accidents occur. For this purpose, the~~ assessment of the independence~~implementation~~ of the levels of defence in depth should aim to verify that the vulnerabilities for common cause failures between structures, systems and components~~, originated in the layout, design, manufacturing, operation and maintenance, between SSCs~~ 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. In addition~~In particular~~, functional dependence between structures, systems and components~~dependencies~~ should be removed or justified.

~~3.64~~3.65 The assessment should demonstrate that ~~the~~ safety ~~features~~ 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~~the event if escalating to a DBA~~.

~~3.65~~3.66 The assessment should demonstrate that a failure of a supporting~~support service~~ 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

Commented [AKE178]: Consider adding a subheading here

Commented [AKE179]: the assessment of the implementation of defence in depth was the previous section

Commented [LHJ180R179]: previous section was related to considering independence of levels of DiD at design, here we assess how that achieved.

Commented [AKE181]: I think functional dependence is not a particular example of CCF? in appendix 3 of TECDOC 1971 they seems to be classified as different types of dependence

Commented [LHJ182R181]: Independently of what it is mentioned in TECDOC 1791, functional dependencies are a root cause of CCF, e.g. loss of electric power supply leads to loss of all systems depending on it.
I suggest to keep the text.

independence of supporting systemsthe support service is commensurate with the significance to safety of the system being supported.

3.663.67 An assessment should be conducted of the independence of structures, systems and componentsSSCs that mightmay be necessary at different levels of defence in depth to mitigate the consequences of a single hazard or a likely combination of internalinexternalinexternal or externalinexternal hazards (natural and human induced hazards) on the plant. should be conducted. It should be demonstrated that the postulated initiating event and the failures induced in the plant cannot result in common cause failure of the structures, systems and componentsbetween the SSCs necessary for its mitigation of the hazard at different levels of defence in depth. In particular, the necessary safety features for design extension conditions for core melting should always remain available.

Commented [AKE183]: not needed

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

4.1 Paragraph The concept of practical elimination is introduced in para. 2.11 of SSR-2/1 (Rev. 1) [1]], which states [footnote omitted]:

> that "Plant event sequences that could result in high radiation doses or in a large radioactive release have to be 'practically eliminated'… An essential …". This is an objective is thatof the necessity fordesign, but as indicated in this paragraph, 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]:

> "Eventalso introduces the expectation that event sequences that would lead to an early radioactive release or a large radioactive release are required towill be 'practically eliminated'."

4.1 Although . The footnotes to the termrelevant paragraph provide further clarification as follows:

> " An 'early radioactive release' is predominantly used in in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the" protection of people and of the environment" (Footnote 3 of SSR-2/1 (Rev. 1) [1], the term '}).
>
> "The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise (Footnote 4 of SSR-2/1 (Rev. 1) [1]).

4.24.3 It should be clarified that "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 " and "early radioactive release,releases" are not fully equivalent terms. Early radioactive releases would result into high radiation doses to the population because protective actions could not be effectively implemented in time to prevent. The term "early radioactive releases" is predominantly used in "SSR 2/1, (rev.1) [1]. When the term "high radiation doses" is used in 2.11 and req. 5 of SSR-2/1 (Rev. 1) [1], it is interpreted to mean as the result of early radioactive releases. This guide refers to early radioactive releases in relation to the practical elimination of the conditions leading to them.

Commented [LHJ184]: To be consistent

Commented [AKE185]: IEC was worried about this usage, but it's definitely better if we just quote the requirement, as above

Commented [AKE186]: these footnotes have been introduced in Section 1 and discussed a lot

Commented [AKE187]: concept moved to end of this para

Commented [YJ188]: Number this paragraph

4.34.4 The concept of RWith regarding the to design, 'practical eliminationelimination' is normally appliedconsidered to refer only to those events or sequences of events that could leadleading to or involveinvolving significant fuel degradation, i.e. a 'severe accidentaccident', for which the confinement of radioactive materialmaterials cannot be reasonably achieved. The practical elimination of such plantThose event sequences is requiredhave to be ensured byconsidered in the design [1],for 'practical elimination', either ensuring that the plant event sequence is physically impossibleby physical impossibility (see also paras. 4.343030–4.353131) or because the plant event sequence is considered, with a high level of confidence, to beby being extremely unlikely to arise (see also paras. 4.363232–4.43).38) to occur with a high level of confidence.

4.5 The concept of 'practical eliminationelimination' should be appliedconsidered as part of the overall safety approach tofor the design of nuclear power plants, as set out in sectionaccordance with Chapter 2 of SSR-2/1 (Rev. 1) [1]. As a result of the implementation of the first, second, third and fourthfour levels of defence in depth, the likelihood of an off-site radioactive release that could potentially resultreleases resulting from an accident will the failure of the prevention and mitigation of severe accidents should be very low. However, it is necessary to verify that there would not be credible plant conditions that could notcannot be effectively mitigated and which could thus lead to unacceptable radiological consequences. This is where the aim of the 'practical eliminationelimination' 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.

4.44.6 radioactive releases'. Practical elimination should not be seen as an alternative to mitigation of the consequences of a severe accident (i.e. implementation of the fourthmitigation: instead, efficient and fifth levels of defence in depth); rather, the application of practical eliminationreliable provisions should be in addition to the provision of safety features for design extension conditions withimplemented, if they are reasonably practicable, to mitigate any core melting, and on-site and off-site emergency response facilities. Moreover, the practical elimination of event sequences that could lead to a large radioactive release or an early radioactive release does not remove the need for emergency preparedness and responsemelt consequence, in accordance with principle 9 of SF-1 [3] and the requirements of GSR Part 7 [12].the defence in depth concept if they are reasonably practicable.

4.7 The concept of practical elimination should be applied only in relation to plant 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, technical means should be considered in accordance with the strategy for accident mitigation at the plant. This would not constitute application of the concept of practical elimination.

4.5 The main issue of a severe accident condition is that there is the potential for having both large quantities of radioactive substances available and not confined in the fuel or by the reactor coolant system, together with severe accident phenomena that can potentially generate large

Commented [AKE189]: it's not a should statement

Commented [AKE190]: this phrase is well established. the phrase 'unacceptable release' is not established, so I have changed it throughout.

Some places I have replaced it with 'large radioactive release or early radioactive release', where it seemed better to emphasise the release itself

Commented [AKE191]: can you link this concretely back to the DiD concept?

Commented [LHJ192R191]: Agree with the text proposed

Commented [AKE193]: this was a comment of the IEC's at the Coordination Committee. They had wanted it in SCOPE, but I think it's better here

Commented [LHJ194R193]: Agree

Commented [AKE195]: moved from below

Commented [AKE196]: make it a should statement

Commented [LHJ197]: It should be "plant event sequences"

amounts of energy and also very rapidly, making it impossible to ensure the containment integrity and thus giving rise to unacceptable releases.

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

4.7 SSR-2/1 (Rev. 1) [1] does not provide quantitative acceptance criteria for the radiological consequences of accident conditions, noror for the magnitude of what is to be considered as a large radioactive release or an early radioactive release or a large radioactive release.. In some Member States an early radioactive release is defined for considering a specific site specific considering restrictions on implementingto implement off-site protective actions in ameasures timely manner. In some Member States, acceptable limits on radioactive releases for purposes of for radiation protection, andas well as probabilistic criteria or target values for the purpose of demonstrating athe low frequency of a core damage accident or accident sequences leading to radioactive releases, have been established, consistent with the any regulatory requirements or objectives. However,It should be noted that the justification that an plant event sequence has been practically eliminated should relyofof the application of the 'practical elimination' concept relies primarily on a deterministic evaluation and should notcannotcannot be solely demonstrated by demonstrating showing the compliance with suchthesethese probabilistic values.

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

4.94.8 criteria.The concept of 'practical elimination' is should be used to demonstrate that adequate provisions have been implemented in the design, across all levels of defence in depth to ensure that plant conditions or event sequences for which a large radioactive release or an early radioactive release could not be prevented, are physically impossible or highly unlikely with a high degree of confidence. Sufficiently robust arguments and evidence are needed to demonstrate the reliability of the lines of defence that are in place. The concept of "practical elimination" is only applied in relation to plant conditions or event sequences that can lead to early radioactive releases or large radioactive releases, for which reasonably practicable technical means for their mitigation cannot be implemented. Otherwise, such means should be considered under the strategy for accident mitigation and would not be part of the application of the concept of practical elimination.

Commented [LHJ198]: It should be plant event sequence

Commented [AKE199]: I think this needs to be a should statement.

Commented [YJ200]: After discussion with France

4.104.9 The conceptAs part of the overall safety approach, the 'practical elimination elimination' concept should be applied into a new nuclear power plant from an early stage, when it isit's more practicable to design and implement additional[19] safety features. The incorporation of such features should beis an iterative process, which should use using insights from engineering experience, and from deterministic safety analyses and probabilistic safety assessmentanalyses in a complementary manner.

IDENTIFICATION OF RELEVANT PLANT EVENTPOTENTIAL SEVERE ACCIDENT SEQUENCES LEADING TO AN EARLY RADIOACTIVE RELEASE OR A LARGE RADIOACTIVE RELEASE

4.10 The first step in demonstrating the practical elimination of plant 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.

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 that can generate large amounts of energy very rapidly. Together, this can make it impossible to ensure the containment integrity, thus giving rise to unacceptable radiological consequences.

4.11 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 a severe accidents. In such cases, it may be necessary to demonstrate practical elimination by justifying proving the physical impossibility of the accident or by proving with a high degree of confidence that such severe accidents would be extremely unlikely.

4.12 Therefore, the issue when considering whether a particular plant event sequence should be to practically eliminated eliminate a severe accident sequence is the potential for the event sequence to lead to a failure of thea confinement function failure.

4.13 To help ensure that the demonstration of practical elimination is manageable, the whole set of individual plant eventaccident sequences that might lead to an unacceptable radioactive release should could be grouped to form a limited number of bounding cases or typestype of accident conditions. TheThus, the following five general types of plant event sequences

[19] Such additional safety features include'Additional' is intended here to describe any design provision that is implemented following an practical elimination assessment supportingto support the demonstration of 'practical eliminationelimination' of some plant accident event sequences. Some, considering that some design provisions will already have been implemented to support other safety objectives and analyses and can also supportparticipate in the demonstration of practical elimination.

Commented [AKE201]: pls check the changes in the footnote

Commented [LHJ202R201]:

Commented [AKE203]: maybe we don't need to repeat this each time

Commented [AKE204]: not when, yikes!

Commented [AKE205]: this sentence has been said many times. Is it different here?

Commented [AKE206]: I think this follows logically from the previous paras?

Commented [LHJ207R206]: Agree

Commented [AKE208]: yes?

shouldcould be considered, depending on their which should be assessed for applicability forto specific designs:

(a) Plant eEvents sequences Events that could lead to prompt reactor core damage and consequent early containment failure, such as:
  (i) Failure of a large pressure-retaining component in the reactor coolant system;
  (ii) Uncontrolled reactivity accidents.

(b) Plant Eevent Severe accident sequences that could lead to early containment failure, such as:
  (i) Highly energetic direct containment heating;
  (ii) Large steam explosion;
  (iii) Explosion of combustible gases, including hydrogen and carbon monoxide.

(c) Plant event Severe accident sequences that could lead to late containment failure, such as:
  (i) Basemat penetration or containment bypass during molten coriumcoriume concrete interaction;
  (ii) Long term loss of containment heat removal;
  (iii) Explosion of combustible gases, including hydrogen and carbon monoxide.

(d) Plant event sequences Severe accidentsaccidentaccident with containment bypass, such as:
  (i) A lossLoss 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)[20]. LOCAs). As the containment function might be jeopardised by the initiating event, any escalation to significant fuel degradation has to be analysed and, where relevant, considered for 'practical elimination';
  (ii) Plant event sequences producing a consequential Ccontainment Containment bypass consequential to severe accident progression (e.g. an induced steam generator tube rupture);
  (iii) A severe accidentplant event sequence with core melt and Severe accident in which the containment is open[21] (e.g. in the shutdown state).

(e) Significant fuel degradation in a spentstorage fuel pool and uncontrolled releases[22].

4.14 The classification and grouping in para. 4.1412 is consistent with the recommendations provided in SSG-53 [65] and SSG-2 (Rev. 1) [9], and highlights8], highlighting some examples

[20] 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'

[21] InCurrentlyOn many LWR designs, the technology used for equipment hatches mightmay not be fast enough to ensure re-closure and restoration of the containment integrity before a radioactivesignificant activity release occurs. Therefore, any significant rapid fuel degradation mechanism in shutdown operating modes with an open containment needs to be considered for 'practical elimination'.

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

Commented [LHJ209]: In the bullets, you suggested to change to "Event sequences" instead of "severe accidents", however we are considering "plant event sequences" for practical elimination therefore for consistency it should be considered the same text everywhere. Then, "severe accidents" term has to be changed to "plant event sequences" according to your suggestion.

Commented [AKE210]: ok?

Formatted: Indent: Left: 0 cm, Hanging: 1 cm

Formatted: Indent: Left: 1 cm, Hanging: 0.75 cm

Formatted: Indent: Left: 0 cm, Hanging: 1 cm

Formatted: Indent: Left: 1 cm, Hanging: 0.75 cm

Formatted: Indent: Left: 0 cm, Hanging: 1 cm

Formatted: Indent: Left: 1 cm, Hanging: 1 cm

Formatted: Indent: Left: 0 cm, Hanging: 1 cm

Formatted: Indent: Left: 1 cm, Hanging: 1 cm

Commented [AKE211]: or e.g.?

Commented [AKE212]: can we delete from this list – it doesn't match the rest of the bullets

Commented [LHJ213R212]: This is the explanation for this type of LOCA that needs to be carefully considered in case of escalation. I suggest keeping the text as it is part of the example.

Commented [LHJ214]: Could (ii) be:
Plant event sequences producing a consequential containment bypass (e.g. an induced steam generator tube rupture during a severe accident progression)

Commented [NM215R214]: This is now listed as an example of "plant event sequence with containment bypass", so what you are proposing wouldn't fit under this.

Commented [LHJ216]: A plant event sequence where there is core melt and in which the containment is open (e.g. in the shutdown state)

Commented [AKE217]: in the footnote, what is a significant release?

Commented [LHJ218R217]: Agree, to delete

Commented [AKE219]: all of these examples above lead to uncontrolled releases, so no need just to mention this one

Commented [LHJ220R219]: OK

Formatted: Indent: Left: 0 cm, Hanging: 1 cm

Commented [AKE221]: we generally use classify to imply some kind of hierarchy. I think this is not really a hierarchy

of plant event sequences (e.g. severe accident conditions) for consideration for practical elimination.

4.144.15 ~~consideration.~~ Other ~~classification or grouping~~ criteria for grouping are also possible. The ~~Note also that the~~ consequences of~~from~~ the accidents in para. 4.1412(c)(i) and 4.1412(c)(ii) could in fact be mitigated by the implementation of reasonable technical means. In such cases, for scenarios not retained within the scope of consideration for practical elimination, evidence of the effectiveness and an appropriate reliability of the mitigation should be provided.~~is necessary.~~ To facilitate the grouping proposed, each type of plant event~~accident~~ sequence should be analysed to identify the associated combination of failures or associated physical phenomena that are specific to the plant design, and which have the potential to lead to~~both to severe accident sequences and 'unacceptable radioactive releases'. This analysis helps identifying accident sequences that could lead to an early radioactive release or~~ a loss of the confinement function. ~~large radioactive release.~~

4.154.16 The identification and grouping~~approach~~ described in paras 4.1412 and 4.16 should combine~~13 combines~~, when relevant, the following approaches:

(a) A phenomenological (top-down) approach, in which ~~considers any~~ phenomena are considered that might challenge the confinement ~~safety~~ function before or in the course of a severe accident, in order to define a comprehensive list of plant event sequences, i.e.~~severe accidents~~ as listed~~described~~ in para. 4.1412;

(b) A sequence-oriented (bottom-up) approach, in which all plant event ~~reviews any accident~~ sequence that could lead~~leading~~ to a severe accident are reviewed.~~.~~ For each sequence, any challenge to the confinement ~~safety~~ function is assessed (this might involve~~may require~~ evaluation of the loads on the~~onto~~ containment and of possible release routes via leakages and bypasses). The sequence-oriented approach~~This~~ supplements the phenomenological~~top-down~~ approach with ~~a~~ broader screening to identify all~~any~~ relevant plant event sequences~~accident sequence~~.

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

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

IDENTIFICATION AND ASSESSMENT OF SAFETY PROVISIONS FOR JUSTIFYING~~ACHIEVING~~DEMONSTRATING PRACTICAL ELIMINATION

4.184.19 Following~~To achieve~~ the identification~~objectives~~ of relevant event sequences~~practical elimination, designers of new NPPs will need to consider an appropriate short list of accident scenarios~~, and grouping them into a smaller set of plant conditions, as the next step, the designer should undertake an~~undertake~~ assessment aimed at identifying safety provisions in the form of design and operational features that could be implemented~~, either for~~

Commented [AKE222]: can we not repeat this phrase? to reinforce the point above?

Commented [LHJ223R222]: Agree

Commented [AKE224]: this is said above

Commented [YJ225]: WNA

Commented [AKE226]: otherwise it looks like the safety provisions themselves are to be practically eliminated

Commented [LHJ227R226]: I agree with adding something, however I prefer justifying instead of achieving

Commented [AKE228]: by 'short list of accident scenarios' I guess you mean the same groups of event sequences that was identified in the previous step? Or it is a different short list?

Commented [LHJ229R228]: It is the same for PE

Commented [NM230R228]: ok

Formatted: Font color: Auto

Commented [AKE231]: better have this word in this sentence

Commented [AKE232]: See Req 5 of SSR-2/1 (Rev. 1). It seems that only design features are relevant for ensuring practical elimination?

~~achieving~~ demonstrating ~~mitigation of the consequences of the severe accident condition or for its~~ practical elimination of each relevant plant ~~condition~~event sequence. ~~.~~ In this assessment ~~and later in the demonstration of 'practical elimination' of a severe accident condition~~, the following aspects should be considered:

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

~~(a)~~(b) Experience ~~, including the industry experience~~ from the operation of nuclear power plants~~NPP~~ and from accidents;

~~(b)~~(c) Proven~~The~~ technical and industrial ~~proven~~ feasibility of safety provisions;

(d) The capability of the safety provisions~~provision~~provision to provide sufficient margins for dealing with uncertainties and to avoid cliff edge effects;

~~(c)~~(e) Potential~~The potential~~ drawbacks of safety~~additional~~ provisions, which ~~that~~ might only become evident after the plant is put into operation~~not be seen immediately~~ (e.g. operational constraints or spurious ~~operator~~ ~~action~~actuations~~action~~);

~~(d)~~(f) The kinetics~~kinetic~~ of the ~~adverse~~ severe accident phenomena that might threaten the containment integrity or its leaktightness;

~~(e)~~(g) Avoiding the~~The no~~ need to conduct~~execute~~ on-site actions or use ~~of~~ off-site personnel or~~staff and~~ equipment.

~~4.19~~4.20 The identification of safety provisions necessitates a comprehensive analysis of the physical phenomena involved and it might~~may~~ be necessary to further refine the identification of event~~elementary accident~~ sequences performed in accordance with the approaches described in para. 4.17~~14~~.

~~4.20~~4.21 The designer should establish a decision ~~This identification aims at defining several options to be submitted to the decision~~ making process for determining~~establishing~~ reasonably practicable safety~~design and operational~~ provisions to achieve practical elimination. Several options for safety provisions should be developed and submitted to the decision making process.

~~4.21~~4.22 The safety ~~design of~~ provisions identified~~considered~~considered to ~~justify~~ ~~achieve~~demonstrate the ~~for~~ practical elimination of relevant event~~accident~~accident sequences should be associated,identified ~~done~~ on a case ~~-~~by ~~-~~case basis, ~~and, where relevant, associated~~ to the appropriate level of defence in depth or plant state at which the event sequence ~~of events~~ would need to be interrupted to prevent unacceptable radiological consequences. It should be verified that the appropriate engineering design rules, such as 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, to ensure that the safety provisions~~they~~ would achieve their safety function with~~to provide~~ sufficient margins to account for uncertainties, under the prevailing conditions, e.g. the harsh environmental conditions associated with~~to~~ a severe accident. In applying the engineering design rules and technical~~assigning~~ requirements, where relevant, appropriate testing should be applied, operational procedures should be followed, and, in operation, surveillance ~~monitoring~~ as well as in-service testing and inspection should be conducted~~considered~~. The engineering design rules and technical requirements should be applied at all steps in the development of the

Commented [LHJ233]: For consistency, we should mention "plant event sequence"

Commented [AKE234]: if we are doing a step by step approach, this isn't so helpful. In the next section, I've referred back to this para

Commented [AKE235]: this seems like a different – less sciency – thing than the first bullet. Thus a separate bullet

Commented [AKE236]: earlier you have a long explanation of 'additional', but unless you mean exactly that here too, I suggest removing it

Commented [AKE237]: ?

Commented [LHJ238R237]: No, maybe "spurious actuation".

Commented [NM239R237]: If you think this is the meaning.

Commented [AKE240]: you have to say something about where this decision making process has come from. I assume it is within the designer?

Commented [LHJ241R240]: Text modified

Commented [NM242R240]: ok

Commented [AKE243]: I think it's not ok to say the design should be identified

Commented [YJ244]: Canada, ENISS, France UK

Commented [YJ245]: Canada, ENISS, France UK

Commented [LHJ246]: The safety provisions are considered to justify how the PE concept could acceptable not to achieve it.

Commented [AKE247]: you've already identified them

Commented [AKE248]: I think you need to explain what you mean by 'appropriate' rules, and link it back to the introductory sentence of the para

Commented [LHJ249R248]: Text added

Commented [NM250R248]: ok

Commented [AKE251]: is assigning requirements the same as applying requirements? In that case, this seems to be a repeat of the subsequent sentence

but if it means 'determining the requirements to be applied' then we'd need to reword the sentence

safety provisions, from design to operation, including their manufacture, construction or implementation at the plant, and theiron site, commissioning and periodic testing.

4.224.23 Safety provisions for justifyingachievingdemonstratingDesign provision and operational provision for practical elimination of some severe accident conditions could include operational provisions as well as design provisions, and as such they could involve the performance of operator require human actions to be performed (e.g. the opening of primary circuit depressurization valves to prevent high-pressure core melt conditions). In such cases,this case a human factor assessment should be part of the justification supportingneeded to support any claim for high reliability of operator actions. The human factor Examples of items the assessment should addressinclude as part of the followingdetermination of high reliability are as follows:

(a) The availability of information given to operating personnel to perform the actionsaction from the control room or locally, and the quality of the procedures or guidelines to implement the actions.;
(b) The environment for performing the action (e.g. access to the local area, components to be handled, identification of thecomponents location of components,and ambient conditions). If localLocal actions are expected to be takenduring a severe accident in harsh environmentalenvironmentalzardousenvironmentalzardous conditions, this is are likely to reduce the necessary reliability for demonstration of practical elimination.;
(c) The timescales for performingto perform the actionsaction, including sufficient margin to achieve the expected outcomesit.

4.234.24 Some safetydesign and operational provisions claimed to contribute towards for the "practical elimination" of some eventsevere accident sequences could be vulnerable to potential human errors that might have occurred prior to the onsetaccident. This type of the accident. Such human errorserror could introducecause latent risks to be introduced that might prevent successful operation of a system or component when it iswhen called upon during an event or accident. In such casesa case, the system or componentSSCs used to performdeliver the action should be subject to relevant operational provisions (e.g. periodic testing, in-service inspection and surveillance,inspections and monitoring, commissioning qualification tests following maintenance activities and, periodic system alignment checks) to limit the risk from human errors of this type of human error.

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

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

Commented [LHJ252]: Could be say justifying instead of achieving?

Commented [AKE253]: probably not a structure, I think? we do't usually have operator actions on structures

Therefore, certain safety provisions for ~~achievingjustifying~~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.

~~4.25~~4.26 Where safety~~design~~ provisions for ~~achievingjustifyng~~demonstrating practical elimination ~~and operational provisions~~ rely on support functions, the relevant supporting ~~and~~ systems should~~, the latter are~~ all be designed to the standards necessary to ensure that~~the SSCs~~ they ~~support will~~ have same level of separation, diversity, and robustness to hazards as the safety~~main design~~ provisions they support, or that the safety~~main design~~ provisions are~~, or be~~ tolerant to the loss of support functions.

DEMONSTRATION OF ~~'~~PRACTICAL ELIMINATION~~ELIMINATION'~~

~~**General Aspects**~~

~~4.26~~4.27 The overall effectiveness of the safety provisions identified by the designer to ~~justify~~~~achieve~~demonstrate practical eliminationpractically practically eliminate large or early releases should be demonstrated through a safety assessment thatwhichwhich includes engineering judgement, deterministic analyses and probabilistic assessments. The demonstration of practical elimination should be conducted~~be based on the assessment of provisions that would generally include engineering judgement and deterministic and probabilistic analyses. Some of the categories of conditions defined in para. 4.12 for the demonstration of practical elimination entail very severe challenges to the integrity of the physical barriers for radionuclide retention and necessitate specific design and operation provisions for their practical elimination. The demonstration of practical elimination can be considered~~ as part of the design and safety assessment process for the plant, including the necessary inspection and surveillance processes during manufacture~~manufacturing~~, construction, commissioning and operation.

~~4.27~~4.28 The safety provisions developed~~measures~~ to prevent the event sequences in each of the groups~~categories~~ in para. 4.~~14~~12 from occurring should all be ~~provided and their effectiveness should be~~ analysed. None of the phenomena or accident~~and plant~~ conditions indicated should be overlooked because of their low likelihood of occurrence. Credible~~, but credible~~ research results should be employed~~and dedicated means to minimize the identified risks are necessary~~ to support ~~the safety~~ claims of effectiveness of the safety provisions.

~~4.28~~4.29 For each ~~accident sequence~~ group of event sequences considered for ~~'~~practical elimination~~elimination'~~, an assessment should~~has to~~ be performed to demonstrate the effectiveness~~acceptability~~ of the associated safety provisions. Either it~~design. It~~ should be demonstrated that it is physically impossible for the eventaccidentaccident sequence ~~condition~~ to arise (see paras 4.34 and 4.35) or it should~~or for the~~ accident sequence ~~condition to~~ be demonstrated~~extremely unlikely to arise~~, with a high level of confidence, that the event sequence is extremely unlikely to arise (see paras 4.36 to 4.43). 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.

Commented [LHJ254]: for justifying?

Formatted: Indent: Left: 0 cm

Commented [AKE255]: seems it should be a should statement

Commented [AKE256]: seems it should be a should statement

Commented [LHJ257]: justify?

Commented [AKE258]: seems like is the same as the previous sentence

Commented [AKE259]: I don't see how this links to the topic of the paragraph. It seems a repeat of the introductory paragraph to the previous subsection

Commented [AKE260]: I think this should be a should statement

Commented [AKE261]: the dedicated means are just the safety provisions, right? so including this in the sentence seems to make the paragraph circular

Commented [LHJ262R261]: Agree

4.294.30 As evident from shown in para. 4.1412, the various eventaccident sequences to be considered for 'practical eliminationelimination' are inherently rather different in essence. As a consequence, their demonstrations of 'practical elimination shouldelimination' are expected to be demonstratedprovided on a case by case basis reflecting this variety.

4.304.31 Uncertainties due to limited knowledge of some physical phenomena, in particular those resulting from severe accident phenomena, shouldhave to be considered when conducting engineering analyses as well as deterministic safety analyses and probabilistic safety assessment, so thatanalyses to ensure a high level of confidence in the result can be assured.

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

4.32 Computer codes and calculations used to support the demonstration of 'practical eliminationelimination' should be verified and validated and models used should reflect best understanding of the physical phenomena involvedshould reflect best practicesknowledge so as to provide acceptable prediction of the eventaccident sequences and the phenomena involved. Section 5 of phenomena. SSG-2 (Rev. 1) [9] provides recommendationsfurther guidance on the use of computer codes for the deterministic safety analyses (see Section 5 of SSG-2 (Rev. 1) [8]).

Practical elimination of event sequences because they would be physically impossiblePhysical impossibility

4.33 Where a claim is made that an eventaccidentaccident sequence cancondition that needs to be 'practically eliminated because iteliminated' is physically impossible, it should be demonstratedis necessary to demonstrate that the inherent safety characteristics of the system or reactor type are suchensure that the eventaccidentaccident sequence condition 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 are fulfilled.

4.34 In practice, the demonstration of physical impossibility approach is limited to very specific cases. Demonstration of physical impossibility cannot rely on measures that involverequiring active components or operator actions. human interactions. Should such a case arise, it would be heavily challenged. An example is the practical elimination of could be the effect of heterogeneous boron dilution, for which the main protection is provided by ensuring first by injecting a limited volume of injection of non-borated water which does not allow that effect to happen and second because of thesecondand seconda a negative reactivity coefficient for all possible combinations of the reactor power and coolant pressure and temperature. In this case, physical impossibility applies only to a prompt reactivity insertion accident could be considered physically impossible.

Commented [AKE263]: does this para apply to practical elimination both by physical imposssibilyt and by extremely to occur? If it is only the latter, then it is already said below in that section and could be deleted here. But if it is both, then it is OK to leave it here

Commented [LHJ264R263]: uncertainties apply to both

Commented [NM265R263]: OK

Commented [AKE266]: or something like: 'and models used should reflect best understanding of the physical phenomena involved'

I think you mean something about the quality of the model?

Or maybe you mean 'should use a best estimate approach'?

Commented [LHJ267R266]: Agree and text added

Commented [AKE268]: I think this demonstrates a kind of weakness to your argument – better just to say it cannot be permitted

Commented [LHJ269R268]: Agree

Commented [AKE270]: this example is not clear to me, but if you explain it, then we can rewrite it a bit

Commented [LHJ271R270]: Text provided

Commented [NM272R270]: I guess it's ok

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

4.35 The demonstration that certain plant sequences are extremely unlikely occur should rely on the assessment of engineering aspects, deterministic considerations, supported by probabilistic considerations to the extent possible, taking into account the uncertainties due to the 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.~~probabilistically.~~ Probabilistic insights should be used only in~~to~~ support of deterministic and engineering analyses. Meeting~~analysis for the demonstration of practical elimination. Also, meeting~~ a probabilistic target alone is not a justification to exclude further deterministic and engineering analyses~~the analysis~~ and possible implementation of additional reasonable safety provisions~~design or operational measures~~ to reduce the risk. Thus, the~~a~~ low probability of occurrence of an accident with core damage is not a reason for not protecting the containment against the conditions generated by such an accident. In contrast~~fact~~, design extension conditions with core melting are required~~need~~ to be postulated in the design, in accordance with Requirement 20 of SSR-2/1 (Rev. 1) [1].

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

(a) An adequate set of safety provisions, including both equipment and organizational~~organisational~~ provisions;
(b) The robustness of these safety provisions (e.g. adequate margins, adequate reliability, qualification ~~against~~ for the operational~~operation~~ conditions);
(c) The independence between these safety provisions (i.e. an adequate combination of redundancy, ~~and~~ physical separation, diversity and, ~~functional~~ independence).

4.37 Deterministic analyses~~analysis~~ of severe accidents should be performed using a realistic approach (see Option 4 in table~~Table~~ 1~~, Section 2~~ of SSG-2 (Rev. 1) [9]),~~8])~~ to the extent practicable. Because explicit quantification of uncertainties might~~may~~ be impractical owing~~due~~ 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 ~~severe accident~~ analyses. Sensitivity studies could also be used to confirm the adequacy of a conservative bounding analysis.

4.38 If probabilistic arguments are used to support a claim ~~When it is claimed~~ that a particular event accident accident sequence ~~accident condition~~ has been practically eliminated, it should ~~with the support of probabilistic arguments, it needs to~~ be ensured~~taken into account~~ that the cumulative contribution of all the different event sequences considered does not~~cases cannot~~ exceed the target ~~for large or early release~~ frequency for early radioactive releases or large

Commented [AKE273]: we'd better be consistent in calling this extremely

Commented [LHJ274R273]: Agree

Commented [AKE275]: I deleted not because it's wrong, but just because you never call it that elsewhere

Commented [AKE276]: this needs some explanation in this context, because in SSG-2 *conservative* is option 1. And you don't call on 'conservative' approaches for anything else here regarding practical elimination. Conservative is normally only for safety systems and DBA

Commented [NM277R276]: Please insert a note "in the context of this safety guide…."

Commented [YJ278]: Agreed with France

Commented [AKE279]: is that what you mean by cases?

Commented [LHJ280R279]: Yes

radioactive releases, if~~where~~ such a target has been claimed by the ~~NPP~~ designer or operating organization~~/ operator~~ in the~~its~~ safety assessment of the plant~~report~~ or has been established by the regulatory body.

4.39 The validity of any~~the~~ probabilistic models ~~model~~ used should be checked against the event~~dedicated~~ accident sequence at hand.~~condition to assess.~~ Assumptions made in support of this check~~for the proof~~ should be well justified and validated.

~~4.38~~4.40 The limitations of and uncertainties associated with the models used in demonstration of practical elimination should be identified, taking into account~~bearing in mind~~ that limitations of probabilistic safety assessment studies are associated with the probabilistic modelling, as well as the supporting deterministic best-estimate studies.

~~4.39~~4.41 If~~When~~ the event~~accident~~ sequence to be '~~'~~practically eliminated~~eliminated'~~ is the result of a single initiating event, such as the failure of a large pressure-retaining component[23] in normal operation~~operational states~~, the demonstration of practical elimination should rely on the substantiation that ~~achieving~~ a high level of quality is achieved at all stages of the lifetime of the component, i.e. its ~~lifetime:~~ design, manufacture~~manufacturing~~, implementation, commissioning and~~,~~ operation (including periodic testing and in-service surveillance~~monitoring~~, if any) so as~~could~~could be achieved to prevent the occurrence and propagation of any defect liable to cause the failure of the component. Hence, ~~either~~both the occurrence of the single initiating event (e.g. failure of a large pressure-retaining component) and ~~of the facility) or~~ the consequential event (i.e. uncontrolled reactivity accident) should~~needs to~~ be considered for '~~'~~practical elimination~~elimination'~~.

~~4.40~~4.42 If~~When~~ the event~~accident~~ sequence to be '~~'~~practically eliminated~~eliminated'~~ is the result of an event~~accident~~ sequence in which~~where~~ the confinement function degrades~~is degraded~~ before ~~the~~ core melt occurs, then it should~~core melt has to~~ be demonstrated,~~prevented~~ with a high degree of confidence, that core melt will be prevented.~~.~~ This means that, at least, the usual levels~~lines~~ of defence in depth should be implemented (i.e. for anticipated operational occurrences, design basis accidents~~AOO, DBA~~ and design extension conditions~~DEC~~ without fuel degradation) with enhancements, as~~and enhance them when~~ necessary, to prevent design extension conditions with core melt. ~~.~~

DOCUMENTATION OF THE APPROACH TO PRACTICAL ELIMINATION

~~4.41~~4.43 The safety analysis report of the plant should reflect the measures taken to demonstrate~~to~~ justify the practical elimination~~practically eliminatione~~ of event~~accident~~accident sequences ~~conditions arising~~ 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~~conditions~~ accident sequences, the design and operational safety provisions implemented to ensure that the

[23] In~~Note that in~~ some ~~Member~~ States, this demonstration is associated with~~to~~ other concepts such as 'incredibility~~Incredibility~~ of failure', 'high integrity component', 'non~~Failure', 'High Integrity Component', 'Non~~-breakable component', rather than with~~to~~ the concept of '~~'~~practical elimination~~elimination' concept~~.

Commented [AKE281]: I've made this more wishy-washy because above you emphasise that one is not supposed to rely on probabilistic

Commented [LHJ283R282]: Agree with the changes, the assessment corresponds to those event sequences leading to PE

Commented [AKE282]: please review this sentence. What does dedicated mean here? Why does the sentence end with 'to assess'

Commented [AKE284]: as it's just an example, OK if we say this instead?

Commented [AKE285]: is this an either/or? or both/and?

Commented [AKE286]: did I get the right meaning here? I.e. this is a way of handling PE by looking at DEC with core melt?

Commented [LHJ287R286]: Yes, agree with the change

Commented [AKE288]: seems this needs a new subheading, as it's broader than the previous subheading

Commented [LHJ289R288]: Agree

possibility of such eventconditions accident sequences arising has been 'practically eliminatedeliminated' 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 SSR-2/1 requirement 14 of SSR-2/1 (Rev. 1) [1], the design basis for of items important to safety at nuclear power plants should be take established taking into account the most limiting conditions under which they need to operate or maintain their integrity. This includes the conditions resulting from natural external natural hazards. In accordance with Requirement 17 of SSR-2/1 (Rev. 1) [1], the effects of The external hazards and relevant combinations of hazards to be considered, as per requirement 17 of SSR-2/1 are required to be evaluated. This identified and their relevant severity to achieve adequate protection of the public and the environment is done is defined as part of the site evaluation for the plant (see IAEA Safety Standards Series No. (SSR-1. Site Evaluation for Nuclear Installations [16][16]). (SSR-1).

5.2 There have been cases in which some external natural hazards, such as extreme earthquakes, floods and tsunamis, have exceeded the levels of external hazards considered for the design. as a result from the site evaluation. Paragraphs 5.21 and 5.21A21.A of SSR-2/1 (Rev. 1) [1] state that adequate require sufficient margins are required to be provided in the design to protect against external hazards for such cases.[24] in the design[25].

5.3 To provide resilience against levels of external hazards exceeding those considered for design, several requirements are established in derived from the hazard evaluation for the site, SSR-2/1 (Rev. 1) [1] regarding introduced the inclusion of need to include features in the design to enable the safe use of non-permanent equipment for the following purposes[26]:

(a) Restoring the necessary electrical power supplies (see para. 6.45A of SSR-2/1 (Rev. 1) [1]);
(b) Restoring the capability to remove heat from the containment (see para. 6.28B of SSR-2/1 (Rev. 1) [1]);
(c) Ensuring sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation (see para. 6.68 of SSR-2/1 (Rev. 1) [1]).

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

5.4 Non-permanent equipment is primarily intended for preventing unacceptable radioactive consequences. The aim of the use of such equipment is to restore safety functions that have been lost, but not to be the regular means to achieve these functions in the long term after an accident

[24] 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.

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

[26] 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].

Formatted: Don't keep with next, Don't keep lines together

Commented [AKE290]: I have shifted the position of the footnote

Commented [LHJ292R291]: Agree

Commented [AKE291]: para moved from SCOPE

Commented [AKE293]: or 'Design features enabling the use of non-permanent equipment are….'

Commented [LHJ294R293]: As the text is proposed now is OK, there is no need to add design features.

~~after a postulated initiating event~~phase of ~~accidents~~accident ~~conditions~~, i.e. ~~in DBA~~ and after very rare events (e.g. natural external hazards exceeding the levels considered for ~~DEC.~~

5.5 Consistent with the intentions of para. ~~7.51 and 7.64 of SSG-2 (Rev.~~ design, derived from 11) [8][27], the hazard evaluation for aim of the site) for which the capability and availability of design features installed on-site might be affected. The aim of the use of non-permanent use of such equipment is to restore safety functions that have been lost, but it should not to be the regular means for coping to to cope with accident sequences for DEC in the short -term ~~phase~~ for design basis accidents or for design extension conditions (see also paras of the of the accident. 7.51 and 7.64 of SSG-2 (Rev. 1)).

~~5.5 To meet In order to approach~~ the requirements set out in para. 5.3 ~~implementation of design features for using non-permanent equipment~~, levels of natural 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. ~~This should be done to establish accident management measures to increase the response capability of the nuclear power plant.~~

5.6 Particularly for external hazards, if the design basis for the plant is well established, it is expected that the frequency of occurrence of a natural hazard of a severity significantly exceeding ~~a well-established design basis derived from~~ the levels considered for design will be ~~site evaluation is~~ very low. However, as such frequencies are generally associated with significant uncertainties, ~~it is very important to understand~~ the behaviour of structures, systems and components ~~SSCs~~ to loading parameters resulting from ~~for~~ levels of external hazards exceeding those considered for ~~beyond above~~ the design should be well understood.

~~5.6~~5.7 An evaluation should be conducted to demonstrate that ~~basis,~~ the plant would ~~should~~ be able to cope with a hazard of a severity exceeding the levels considered for the design as follows ~~the situation~~:

- To a certain extent, on the basis of the demonstration of the ~~behaviour (~~margin~~)~~ of a set of structures, systems and components ~~SSCs (~~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 ~~hazards~~, and/or in addition to this, on the basis of the use of non-permanent equipment to restore the necessary safety functions.

~~5.7~~5.8 For each relevant scenario involving ~~of~~ an external hazard of a level beyond the design basis, the evaluation should identify limitations on the ~~plant~~ response capabilities of the plant ~~capability~~ and ~~should define~~ a strategy should be defined to cope with these limitations. The ~~In the~~ evaluation should also identify~~,~~ the various coping provisions, accident management

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

Commented [AKE295]: how about this phrase? – there is something similar in SSG-2 (Rev. 1)

or 'for long term event sequences' would also be something similar to what is used in SSG-2 (Rev. 1)

Commented [LHJ296R295]: long term phase of accident conditions is clear, why change it, should IEC needs to specify "phase" in their SGs? The word "phase" is used in SSG-4 and SSG-53, with the same meaning: to identify the time when the accident has already evolved and it is opposite to early phase (SSR-2/1 (Rev. 1)), therefore why not here? Sorry, but I do not agree.
Note: We are going to have the same discussion with DS528.

Commented [AKE297]: ok as a should statement?

Commented [LHJ298R297]: Agree

Commented [AKE299]: I think you don't need this sentence here – it seems you are setting out in the subsequent paras what you would do to 'establish accident management measures'

It also seems to be a repeat of the 1st sentence of 5.3

Commented [AKE300]: should statement ok, rather than 'it is important'?

Commented [AKE301]: you talk about '*the* evaluation' below, so perhaps good it introduce it here. As a new para?

Commented [AKE302]: this doesn't seem like a should statement.

Formatted: No widow/orphan control, Don't keep with next, Don't keep lines together

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 should be identified. Such an evaluation should include the following:

(a) A robustness analysis of a relevant set of items important to safety to estimate the extent to which those items would be able to withstand 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 beingreaching unacceptable radiological consequences for the public and the environment;
(c) TheA definition of the coping strategies to limit and mitigate the consequences of the scenarios that could leadleading to a loss of relevant safety functions;
(d) An estimate of the necessary resources (i.e.in terms of human resources, equipment, logistics and communication) to confirm the feasibility of the coping strategies.

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

5.85.10 The evaluation should consider the possibility that multiple units at the same site could be simultaneously affected by such an extreme external hazard.

5.95.11 The plant response and the coping strategiesstrategy for a level of external hazards exceeding the levelsthose considered for design, derived from the hazard evaluation for the site should be assessed based on a realistic approach and should be supplemented where relevant (e.g. in the case of cliff edge effectseffect) by sensitivity analyses where assumptions in the modelling or where important operator actions by operating personnel are identified as essential factors for the credibility of the strategy.

5.105.12 The coping strategies should be defined, and the associated coping provisions should be specified and designed taking into account the most unfavourable possible scenarios, in accordance with para. defined according to 5.86.

5.115.13 To make the coping strategies more reliable, an adequate balance should be implemented between fixed equipment and non-permanent equipment. should be implemented. This balance should be defined in accordance withconsidering the coping time, 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 by operating personnel needed for the whole coping strategy. The use of permanent fixed equipment should be preferred for the implementation of short-term actions.

Commented [AKE303]: yes? this kind of protection

Commented [LHJ304R303]: Yes, that is the protection

Commented [AKE305]: needs to be a new para, I think

Commented [AKE306]: this term is used a lot and needs an explanation

Commented [LHJ307R306]: Agree

However, use of non-permanent equipment should be considered as backup to fixedpotentially failed installed equipment that might fail, including for short -term actions, as it canmay provide innovative and diverse means to further reduce risk and should be considered.

5.125.14 The use of non-permanent equipment should be such that the time period needed for thetheir installation and putting intoin 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 operatorto implement actions before the occurrence of a cliff edge effect. should be established. This time period should be derivedbased, where possible, on the basis of times recorded during drills, or using other approaches for validating operatorthe actions. of operating personnel. The ability to deliver and operate non-permanent equipment on time under adverse conditions at the site should also be demonstrated, particularly , and for events that could involveinvolving significant degradation of infrastructureinfrastructures and roads caused by extreme hazards on the site and off the site. Considerations, should also be given to storingdemonstrated. The storage location of non-permanent equipment at a distance from the units can be of advantage in the case of some extreme natural hazards.

Commented [YJ308]: Agreed with France

5.135.15 The installation and use of non-permanent equipment, if any, should be documented, and comprehensive training, testing and drills should be periodically conducted to maintain operator proficiency in the use of the equipment and associated procedures. ToDrills should consider to the extent reasonably possible, drills should consider the conditions of real emergencies.

Commented [YJ309]: Agreed with France

5.145.16 Once the coping strategies have beenare defined and validated, guidance for the operators, as well as thetheir technical basis of the strategies, should be established and documented (e.g. in emergency operating procedures or severe accident management guidelines).

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

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

[2][3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

[3][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).

[4][1] ~~INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2 (Rev. 1), Vienna (2019).~~

[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).

[9][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.)

[10][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.)

[11][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).

~~[12]~~[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.)

~~[13]~~[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).

EXAMPLESABBREVIATIONSABBREVIATIONS

AOO	Anticipated Operational Occurrence
DBA	Design Basis Accidents
DEC	Design Extension Conditions
NPP	Nuclear Power Plant

ANNEX I. ILLUSTRATION OF POTENTIAL CASES OF PRACTICAL ELIMINATION

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 whichwhere 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 provisions would not be effective in a such situation and an early radioactive release or large radioactive release couldwould follow. This is a very exceptional type of initiating event for which safety systems and safety features are not designed for itstheir mitigation and therefore it needs to be demonstrated that thetheir likelihood of such an initiating event occurring would be certainly so low that itthey can be excluded, i.e. 'practically eliminatedeliminated', from consideration. This is particularly importantessential at least for the reactor vessel, in which a break would eliminate the capability of holding and cooling the core. In addition, the likelihood of a failure of the pressurizer or theand steam generator shell failure need to be shown to be extremely low, or alternatively it needs to be demonstrated that a failure of the pressurizer or the steam generator shell would not lead to unacceptable consequences forto the containment.

Commented [AKE310]: is this correct?

Commented [LHJ311R310]: Yes

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

(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 practicesoperation practice need to be in place to minimize thermal fatigue, stress corrosion, embrittlement, pressurized thermal shock and over-pressurization of the primary circuit;
(f) EffectiveAn effective in-service inspection and surveillance and chemistry control programmes needprogramme needs to be in place during the manufacturemanufacturing, construction, commissioning and the operation of the equipment, so that to detect any defectsdefect or degradation mechanisms are detected and to ensure that the equipment properties are preserved over the lifetime of the plant.

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

Commented [AKE312]: level of integrity is not normally used

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

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

I-6. The demonstration, ~~of low failure likelihood~~ 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 ~~includes~~ assessments address aspects such as ~~of~~ material fracture toughness and~~,~~ weld residual stress, ~~etc.,~~ which in turn consider~~considers~~ deterministic analysis, engineering judgement and the measurements of monitored values ~~as well~~.

FAST REACTIVITY INSERTION ACCIDENT IN A LIGHT WATER REACTOR~~ACCIDENTS~~

~~a) LWRs~~

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 possible, thet~~The~~t~~T~~he prevention of such accidents is to~~needs to~~may 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 depth33 by provision of two diverse, independent means of shutdown.

~~I-7.~~I-8. ~~.~~The first level of defence in depth11 of~~main protection is~~ may be provided by the core nuclear characteristics (such as the negative reactivitypowerpower coefficient in light water reactors),of reactivity in LWR) ~~an overall negative reactivity coefficient~~ which, under all possible combinations of reactor power, neutron absorber concentration, coolant pressure and temperature, suppresses any increase in~~thus~~ could ~~suppress~~ing reactor power ~~increase~~ during any disturbances and eliminate any ~~eliminating the~~ uncontrolled reactivity excursion. Therefore, this is a case ~~with help of the laws~~ of ~~nature (~~demonstration of practical elimination by physical impossibility of the event sequence.~~conditions).~~

~~I-8.~~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~~with a high level of confidence, to be extremely unlikely to occur~~.

~~I-9.~~I-10. Therefore, the~~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~~insertions~~ of reactivity, which~~e.g. injection of water with low boron concentration in the core that~~ can be evaluated deterministically and probabilistically as appropriate to demonstrate that the conditions~~they~~ are extremely unlikely to occur.

~~I-10.~~I-11. A more~~More~~ complex situations~~situations~~ could arise however if criticality can be reached during a severe accident~~accidents~~. This has been a topic of concern for~~in~~ specific core meltdown scenarios in reactors ~~using enriched fuel~~, for which ~~where~~ the control rod material has a lower melting point and eutectic formation temperature than the fuel rods. A potentially hazardous scenario might occur if the reactor vessel were reflooded with un-borated water in a situation when 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~~a~~ generation of additional heat on a continuing or intermediate basis, depending on the presence of water.

Commented [AKE313]: there is no (b)

Commented [AKE314]: I broke up the para because the next bit is only about level 1

Commented [AKE315]: is this an alternative example? for level 3 DiD protection? And the other kind of practical elimination? It looks like the example in 4.34 (b)

Commented [LHJ316R315]: yes it is the same situation as 4.34 (b).

Commented [AKE317]: it would be good to make this parallel to the previous paragraph

Commented [LHJ318R317]: To be in agreement with para 4.34, the demonstration is based on physical impossibility and not on high level of confidence, to be extremely unlikely to occur

Commented [AKE319]: the example is already in the previous sentence

Commented [LHJ320R319]: Even though the negative reactivity coefficient is important, it needs to be together with the reduce volume of clean water that could be injected.

Commented [AKE321]: this difference in melting points is the case for all enriched fuel? or only some enriched fuel?

Commented [LHJ322R321]: Text modified

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~~to reach a plausible conclusion~~ that the plant sequence~~condition~~ has been practically eliminated because it is considered, with a high level of confidence, to be extremely unlikely to occur.

~~b) PHWRs (if Canada provides a text. If not, this case will be presented as only for LWRs)~~

DIRECT CONTAINMENT HEATING

I-12. In a pressure vessel reactor~~reactors~~, core meltdown at high pressure could cause a violent discharge of molten corium~~cor~~ium~~e~~ material into the containment atmosphere and this would result in direct containment heating from the hot melt and exothermic chemical reactions. Event sequences involving high~~High~~ pressure core melt ~~situations~~ 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-11.~~I-13. ~~.~~ In a pressurized heavy water reactor, in contrast~~reactors~~, direct containment heating due to ejection of the molten corium~~cor~~ium~~e~~ at high pressure is practically eliminated because pressure tubes would fail rapidly at high fuel temperature. This would depressurize~~depressurise~~ 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-12.~~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 a~~ design provisions in place~~objective~~ to ensure, with a ~~convert the~~ high level of confidence, that such small coolant leaks or boiling of the coolant instead would result in~~pressure core melt to~~ a low pressure core melt sequence with a high reliability, so that high pressure core melt conditions can be practically eliminated. The depressurization needs to be such that very low pressure can be achieved before any~~a~~ discharge of molten corium~~cor~~ium~~e~~ from the reactor vessel can take place. In addition~~On the other hand~~, it is important that dynamic loads from depressurization do not cause a threat to the ~~essential~~ containment structures. Design provisions need to be in place to ensure, with a high level of confidence, that any high pressure core meltdown scenario ~~this~~ does not occur.

~~I-13.~~I-15. Dedicated depressurization systems have been installed in existing plants and designed for new plants. At pressurized water reactors, such systems~~they~~ are based on simple and robust devices and straightforward actions by operating personnel that eliminate the risk of erroneous automatic depressurization but provide adequate time to act if the~~when~~ need arises. At boiling water reactors, the existing steam relief systems generally provide means for depressurization, with possibly some modifications in valve controls to also ensure reliable valve opening and open valve positions at~~in~~ very low pressures.

~~I-14.~~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, ~~the practical elimination of~~ 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.

Commented [AKE323]: I think you cannot say plausible here. It doesn't mean the same at all as 'high level of condifidence'

Commented [AKE324]: a new para, a new situation

Commented [LHJ326R325]: Yes, it is. Since the potential consequences of the high pressure core melt ejection there is a need to perform a fast depressurization

Commented [AKE325]: I don't think you mean that a high pressure melt is converted to a low pressure melt sequence (in reality)

Commented [AKE327]: where are you going with this statement? see the proposal for another sentence straight after this one

Commented [LHJ328R327]: Dynamic loads from depressurization are important see para. 7.26 of SSG-56. It should be also mentioned that here.

LARGE STEAM EXPLOSION

I-15.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 mightmay occur in-vessel, during flooding of a degraded core or ifwhen a molten core relocates into the lower head filled with water. Such interactions mightThey may also occur ex-vessel, ifwhen 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 integrity.

I-16.I-18. The conditions of the triggering of athe steam explosion and the energy of explosion in various situations have been widely studied in reactor safety research programmesprograms. The risks of steam explosion cannot be fully eliminated forin all core meltdown scenarios in whichwhere molten core might dropmay be dropped to water.

I-17.I-19. For the practical elimination ofeliminating steam explosions that could damage the integrity of the containment barrier, the preferred method is to avoid the dropping of molten core into water for allin any 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 ofdesigned boiling water reactors, the molten core would in all severe accident scenarios drop to a pool below the reactor vessel in all severe accident scenarios and wouldand be solidified and cooled in the pool. In allany such circumstances in which thewhere 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 ofrisks from steam explosion damagingto the containment integrity hashave been practically eliminated owing to the physical impossibility of the event sequence. . The role of probabilistic safety assessment in this demonstration, if there is one at all, is very limited.

EXPLOSION OF COMBUSTIBLE GASES: HYDROGEN AND CARBON MONOXIDE

I-18.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 atofof hydrogen in critical concentrations, and to eliminate hydrogen detonation, are needed at all nuclear power plants, although different means are preferred for different plant designs.

I-19.I-21. In boiling water reactor containments, which that 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-20.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 eliminateseliminate excessive local hydrogen concentration, taking into account thatconcentrations. Furthermore, the risk of hydrogen detonation increases if steam providing inertization is condensed.

Commented [AKE329]: is this subsection about 2 separate things:
1.hydrogen generation and accumulation
2.hydrogen detonation

Commented [LHJ330R329]: Yes, first prevention and then mitigation

Commented [AKE331]: correct? only the first thing? or also detonation?

Commented [LHJ332R331]: Yes, it is right

I-21.I-23. The consequences of hydrogen combustionConsequences will depend onbe sensitive to the highest conceivable rate and the total amount of hydrogen generation inside the containment. Some of the current core catchers that are currently installed in nuclear power plants can significantly reduce or even eliminate the ex-vessel hydrogen generation in anthe accident phase when the molten core has dropped to the catcher, and this could bring major reduction also considerably reduceto the total amount of hydrogen generated inside the containment.

I-22.I-24. In particular, TtheThe design provisions for preventing hydrogen detonation alsoalso 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.

Commented [AKE333]: see comment in first para in this subsection

Commented [LHJ334R333]: text modified

I-23.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 thisthe chemical reaction is less energetic than the hydrogen combustion and the burning velocity is also lower. Therefore, the contribution of carbon monoxide to the risks to thethreats of 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 .. A practical elimination of hydrogen combustion. A design provisionmeasure to minimize the impact of carbon monoxide is the use concrete with low contents of limestone.

LONG TERM LOSS OF CONTAINMENT HEAT REMOVAL

I-24.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 meansmean for preventing its overpressure.

I-25.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 mightmaymay be capable of supporting theaa demonstration oftoto practical elimination are considered to practically eliminate the risk of containment rupture by overpressure.

I-26.I-28. An alternative to cooling ofis to eliminate 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 mightmay be needed for design basis accidents and design extension conditionsboth in the DBA as well as in DEC with core melt. The existing 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, may 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-27.I-29. Containment venting avoids a riskthreat to the containment integrity due to overpressurization, but the stabilization of the core and the cooling of the containment are still necessary in the longer term.

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

CONTAINMENT PENETRATION BY INTERACTION WITH THE MOLTEN CORE

~~I-29.~~I-31. In~~ the event of~~ a severe accident in which the core has melted through the reactor vessel, it is possible that containment integrity could be breached if the molten core is not sufficiently cooled. In addition, interactions between the core debris and concrete can generate large quantities of additional combustible gases, hydrogen and carbon monoxide, as well as other non-condensable gases, which could contribute also to eventual overpressure failure of the containment.

~~I-30.~~I-32. Alternative means have been developed and verified in extensive severe ~~reactor~~ accident research programmes~~programs~~ in this area conducted in several States~~nationally~~ and also with~~in~~ international co-operation. The means suggested include the following:

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

~~I-31.~~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-32.~~I-34. While probabilistic safety assessment can play a role in~~on~~ 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 ~~melt through~~ 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-33.~~ 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~~as well as~~ 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 ~~All these~~ conditions. Nevertheless, all these event sequences have to be ~~'~~practically eliminated~~eliminated'~~ by design provisions such as adequate piping design pressure and isolation mechanisms.

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

Commented [AKE335]: yes? below you talk about core catcher cooling

Commented [LHJ336R335]: Yes, agree

Formatted: No bullets or numbering

I-35. The safety demonstration for elimination of bypass sequences includesneeds to include a systematic review of all potential containment bypass sequences and coverscover all containment penetrations.

I-36. 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 penetrationpenetrations. 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 interfaceinterfaceing systems loss of cooling accidents.

Commented [AKE337]: this is the only example that highlights a particular requirement

I would delete this entire para actually, as it makes it seem that containment bypass is really something special compared to the other examples

Commented [LHJ338R337]: Yes, but it is special indeed, mainly because containment bypass might lead to a direct large early radioactive release.
I suggest keep it.

I-37. 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 operatorhuman actions, other analysis aspects mightmay involve the use of other probabilistic methods together with deterministic methods and engineering judgement to demonstrate the practical elimination of containment bypass. This would lead on one hand to a defensible low frequency estimate of the bypass mechanisms associated withto each penetration. In addition based. On the other hand, the reliability of design provisions for the isolation of bypass paths based upon conventional probabilistic assessmentsanalysis would complement the demonstration that event sequencessevere accidents with containment bypass have been practically eliminated.

SIGNIFICANT FUEL DEGRADATION IN THE SPENTIRRADIATED FUEL STORAGE POOL

I-38. Facilities for spent fuel storage need to be designed to ensure that event sequences that could lead to an early the potential for high radiation doses or radioactive release or a large radioactive releasereleases 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 involvesrequires 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 sufficientlyredundant andsufficiently 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.

Formatted: Font: 11 pt

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

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

I-40. In designs where the spent fuel pool is outside the containment, the uncovering of the fuel would lead to fuel damage and a large 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.~~eliminated'~~

I-41. In some designs, the spent fuel pool is located inside the containment. In this case, even though ~~the~~ spent fuel damage would not lead directly to a large 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~~would~~ 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~~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–1]~~[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Fuel Handling and Storage Systems for Nuclear Power Plants, IAEASpecificSpecific Safety Standards Series No. Guides, SSG-63, IAEA, Vienna (2020).

ANNEX II.
APPLICATION OF THE CONCEPTS OF DESIGN EXTENSION CONDITIONS AND PRACTICAL ELIMINATIONTOTO 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 event sequencesplant conditions that couldcan lead to an early radioactive releasereleases or ato large radioactive releasereleases need to be assessed as part of the periodic safety review processes (ENISS) with the objective of further improving the level of safety, where reasonably practicable. (ENISS).

II-2. The concepts of design extension conditions and practical elimination of event sequences that could lead to an early radioactive releasereleases or a large radioactive releasereleases are not totally new. In fact, the last concept of practical elimination was already introduced in the 2004 IAEAformer Safety Guide for the design of the reactor containment[28], and both concepts mightmay 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 plant conditions or event sequences that could lead to an early radioactive releasereleasesreleases or a large radioactive releasereleasesreleases to be practically eliminated have been addressed also in many designs already, although a specific demonstration of in accordance with the concept of practical elimination of such event sequences has not been carried out.

II-3. In relation to practical elimination, a number of measures mightmay 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 spentirradiated fuel poolstorage. However, a demonstration that the existing safety provisions are sufficient to claim the practical elimination of such event sequencesconditions 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,It is important to note however, that an accident condition commonly considered as a design extension condition in a new nuclear power plantplants (e.g. station

[28] 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].).).

blackout or anticipated transient~~transients~~ without scram), can~~is~~ only be considered a design extension condition for an existing nuclear power plant~~such~~ if safety features have been introduced in the original design of the existing plant to mitigate the~~its~~ consequences of this condition.~~. Otherwise, it would remain a beyond design basis accident.~~ For the case of station blackout, an alternate power source capable of supplying power in due time to essential loads over a sufficient time period until external or emergency power is recovered would be such an original design safety feature. Likewise, for~~F~~f~~or~~ anticipated transient~~transients~~ without scram, additional design features capable of rendering ~~are necessary to render~~ the reactor subcritical in case of failure in the insertion of control rods, would need to have been included in the original design. Without such additional design features in ~~to prevent the failure of the~~ original design, these accident conditions would need to be considered to be beyond the design basis of the plant~~, reactor coolant system~~.

Commented [AKE339]: ok to avoid 'beyond design basis accident'?

Commented [LHJ340R339]: Yes. This means the event sequences there are part of the residual risk for those plants. Higher than for new plants, but this is the maximum we can do.

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~~a~~ feasibility of reasonable safety improvements in relation to design extension conditions and practical elimination would be considered. There can, however, be ~~important~~ constraints on installing~~to installation of~~ 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. In the same context, there can be constraints on ensuring the independence~~the independency~~ of safety provisions relating~~related~~ to the different levels of defence in depth ~~will need to be taken into account~~.

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

Commented [AKE341]: can we delete this bit of the sentence? it's very hard to understand

II-7. Safety systems of existing plants were designed for design basis accidents, without account being taken in~~of~~ the design~~possibility~~ 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~~3.19~~, for design extension conditions without significant fuel degradation, ~~it can be acceptable~~ for postulated initiating events less frequent than those considered for design basis accidents it can be acceptable ~~DBAs~~ to demonstrate that some safety systems would be capable of and qualified for mitigating the consequences of such events if best estimate analyses and less conservative assumptions are used. For ~~This is a possibility 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.

Commented [AKE342]: I think it's not OK to say that existing plants never considered the *possibility* of more severe accidents

Commented [LHJ343R342]: Maybe it is not OK, but it is true, they were not considering in their design those severe accidents.

Commented [AKE344]: ok?

Commented [LHJ345R344]: OK

II-8. The consideration of external events of a magnitude exceeding the original design basis derived from the hazard evaluation for the site, as ~~it is~~ 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~~, derived from the hazard evaluation for the site~~ 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~~may~~ be adequate provided there is a justification to demonstrate that the coping time to prevent the loss of the safety function that the equipment is intended to fulfil is long enough to connect and put into service the equipment under the conditions associated with the accident. The recommendations in this regard provided in Section 5 are~~would be~~ 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 timely 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.

Commented [AKE346]: can we delete this to make the sentence easier to read?

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–2]~~[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–3][II–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-53, IAEA, Vienna (2019).~~

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

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

CONTRIBUTORS TO DRAFTING AND REVIEW

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.	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.	Sweden
Hardwood, C.	Canadian Nuclear Safety Commission (CNSC/CCSN), Canada
Ibrahim, M. A.	
Jansen, R.	
Järvinen, M.L.	
Kim, K.T.	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.	Czech
Rodriguez Mate, C.	Nuclear Safety Authority (ASN) France
Matthieu, B.	EDF
Muellner, N. A.	Austria
Nakajima, N.	Japan
Nuenighoff, K.	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Germany

Formatted Table

~~Obenius Mowitz, A.~~	~~Sweden~~
~~Okano, T.~~	~~Japan~~
~~Poulat, B.~~	~~Consultant~~
~~Ranval, W.~~	~~European Nuclear Installations Safety Standards (ENISS)~~
~~Rogatov, D.~~	~~Russian Federation~~
~~Schwartz, G.R.~~	~~Canada~~
~~Stoppa, G.~~	
~~Tas, F.B.~~	~~Turkey~~
~~Titus. B.A~~	~~US Nuclear Regulatory Commission, USA~~
~~Uhrik, P.~~	~~Slovakia~~
~~Virtanen, E.~~	~~Finland~~
~~Wattellle, E.~~	~~Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France~~
~~WONG, E.K.Y~~	~~Singapore~~
~~Yllera, J.~~	~~International Atomic Energy Agency~~

Formatted Table

Formatted Table

Formatted Table

Formatted Table

DEFINITION

~~DEFINITIONS~~

Formatted: Heading 1,Section Heading, Left

Practical elimination

Ensuring by design ~~SSR-2/1, rev. 1 clarifies in footnotes the usage of the term "practically eliminated" in relation to conditions leading to harmful offsite consequences indicating~~ that event sequences that could lead to an early radioactive release or a large radioactive release are either "~~*The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be*~~ physically impossible ~~*for the conditions to arise*~~ or are~~*if these conditions could be*~~ considered, with a high level of confidence, to be extremely unlikely to arise.~~."~~

Commented [AKE347]: I think we need to 'go for' an actual definition of this term, but am open to further discussion

Formatted: Justified

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

ⓘ The concept of "~~practical elimination~~" is applied in relation to event sequences~~plant conditions that can lead to early radioactive releases or large radioactive releases,~~ for which reasonably practicable technical means for their~~its~~ mitigation cannot be implemented.

Commented [AKE348]: these can be information notes in the Glossary

Formatted: Justified, Indent: Left: 1 cm

ⓘ Practical elimination~~Due to the important consequences of failing to prevent such conditions from happening, practical means need to be implemented to prevent them and a very solid demonstration~~ is ~~necessary to affirm that such conditions have been practically eliminated. This means they are extremely unlikely to occur or even physically impossible~~

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

~~Warning: The concept of 'practical elimination' must not be misinterpreted or misused. It is to be considered as~~ part of a general approach to design safety and is ~~its appropriate application as~~ an enhancement of the application of the concept of defence in depth.

CONTRIBUTORS TO DRAFTING AND REVIEW

Commented [AKE349]: I put the CONTRIBUTORS at the end, after the Definition

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
Matthieu, B.	DIPNN, Electricité de France (EDF), France
Muellner, N. A.	University of Natural Resources and Life Sciences, Institute for Safety and Risk Sciences, Vienna, Austria

Formatted Table

Formatted Table

Formatted Table

Formatted Table

Formatted Table

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

Formatted Table

Formatted Table

Formatted Table

Formatted: Font: 10 pt

Formatted: Justified, Indent: Left: 1 cm