6 April 2017

IAEA SAFETY STANDARDS

for protecting people and the environment

Step 11a

Submitting the draft to review by the review Committees

Deterministic Safety Analysis for Nuclear Power Plants

SSG-2 Rev. 1

DS491

DRAFT Revised SAFETY GUIDE

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide provides recommendations and guidance on the use of deterministic safety analysis and its application to nuclear power plants in compliance with the IAEA's Safety Requirements publications on Safety of Nuclear Power Plants: Design, SSR-2/1 (Rev. 1) [1] and Safety Assessment for Facilities and Activities, GSR Part 4 (Rev.1) [2].

1.2. Current developments for ensuring the stable and safe operation of nuclear reactors are closely related to the advances that are being made in safety analysis. Deterministic safety analyses for normal operation, anticipated operational occurrences, design basis accidents and design extension conditions including severe accidents, as defined in Ref. [1] and in the IAEA Safety Glossary [3], are essential instruments for confirming the adequacy of safety provisions.

1.3. This Safety Guide supersedes the guidance provided in the previous version[1]. The modifications incorporated in this Safety Guide reflect recent experience with deterministic safety analysis included in Safety Analysis Reports for present reactor designs and with various applications of deterministic safety analysis of existing nuclear power plants. Updating of the Safety Guide is also aimed at ensuring consistency with current IAEA Safety Standards, including updating of Safety Standards implemented with lessons from the Fukushima Daiichi nuclear power plant accident.

OBJECTIVE

1.4. The objective of this Safety Guide is to provide recommendations and guidance on performing deterministic safety analysis and its application to nuclear power plants for designers, operating organizations, regulatory bodies and technical support organizations. It also provides recommendations on the use of deterministic safety analysis in:

(a) Demonstrating or assessing compliance with regulatory requirements;

(b) Identifying possible enhancements of safety and reliability.

The recommendations are based on the safety requirements established in SSR 2/1 (Rev. 1) [1] and GSR Part 4 (Rev. 1) [2] and supported by current practices and experience from deterministic safety analysis being performed for nuclear power plants around the world.

SCOPE

1.5. This Safety Guide applies to nuclear power plants. It addresses the ways for performing deterministic safety analyses that are required to demonstrate adequate fulfilment of safety functions

[1] Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009).

in order to ensure that barriers to the release of radioactive material will prevent an uncontrolled release to the environment for all plant states. Deterministic safety analyses are required to determine the characteristics of the releases (source term) depending on the status of the barriers for different plant states.

1.6. This Safety Guide focuses primarily on the deterministic safety analysis for the design safety of new nuclear power plants and, as far as reasonably practicable or achievable, also the safety re-evaluation or assessment of existing nuclear power plants when operating organizations review their safety assessment. The guidance provided is intended to be as much as possible consistent with paras 1.3 and 1.6 of SSR-2/1 (Rev. 1) [1] and it is particularly based on experience with deterministic safety analysis for water cooled reactors.

1.7. The guidance provided in this Safety Guide focuses on best practices in the analysis of all plant states considered in the design, from normal operation through anticipated operational occurrences and design basis accidents up to design extension conditions including severe accidents.

1.8. Regarding deviations from normal operation this Safety Guide deals with human errors and failures of plant systems (e.g. systems from the reactor core, reactor coolant system, containment, fuel storage or other systems containing radioactive material) having the potential to affect the performance of safety functions and thus leading to loss of physical barriers against releases of radioactive material. Analysis of hazards themselves, either internal or external (natural or human induced) is not covered by this Safety Guide, although the effects and loads potentially inducing the failures in plant systems are taken into account in determining initiating events to be analysed.

1.9. This Safety Guide is devoted to the deterministic safety analysis for design or licensing purposes, which are aimed at demonstrating, with adequate margins, compliance with acceptance criteria.

1.10. This Safety Guide covers different options available for performing deterministic safety analysis, whether conservative or not.

1.11. This Safety Guide focuses on neutronic, thermal-hydraulic, fuel (fuel channel for pressurized heavy water reactors) and radiological analysis. Other types of analysis, in particular structural analysis of components and structures, are also important means of demonstrating the safety of a plant. However, detailed guidance on performing such analysis is not included in this Safety Guide since such information can be found in specific engineering guides. It is also clear that neutronic and thermal-hydraulic analysis provides necessary boundary conditions for structural analysis.

1.12. The extent of radiological analysis in this Safety Guide includes the transport of radioactive material within the buildings and structures of the nuclear power plant, in particular in anticipated operational occurrences and accident conditions, as one of the inputs for determining the radiation doses to the nuclear power plant staff (see GSR Part 3) [4]. The aspects going beyond the determination of source term release to the environment, such as dose calculation, radioactive gaseous

and liquid effluent calculations or dispersion of radioactive substances in the environment, are not covered by this Safety Guide. It is however recognized that minimization of exposures and optimizing radiation protection is a much more complex issue, which primarily includes such measures as minimization of radiation sources, appropriate nuclear power plant configuration, adequate shielding and ventilation design, limitation of staff exposure time and monitoring of staff exposure. Determination of the doses to personnel at the nuclear power plant is therefore not covered by this Safety Guide.

1.13. This Safety Guide also covers aspects of the analysis of releases of radioactive material, up to and including the determination of the source term to the environment for anticipated operational occurrences and accident conditions (paras 2.16 to 2.18). Radioactive gaseous and liquid effluents and discharges during normal operation are primarily controlled by operational measures and are not covered by this Safety Guide. Similarly, dispersion of radioactive material in the environment and prediction of the radiological effects on people and non-human biota is outside the scope of this Safety Guide. While general rules for deterministic safety analysis apply also to the analysis of radiological consequences of anticipated operational occurrences and accident conditions, this Safety Guide does not provide specific guidance for such analysis. Such specific guidance can be found in other IAEA Safety Guides, e.g. Ref. [5].

1.14. This Safety Guide provides general rules and description of processes to be followed in performing deterministic safety analysis. The Safety Guide does not describe specific phenomena and does not identify the key factors essential for neutronic, thermal-hydraulic and radiological analysis. When such kind of information is provided in this Safety Guide it is meant as illustration or example of the processes and should not be understood as a comprehensive description.

Interface between safety and security regarding deterministic safety analysis

1.15. Recommendations on security are out of the scope of this Safety Guide. While in general, documentation and electronic records related to deterministic safety analysis process and outputs provide~~,~~ limited information regarding equipment location and vulnerability and practically no information on cable routes and other aspects of the plant layout, such information needs to be reviewed with regard to containing sensitive information that could be used to support malicious actions. Considerations of sensitive information and guidance on the security of nuclear information are further discussed in Ref. [6].

STRUCTURE

1.16. This Safety Guide consists of nine sections and one annex. Section 2 introduces some basic concepts and terminology used in the area of deterministic safety analysis. It includes general statements necessary as basis for the specific guidance provided in the other sections of this Safety

Guide; the sequence of these sections corresponds to the general approach, in terms of process, to perform deterministic safety analysis.

1.17. Section 3 describes methods of systematic identification, categorization and grouping of initiating events and accident scenarios to be addressed by deterministic safety analysis. The section includes practical advice on selection of events to be analysed for the different plant states.

1.18. Section 4 provides a general overview of acceptance criteria to be used in deterministic safety analysis for design and authorization of nuclear power plants and describes the rules for determination and use of acceptance criteria. Section 5 provides guidance for verification and validation, selection and use of computer codes and plant models, together with input data used in the computer codes.

1.19. Section 6 describes general approaches for ensuring adequate safety margins in demonstrating compliance with acceptance criteria for all plant states, with focus on anticipated operational occurrences and design basis accidents. The guidance provided covers conservative and best estimate approaches for addressing uncertainties and for ensuring adequate margins in safety analysis.

1.20. Section 7 provides specific guidance on performing deterministic safety analysis for each individual plant state.

1.21. Section 8 includes guidance on documentation, review and update of deterministic safety analysis. Section 9 provides guidance for independent verification of safety assessment, including verification of deterministic safety analysis.

1.22. Annex I indicates additional applications of the computer codes used for deterministic safety analysis, besides the nuclear power plant design and authorization.

2. GENERAL CONSIDERATIONS

OBJECTIVES OF DETERMINISTIC SAFETY ANALYSIS

2.1. The objective of deterministic safety analysis for nuclear power plants is to confirm that safety functions and the needed systems, structures and components, in combination where relevant with operator actions, are capable and sufficiently effective, with adequate safety margins, to keep the releases of radioactive material from the plant within acceptable limits. Deterministic safety analysis is aimed to demonstrate that barriers to the release of radioactive material from the plant will maintain their integrity to the extent required. Deterministic safety analysis, supplemented by further specific information and analysis such as those related to fabrication, testing, inspection, evaluation of the operating experience and by probabilistic safety analysis, is also aimed to contribute to demonstrate that the source term and eventually radiological consequences of different plant states are acceptable and that the possibility of certain conditions arising that could lead to an early radioactive release or a large radioactive release can be considered as ‘practically eliminated’ (see para. 3.55).

2.2. The deterministic safety analyses performed for different plant states is aimed to demonstrate adequacy of the engineering design in combination with the envisaged operator actions by demonstrating compliance with established acceptance criteria.

2.3. Deterministic safety analyses predict the response to postulated initiating events possibly combined with additional postulated failures. A set of rules and acceptance criteria specific to each plant state is applied. Typically, these analyses focus on neutronic, thermal-hydraulic, thermal mechanic, structural and radiological aspects, which are often analysed with different computational tools. Computational simulations are carried out specifically for predetermined operating modes and plant states.

2.4. The results of computations are spatial and time dependent values of various physical variables (e.g. neutron flux; thermal power of the reactor; pressures, temperatures, flow rates and velocities of the primary coolant; loads to physical barriers; concentrations of combustible gases, physical and chemical compositions of radionuclides, status of core degradation or containment pressure, source term to the environment and others).

ACCEPTANCE CRITERIA FOR DETERMINISTIC SAFETY ANALYSIS

2.5. Acceptance criteria are used in deterministic safety analysis for judgment of acceptability of the demonstration of safety of a nuclear power plant. The acceptance criteria can be expressed either in general, qualitative terms or as quantitative limits. Three categories of criteria can be recognized:

(a) Safety criteria: these are criteria either directly related to the consequences of operational states or accident conditions or to the integrity of barriers against releases of radioactive material;

(b) Design criteria: design limits for individual structures, systems and components, that are part of the design basis as important preconditions for meeting safety criteria (see Requirement 28 from SSR-2/1 (Rev. 1) [1]; and

(c) Operational criteria: these are rules to be followed by operator during normal operation and anticipated operational occurrences; they provide preconditions for meeting the design criteria and ultimately the safety criteria.

2.6. In this Safety Guide only the safety acceptance criteria that are the targets of the deterministic safety analysis are addressed. These acceptance criteria, as approved by the regulatory body, may include margins with respect to safety criteria.

UNCERTAINTY ANALYSIS IN DETERMINISTIC SAFETY ANALYSIS

2.7. In this Safety Guide, uncertainty analysis is addressed in paras 6.21 to 6.29. Several methods for performing uncertainty analysis have been published (e.g. in Safety Report Series No. 52 [7]). They include:

(a) Use of a combination of expert judgement, statistical techniques and sensitivity calculations;

(b) Use of data from scaled experiments;

(c) Use of bounding scenario calculations.

APPROACHES TO DETERMINISTIC SAFETY ANALYSIS

2.8. Table 1 lists different options currently available for performing deterministic safety analyses with different levels of conservatism associated with the computer code (see Section 5), availability of systems and initial and boundary conditions for the analysis.

TABLE 1. OPTIONS FOR PERFORMING DETERMINISTIC SAFETY ANALYSIS

Option number and title	Computer code type	Assumptions on systems availability	Type of initial and boundary conditions
1. Conservative	Conservative	Conservative	Conservative
2. Combined	Best estimate	Conservative	Conservative
3. Best estimate plus uncertainty	Best estimate	Conservative	Best estimate; partly most unfavourable conditions
4. Realistic[2]	Best estimate	Best estimate	Best estimate

2.9. Option 1 is a conservative approach where both the assumed plant conditions and the physical models are set conservatively. The concept of conservative approach was incorporated in the early days of safety analysis to simplify the analysis and to balance limitations in modelling and insufficient knowledge of physical phenomena with large conservatisms. In a conservative approach any parameter need to be allocated a value that will have an unfavourable effect in relation to specific acceptance criteria. The reasoning was that such an approach would bound many similar transients in a way that the acceptance criteria would be met for all of them.

2.10. At present, experimental research has resulted in a significant increase of knowledge and the development of computer codes has improved the ability to achieve calculated results that correspond more accurately to experimental results and recorded event sequences in nuclear power plants. Due to the improved capabilities of computer codes and the possible drawbacks of the conservative approach

[2] For simplicity in this Safety Guide the term “realistic approach” or “realistic analysis” is meant “Best Estimate without quantification of uncertainties”

(potential masking of important phenomena, counter effects of various parameters) option 1 is rarely used now and not suggested for current safety analysis unless situations when scientific knowledge and experimental support is limited. Option 1 remains also in legacy analysis.

2.11. Option 2 is a combined approach based on the use of 'best estimate' models and computer codes instead of conservative ones (para. 6.12). Best estimate codes are used in combination with conservative initial and boundary conditions, as well as with conservative assumptions regarding the availability of systems, assuming that all uncertainties associated with the code models are well established and plant parameters are conservative based on plant operating experience. The complete analysis requires use of sensitivity studies to justify conservative selection of input data. Option 2 is commonly used for design basis accidents and for conservative analysis of anticipated operational occurrences.

2.12. Option 3 is so called best estimate plus uncertainty approach. This allows the use of best estimate computer codes together with more realistic hypotheses. Best estimate and partially unfavourable initial and boundary conditions may be used taking into account the very low probability that all parameters would be at their most detrimental value at the same time. However, in order to ensure the conservatism required in analysis of design basis accidents the uncertainties need to be identified, quantified and statistically combined. Availability of systems is usually assumed in a conservative way. Option 3 contains a certain level of conservatism and is at present accepted for some design basis accidents and for conservative analyses of anticipated operational occurrences.

2.13. In principle, Options 2 and 3 are distinctly different types of analysis. However, in practice, a mixture of Options 2 and 3 is employed. This is because whenever extensive data are available, the tendency is to use best estimate input data, and whenever data are scarce, the tendency is to use conservative input data. The difference between these options is the statistical combination of uncertainties. In Options 1, 2 and 3, conservative assumptions are made about the availability of plant systems.

2.14. Deterministic safety analysis performed according to options 1, 2 and 3 is considered conservative analysis, with a decreasing level of conservatism from options 1 to 3 (see paras 2.9 to 2.13 above).

2.15. Option 4 allows the use of best estimate code modelling, system availability assumptions and initial and boundary conditions. Option 4 may be appropriate for realistic analysis of anticipated operational occurrences aimed at assessment of control system capability (paras 7.17 to 7.44) and in general for best estimate analysis of design extension conditions (paras 7.45 to 7.67) as well as for the realistic analysis with the purpose of justification of operator actions. Deterministic analysis for operating events that may require short term relaxation of regulatory requirements may rely also on best estimate modelling. More detailed information regarding modelling assumptions applicable for different options is provided in section 7 of this Safety Guide.

SOURCE TERM TO THE ENVIRONMENT

2.16. Deterministic safety analysis includes as one of its essential components determination of the source term as a key factor for prediction of dispersion of radioactive material to the environment and eventually doses to the plant staff, to the public and radiological impact on the environment. In accordance with Ref. [3] (IAEA Safety Glossary) the source term is 'the amount and isotopic composition of material released (or postulated to be released) from the facility'; it is 'used in modelling releases of radionuclides to the environment, particularly in the context of accidents at nuclear installations or releases from radioactive waste in repositories'.

2.17. To evaluate the source term from a nuclear installation, it is necessary to identify the sources of radiation, to evaluate the inventories of radionuclides that are produced and to know the mechanisms of transmission of radioactive material from the source through the installation and released to the environment. Under accident conditions, source term evaluation requires simulation code capabilities dealing with fission product release from fuel elements, transport through primary system and containment or spent fuel pool building and related chemistry.

2.18. The source term is evaluated for operational states and accident conditions for the following reasons:

(a) To ensure that the design is optimized so that the source term will be reduced to a level that is as low as reasonably achievable in all plant states;

(b) To support the demonstration that the possibility of certain conditions arising that could lead to an early radioactive release or a large radioactive release can be considered to have been 'practically eliminated';

(c) To demonstrate that the design ensures that requirements for radiation protection, including restrictions on doses, are met;

(d) To provide a basis for the emergency arrangements[3] that are required to protect human life, health, property and the environment in case of an emergency at the nuclear power plant;

(e) To specify the conditions for the qualification of the equipment required to withstand accident conditions;

(f) To provide data for training activities regarding emergency arrangements;

[3] This application and the establishment of such arrangements are beyond the scope of this Safety Guide. Requirements regarding these arrangements are established in GSR Part 7 (Preparedness and Response for a Nuclear or Radiological Emergency, 2015) [8] and recommendations are provided in GS-G-2.1 (Arrangements for Preparedness for a Nuclear or Radiological Emergency, 2007) [9] and GSG-2 (Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, 2011) [10].

(g) To support the design of safety features and safety systems for the mitigation of severe accidents (e.g. filtered containment venting and recombiners of combustible gases; see NS-G-2.15 [11]).

2.19. General rules presented in this Safety Guide fully apply also to determination of the source term. In several places of this Safety Guide aspects associated with determination of the source term are introduced to remind applicability of the general rules for this specific application.

3. IDENTIFICATION, CATEGORIZATION AND GROUPING OF POSTULATED INITIATING EVENTS AND ACCIDENT SCENARIOS

3.1. In accordance with the definition of "plant states (considered in the design)" from SSR-2/1 (Rev. 1), page 65 [1], the plant states considered in the deterministic safety analysis should cover:

(a) Normal operation;

(b) Anticipated operational occurrences;

(c) Design basis accidents;

(d) Design extension conditions, including sequences without significant fuel degradation and sequences with core melting.

3.2. The deterministic safety analysis should consider the postulated initiating events originated in any part of the plant potentially leading to a radioactive release to the environment, with consideration also of additional failures, e.g. in the control and limitation systems[4] and the associated safety functions. This includes events that can lead to a release of radioactivity not only from the reactor core but from other relevant sources such as fuel elements stored at the plant and systems dealing with radioactive material.

3.3. Where applicable, it should be considered that a single cause can simultaneously initiate postulated initiating events in several or even all reactors, spent fuel storage and any other sources of potential radioactive releases on the given site (SSR 2/1 (Rev. 1), para. 5.15B) [1].

3.4. The deterministic safety analysis should address postulated initiating events that can occur in all modes of normal operation. Initial conditions should consider a controlled plant mode with normal operation equipment operating prior to the initiating event.

3.5. Every configuration of shutdown modes including refuelling and maintenance should be considered. For these modes of operation, contributors potentially increasing risk should be considered, such as the inability to start some safety systems automatically or manually; disabled

[4] In this Safety Guide, the term 'control and limitation systems' refers not only to the instrumentation systems for control and limitation of the plant variables but also the systems for normal operation and those for anticipated operational occurrences actuated by them.

automation systems; equipment in maintenance or in repair; reduced amounts of coolant in the primary circuit as well as in the secondary circuit for some modes; instrumentation switched off or non-functional and measurements not made; open primary circuit and open containment.

3.6. For postulated initiating events related to the spent fuel pool, specific operating modes related to fuel handling and storage should be considered.

3.7. Postulated initiating events taking place during plant operating modes with negligible duration in time may be excluded from deterministic safety analysis after careful analysis and quantitative assessment of its potential of contribution to the overall risk, including to conditions arising that could lead to an early radioactive release or a large radioactive release. Nevertheless, the need to prevent or mitigate these events with appropriate procedures or means should be addressed on a case by case basis.

MANAGEMENT SYSTEM

3.8. The performance and use of deterministic safety analysis should be conducted taking into account the recommendations of GS-G-3.1 [12] and GS-G-3.5 [13] to meet the requirements 1 to 3 of SSR 2/1 (Rev.1) [1] and GSR Part 2 requirements [14].

NORMAL OPERATION

3.9. Deterministic safety analysis should include analysis of normal operation, defined as operation within specified operational limits and conditions. Normal operation should typically include operating conditions such as:

(a) Normal reactor start-up from shutdown, approach to criticality, and approach to full power;

(b) Power operation, including full power and low power operation;

(c) Changes in reactor power, including load follow modes and return to full power after an extended period at low power, if applicable;

(d) Reactor shutdown from power operation;

(e) Hot shutdown;

(f) Cooling down process;

(g) Cold shutdown;

(h) Refuelling during shutdown or during normal operation at power, where applicable;

(i) Shutdown in a refuelling mode or maintenance conditions that open the reactor coolant or containment boundary;

(j) Normal operation modes of the spent fuel pool;

(k) Storage and handling of fresh fuel.

3.10. It should be taken into account that in some cases during normal operation, the main plant parameters are changing due to the transfer to different plant modes or the changes in the plant power output. A major aim of the analysis for normal operation transients should be to prove that the plant parameters can be kept within the specified operational limits and conditions.

POSTULATED INITIATING EVENTS

3.11. Prediction of the plant behaviour in plant states other than normal operation (anticipated operational occurrences, design basis accidents and design extension conditions) should be based on a plant specific list of postulated initiating events possibly combined with additional equipment failures or human errors for specific event sequences definition.

3.12. A comprehensive list of postulated initiating events should be prepared for ensuring that the analysis of the behaviour of the plant is as complete as possible so that ’all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design’ (SSR-2/1 (Rev. 1), Requirement 16) [1].

3.13. The list of postulated initiating events should take due account of operational experience feedback, which includes, depending on availability of relevant data, operating experience from the actual or from similar nuclear power plants.

3.14. The set of postulated initiating events should be defined in such a way that covers all credible failures, including:

- Failures of structures, systems and components of the plant (partial failure if relevant), including possible spurious actuation;
- Failures initiated by operator errors, which could range from faulty or incomplete maintenance operations to incorrect settings of control equipment limits or wrong operator actions;
- Failures of structures, systems and components of the plant arising from internal and external hazards.

3.15. All consequential failures that a given postulated initiating event could originate in the plant should be considered in the analysis of the plant response as a part of the postulated initiating event. These should include the following:

— If the initiating event is a failure of part of an electrical distribution system, the anticipated operational occurrences, design basis accidents or design extension conditions analysis should assume the unavailability of all the equipment powered from that part of the distribution system;

— If the initiating event is an energetic event, such as the failure of a pressurized system that leads to the release of hot water or pipe whip, the definition of the anticipated operational occurrences, design basis accidents or design extension conditions should consider potential failure of the equipment which could be affected;

— For internal hazards such as fire or flood or external hazards such as earthquakes the definition of the induced postulated initiating event should include failure of all the equipment that is neither designed to withstand the effects of the event nor protected from it.

3.16. Additional failures are assumed in deterministic safety analysis for conservatism (e.g. single failure criterion in design basis accidents) or for the purpose of defence in depth (e.g. common cause failure). Distinction should be made between these additional failures and failures that are part of, or directly caused by, the postulated initiating event. Further failures may be added to bound a set of similar events, limiting the number of analyses.

3.17. The postulated initiating events should only include those failures (either initial or consequential) that directly lead to challenging safety functions and eventually to a threat to barriers against radioactive releases. Therefore hazards, either internal or external (natural or human induced) should not be considered as postulated initiating events by themselves. However, the loads associated with these hazards should be considered a potential cause of postulated initiating events, which includes resulting multiple failures.

3.18. Where the results of engineering judgement, deterministic assessments and probabilistic assessments indicate that combinations of independent events could lead to anticipated operational occurrences or to accident conditions, such combinations of events should be considered to be design basis accidents or should be included as part of design extension conditions, depending mainly on their complexity and frequency of their occurrence.

3.19. The set of postulated initiating events should be identified in a systematic way. This should include a structured approach to the identification of the postulated initiating events such as:

- Use of analytical methods such as hazard and operability analysis (HAZOP), failure modes and effects analysis (FMEA), engineering judgement and master logic diagrams;
- Comparison with the list of postulated initiating events developed for safety analysis of similar plants (ensuring that prior flaws or deficiencies are not propagated);
- Analysis of operating experience data for similar plants;
- Use of probabilistic safety analysis insights and results.

3.20. Certain limiting faults (e.g. large break loss of coolant accidents, main steam or feedwater pipe breaks and control rod ejection in pressurized water reactors or rod drop in boiling water reactors) are traditionally considered in deterministic safety analysis as design basis accidents. These accidents

should be considered because they are representative of a kind of risk the reactor has to be protected from. They should not be excluded from this category of accidents without careful analysis and quantitative assessment of its potential of contribution to the overall risk, including to conditions arising that could lead to an early radioactive release or a large radioactive release.

3.21. Failures occurring in the supporting systems that impede the operation of systems necessary for normal operation should be also considered as postulated initiating events if such failures eventually require the actuation of the reactor protection systems or safety systems.

3.22. The set of postulated initiating events should be reviewed as the design and safety assessments proceed and should involve an iterative process between these two activities. The postulated initiating events should also be periodically reviewed throughout plant life to ensure that they remain valid, for example as part of a periodic safety review.

IDENTIFICATION OF POSTULATED INITIATING EVENTS FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENTS

3.23. Postulated initiating events should be subdivided into representative groups of event sequences taking into account physical evolution of the postulated initiating events. These groups gather event sequences that lead to a similar threat to the safety functions and barriers and the need for similar mitigating systems to drive the plant to a safe state. Therefore, they can be bound by a single representative sequence which is usually referred to when dealing with the group (and often identified by the associated postulated initiating event itself). Then these groups are also categorized according to their frequency of occurrence (see para. 3.27). This approach allows the selection of the same acceptance criteria and initial conditions and the application of the same assumptions and methodologies to all postulated initiating events grouped under the same representative event sequence. As an example, the postulated initiating events “stop of a Main Feed Water (MFW) pump”, “stop of all MFW pumps” and “isolable break on MFW system” are all typically grouped under a single representative event sequence such as “Loss of MFW”.

3.24. Representative event sequences can also be grouped by type of sequences with focus on reduced core cooling and reactor coolant system pressurization, containment pressurization, radiological consequences, or pressurized thermal shocks. In the example above (para. 3.23), the representative sequence “Loss of MFW” belongs to “Decrease in reactor heat removal” type of event sequence.

3.25. The postulated initiating events associated with anticipated operational occurrences and design basis accidents should reflect the specifics of the design. Some typical postulated initiating events and resulting event sequences are suggested in para. 3.28 for anticipated operational occurrences and in para. 3.30 for design basis accidents, according to the typical type of sequences listed below:

- Increase or decrease of the heat removal from the reactor coolant system;
- Increase or decrease of the reactor coolant system flow rate;

- Anomalies in reactivity and power distribution in the reactor core or anomalies in reactivity in the fresh or spent fuel storage;
- Increase or decrease of the reactor coolant inventory;
- Leaks in reactor coolant system with potential containment by-pass;
- Leaks outside containment;
- Reduction or loss of cooling of the fuel in the spent fuel storage pool;
- Loss of cooling to fuel during on-power refuelling (pressurized heavy water reactor);
- Release of radioactive material from a subsystem or component (typically from treatment or storage systems for radioactive waste).

3.26. For analysis of the source term, specific grouping of postulated initiating events may be appropriate to adequately address different pathways to the releases of radioactive material to the environment. Special attention should be paid to accidents in which the release of radioactive material could bypass the containment, because of potentially large consequences even in the case of relatively small releases. Moreover, large bypass accidents do not allow much time for taking action to protect the public in the vicinity of the plant.

3.27. Within each group of postulated initiating events, the representative event sequences should also be subdivided into categories depending on the frequency of the most frequent postulated initiating event in the group. The assignment of each postulated initiating event to the frequency ranges should be checked by an appropriate methodology. Possible anticipated operational occurrences and design basis accident categories used in some States for new reactors are indicated in Table 2.

TABLE 2. EXAMPLE OF ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENT CATEGORIES USED IN SOME STATES

Plant state	Alternative names used in some States	Indicative frequency range ($year^{-1}$)
Anticipated operational occurrences	Faults of moderate frequency, DBC[5]-2, PC-2	f >1E-2
Design basis accidents	Infrequent faults, DBC-3, PC-3	1E-2 > f > 1E-4
	Limiting faults, DBC-4, PC-4	1E-4 > f > 1E-6[6]

[5] DBC: Design Basis Condition; PC: Plant Condition; (DBC-1 and PC-1 are used for 'normal operation')

[6] Some other accidents which frequency is lower than 1E-6 should be considered because they are representative of a kind of risk the reactor has to be protected from.

3.28. Typical examples of postulated initiating events leading to event sequences categorized as anticipated operational occurrences should include those given below, sorted by types of sequences. This list is broadly indicative. The actual list will depend on the type of reactor and the actual design:

— Increase in reactor heat removal: inadvertent opening of steam relief valves; pressure control malfunctions leading to an increase in steam flow rate; feedwater system malfunctions leading to an increase in the heat removal rate;

— Decrease in reactor heat removal: feed water pump trips; reduction in the steam flow rate for various reasons (control malfunctions, main steam valve closure, turbine trip, loss of external load and other external grid disturbances, loss of power, loss of condenser vacuum);

— Increase in reactor coolant system flow rate: start of a main coolant pump;

— Decrease in reactor coolant system flow rate: trip of one or more coolant pumps; inadvertent isolation of one main coolant system loop (if applicable);

— Reactivity and power distribution anomalies in the reactor core: inadvertent control rod (or control rod bank) withdrawal; boron dilution due to a malfunction in the chemical and volume control system (for a pressurized water reactor); wrong positioning of a fuel assembly;

— Reactivity anomalies in the fresh or spent fuel storage: dilution in spent fuel pool;

— Loss of moderator circulation or decrease or loss of moderator heat sink (in pressurized heavy water reactor);

— Increase in reactor coolant inventory: malfunctions of the chemical and volume control system; excessive feedwater flow in boiling water reactors; inadvertent operation of emergency core cooling;

— Decrease in reactor coolant inventory: very small loss of coolant due to the failure of an instrument line;

— Reduction or loss of fuel cooling in the fuel pools: loss of off-site power; malfunctions in decay heat removal system; leaking of pool coolant;

— Release of radioactive material due to leak in reactor coolant system, with potential containment bypass;

— Release of radioactive material due to leak from a subsystem or component: minor leakage from a radioactive waste system or effluents system.

3.29. The subset of postulated initiating events which are considered as leading to design basis accidents should be identified. All postulated initiating events identified as initiators of anticipated operational occurrences should also be analysed using design basis accident rules (SSR-2/1 (Rev.1), para. 5.75(e)) [1]. Although it is not usual to include postulated initiating events with a very low

frequency of occurrence, the establishment of any threshold limit should consider the safety targets established for the specific reactor.

3.30. Typical examples of postulated initiating events leading to event sequences categorized as design basis accident should include those given below, sorted by types of sequences. This list is broadly indicative. The actual list will depend on the type of reactor and actual design:

—Increase in reactor heat removal: steam line breaks;

— Decrease in reactor heat removal: feedwater line breaks;

— Decrease in reactor coolant system flow rate: seizure or shaft break of main coolant pump; trip of all coolant pumps;

— Reactivity and power distribution anomalies: uncontrolled control rod (or control rod bank) withdrawal; control rod ejection (pressurized water reactor); rod drop accident (boiling water reactor); boron dilution due to the startup of an inactive loop (for a pressurized water reactor);

— Decrease in reactor coolant inventory: a spectrum of possible loss of coolant accidents; inadvertent opening of the primary system relief valves; leaks of primary coolant into the secondary system;

—Reduction or loss of fuel cooling in the fuel pools: decrease of coolant inventory due to the break of piping connected to the water of the pool;

— Loss of cooling to fuel during on-power refuelling (pressurized heavy water reactor);

— Loss of moderator circulation or decrease or loss of moderator heat sink for a pressurized heavy water reactor;

— Release of radioactive material due to leak in reactor coolant system, with potential containment bypass, or from a subsystem or component: overheating of or damage to used fuel in transit or storage; break in a gaseous or liquid waste treatment system;

— End-shield cooling failure (pressurized heavy water reactor).

3.31. Probabilistic analysis should be used as a support to justify the categorization of postulated initiating events according to their frequency of occurrence. The calculation of the frequency should take account of the relative frequencies of plant operational states according to its occurrence, such as full power or hot shutdown. It should especially be checked that a transient with potential effects on integrity of barriers has a category consistent with the possible damages on the barriers.

3.32. A reasonable number of limiting cases, which are referred to as bounding or enveloping scenarios, should be selected from each category of events (see para. 3.27). These bounding or enveloping scenarios should be chosen so that they present the greatest possible challenge to the relevant acceptance criteria and are limiting for the performance parameters of safety related equipment. Note that a bounding scenario may combine or amplify the consequences of several

postulated initiating events in order to encompass all the possible postulated initiating events in the group. The safety analysis should confirm that the grouping and bounding of initiating events is acceptable.

3.33. It should be taken into account that a single event should in some cases be analysed from different points of view with different acceptance criteria. A typical example is a loss of coolant accident, which should be analysed for many aspects: degradation of core cooling, containment pressure build–up, radioactivity transport and environmental releases, and specifically for pressurized water reactors as leakage of primary coolant to the steam generator by-passing the containment, pressurized thermal shock and boron dilution (reactivity accident) e.g. due to boiling condensing regime.

3.34. Handling accidents with both fresh and irradiated fuel should also be evaluated. Such accidents can occur both inside and outside the containment.

3.35. In addition, there are a number of other different types of postulated initiating events that would result in a release of radioactive material outside the containment and whose source term should be evaluated. Such accidents include:

(a) A reduction in or loss of cooling of the fuel in the spent fuel pool when the pool is located outside the containment;
(b) Reactivity anomalies in the fresh or spent fuel;
(c) An accidental discharge from any of the other auxiliary systems that carry solid, liquid or gaseous radioactive material;
(d) A failure in systems or components such as filters or delay tanks that are intended to reduce the level of discharges of radioactive material during normal operation;
(e) An accident during reload or maintenance where the reactor or containment might be open.

3.36. The frequency associated with a bounding event sequence belonging to an anticipated operational occurrence or a design basis accident should use the bounding frequency established for the postulated initiating events that have been grouped together.

GENERAL CONSIDERATIONS FOR IDENTIFICATION OF DESIGN EXTENSION CONDITIONS

3.37. In accordance with SSR-2/1 (Rev. 1), Requirement 20 [1], design extension conditions more severe than a design basis accident or involving additional failures, should be identified using engineering judgement, as well as deterministic and probabilistic assessment, with the objective of identifying design provisions to prevent as far as possible such conditions or mitigate their consequences.

3.38. Two separate categories of design extension conditions should be identified: design extension conditions without significant fuel degradation and design extension conditions progressing into core melting, i.e. severe accidents[7]. Different acceptance criteria and different rules for deterministic safety analysis may be used for these two categories.

IDENTIFICATION OF DESIGN EXTENSION CONDITIONS WITHOUT SIGNIFICANT FUEL DEGRADATION

3.39. The initial selection of design extension conditions sequences without significant fuel degradation should be based on the consideration of very low frequency single initiating events or multiple failures, to meet the acceptance criteria regarding core damage prevention.

3.40. A deterministic list of design extension conditions without significant fuel degradation should be developed. The relevant design extension conditions should include:

- Initiating events that could lead to situations beyond the capability of safety systems that are designed for design basis accidents. A typical example is the multiple tube rupture in a steam generator of a pressurized water reactor;
- Anticipated operational occurrences or frequent design basis accidents combined with multiple failures (e.g. common cause failures in redundant trains) that prevent the safety systems from performing their intended function to control the postulated initiating event. A typical example is a loss of coolant accident without actuation of the safety injection. The failures of supporting systems are implicitly included among the causes of failure of safety systems. The identification of these sequences should result from a systematic analysis of the effects on the plant of a total failure of any safety system credited in the safety analysis, for each anticipated operational occurrence or design basis accident (at least for the most frequent ones);
- Credible multiple failures postulated initiating events causing the loss of a safety system while this system is used to fulfil its function as part of normal operation. This applies to those designs that use, for example, the same system for the heat removal in accident conditions and during shutdown. The identification of these sequences should result from a systematic analysis of the effects on the plant of a total failure of any safety system used in normal operation.

3.41. Although design extension conditions are, to a large extent, technology and design dependent, the list below should be used as preliminary reference of design extension conditions without significant fuel degradation and specifically adapted to the type and design of the plant:

[7] In some States these two categories of design extension conditions are denoted as design extension conditions A and design extension conditions B.

- Very low frequency initiating events typically not considered as design basis accidents
  - Uncontrolled heterogeneous boron dilution (pressurized water reactor);
  - Multiple steam generator tube ruptures (pressurized water reactor, pressurized heavy water reactor);
  - Main steam line break and induced steam generator tube ruptures (pressurized water reactor, pressurized heavy water reactor);
- Anticipated operational occurrences or design basis accidents combined with multiple failures in safety systems
  - Anticipated transient without scram: anticipated operational occurrences combined with the failure of rods to insert;
  - Station blackout: loss of offsite power combined with the failure of the emergency diesel generators or alternative emergency power supply;
  - Total loss of feed water: loss of main feedwater combined with total loss of emergency feedwater;
  - Loss of coolant accident together with the complete loss of one type of emergency core cooling feature (either the high pressure or the low pressure part of the emergency core cooling system);
  - Loss of required safety systems in the long term after a postulated initiating event;
- Multiple failures postulated initiating events
  - Total loss of the component cooling water system or of the essential service water system;
  - Loss of the residual heat removal system during cold shutdown or refuelling;
  - Loss of the cooling systems designed for normal cooling and for design basis accidents in the spent fuel pool;
  - Loss of normal access to the ultimate heat sink.

3.42. For the identification of design extension conditions without significant fuel degradation, specific attention should be paid to auxiliary and support systems (e.g. ventilation, cooling, electrical supply) as some of these systems may have the potential of causing immediate or delayed consequential multiple failures in both operational and safety systems.

3.43. Different design extension conditions sequences without significant fuel degradation associated with similar safety challenges should be grouped. Each group should be analysed through a bounding scenario that presents the greatest challenge to the relevant acceptance criteria.

3.44. Multiple failures considered in each sequence of design extension conditions without significant fuel degradation should be specifically listed.

IDENTIFICATION OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING

3.45. A selection of specific sequences with core melting (severe accidents) should be made in order to establish the design basis for the safety features for mitigating the consequences of core melting accidents, according to the plant safety objectives. These sequences should be selected in order to represent all main physical phenomena (e.g. primary circuit pressure, reactor decay heat or containment status) involved in core melt sequences.

3.46. Deterministic safety analysis should consider that the features to prevent core melting fail or are insufficient, and that an accident sequence will further evolve into a severe accident. Some representative sequences should be selected by considering additional failures or incorrect operator responses to the design basis accident or design extension condition sequences and to the dominant accident sequences identified in the probabilistic safety analysis.

3.47. Representative design extension condition sequences with core melting, regarding each criterion, should be analysed to determine limiting conditions, particularly those that could challenge containment integrity. The representative sequences should be used to provide input to the design of the containment and of those safety features necessary to mitigate the consequences of such design extension conditions.

3.48. Although design extension conditions are, to a large extent, technology and design dependent, the accidents below are provided as a preliminary reference of design extension conditions with core melt (severe accidents):

- Loss of core cooling capability, such as an extended loss of off-site power with partial or total loss of on-site AC power sources (exact sequence is design dependent), or/and the loss of the normal access to the ultimate heat sink;
- Loss of reactor coolant system integrity, such as loss of coolant accidents without the availability of emergency core cooling systems or exceeding their capabilities.

3.49. The low frequency of occurrence of an accident with core melting is not sufficient reason for failing to protect the containment against the conditions generated by such an accident. Core melt conditions should be postulated regardless of the provisions implemented in the design. To exclude containment failure, the analysis should demonstrate that very energetic phenomena that may result from core melt accident should be prevented (i.e. the possibility of the conditions arising may be considered to have been ‘practically eliminated’).

3.50. Representative sequences of design extension conditions with core melting should be selected to identify the most severe plant parameters resulting from the severe accident phenomena. These parameters should be considered in the deterministic analyses of the plant structures, systems and components necessary to demonstrate the limitation of the radiological consequences of such severe accident sequences. The analysis of these sequences should provide the environmental conditions to

be taken into account in the assessment[8] on whether the equipment used in severe accidents are capable of performing their intended functions when necessary (see Requirement 30 from SSR-2/1 (Rev.1) [1]).

IDENTIFICATION OF POSTULATED INITIATING EVENTS DUE TO INTERNAL AND EXTERNAL HAZARDS

3.51. Determination of postulated initiating events should consider effects and loads from events caused by relevant site specific internal and external hazards (SSR-2/1 (Rev.1), Requirement 17, paras 5.15A to 5.21A) [1]. A list of external hazards can be found in NS-R-3 (Rev. 1) [15]. Analysis of internal and external hazards differs from analysis of postulated initiating events and scenarios originated by a single failure or multiple failures in the nuclear power plant technological systems or by erroneous human actions having direct impact on performance of fundamental safety functions[9]. The hazards themselves do not represent initiating events but they are associated with loads which can initiate such events.

3.52. In accordance with SSR-2/1 (Rev.1), paras 5.15B, 5.19 and 5.63 [1], in determination of postulated initiating events caused by site specific hazards for multiple unit plant sites the possibility to impact several or even all units on the site simultaneously should be taken into account. Specifically, the effects from losing the electrical grid, those from losing the ultimate heat sink and the failure of shared equipment should be taken into account.

3.53 The analysis of hazards[10] which is performed by using probabilistic methods or appropriate engineering methods should demonstrate that either:

- Such hazard can be screened out due to its negligible contribution to risk; or
- The nuclear power plant design is robust enough to prevent any transition from the load into an initiating event; or
- The hazard causes an initiating event considered in the design.

3.54. In cases where an initiating event is caused by a hazard, the analysis should only credit structures, systems and components that are qualified or protected for the hazard.

---

[8]. Although equipment qualification is out of the scope of this Safety Guide, it is understood that typical equipment qualification programmes for these accident conditions may not always be applicable and an assessment on the operability of structures, systems and components is acceptable; according to that, the term ‘survivability assessment’ is used in some States.

[9] According to the IAEA Safety Glossary [3] the term ‘main safety function’ is equivalent.

[10] Available guidance includes: NS-G-1.5 [16], NS-G-1.7 [17] and NS-G-1.11 [18] (Note: NS-G-1.7 and NS-G-1.11, together, are under DS494 (Step 5): Protection against Internal Hazards in the Design of Nuclear Power Plants).

EVENT SEQUENCES AND ACCIDENT SCENARIOS TO BE 'PRACTICALLY ELIMINATED'

3.55. According to SSR-2/1 (Rev. 1), para. 2.13 (4) [1], "The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release[11] are required to be 'practically eliminated'[12]". (See paras 7.68 to 7.72).

3.56. The event sequences requiring specific demonstration of their 'practical elimination' should be classified as follows:

1) Events that could lead to prompt reactor core damage and consequent early containment failure, such as:
   a. Failure of a large pressure-retaining component in the reactor coolant system;
   b. Uncontrolled reactivity accidents;
2) Severe accident sequences that could lead to early containment failure, such as:
   a. Highly energetic direct containment heating;
   b. Large steam explosion;
   c. Explosion of combustible gases, including hydrogen and carbon monoxide;
3) Severe accident sequences that could lead to late containment failure:
   a. Basemat penetration or containment bypass during molten core concrete interaction (MCCI);
   b. Long term loss of containment heat removal;
   c. Explosion of combustible gases, including hydrogen and carbon monoxide;
4) Severe accident with containment bypass;
5) Significant fuel degradation in a storage fuel pool and uncontrolled releases
6) In-vessel and ex-vessel re-criticality after core melting.

[11] SSR-2/1 (Rev. 1) [1], footnote 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".

[12] SSR-2/1 (Rev. 1) [1], footnote 4: 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.

3.57. Consequences of event sequences that may be considered to have been ‘practically eliminated’ are not part of the deterministic safety analysis. However, deterministic safety analysis contributes to the demonstration that design and operation provisions are effective in the 'practical elimination’ of these sequences (see paras 7.68 to 7.72).

4. ACCEPTANCE CRITERIA FOR DETERMINISTIC SAFETY ANALYSIS

4.1. In accordance with GSR Part 4 (Rev. 1), para. 4.57 [2], the acceptance criteria (criteria for judging safety) should be defined for deterministic safety analysis. These criteria should reflect the criteria used by the designers or operating organizations and should be consistent with the requirements of the regulatory body.

4.2. Requirement 42 from SSR-2/1 (Rev.1), para. 5.75 [1], state that the deterministic safety analysis among other objectives shall mainly provide “comparison of the results of the analysis with acceptance criteria, design limits, regulatory dose limits and acceptable doses”. Compliance with the acceptance criteria should be demonstrated by deterministic safety analysis.

4.3. Acceptance criteria should be established for the entire range of operational states and accident conditions. These criteria should aim at preventing damage to relevant barriers against the release of radioactive material in order to prevent unacceptable radiological releases (thus also the consequences). Selection of the criteria should ensure sufficient margin between the criterion and the physical limit for loss of integrity of a barrier against release of radioactive material.

4.4. Acceptance criteria should be related to the frequency of the relevant conditions. Conditions that occur more frequently, such as normal operation or anticipated operational occurrences should have acceptance criteria that are more restrictive than those for less frequent events such as design basis accidents or design extension conditions.

4.5. Acceptance criteria should be established at two levels as follows:

— High level (radiological) criteria which relate to radiological consequences of plant operational states or accident conditions. They are usually expressed in terms of activity levels or doses typically defined by law or by regulatory requirements;

— Detailed/derived technical criteria which relate to integrity of barriers (fuel matrix, fuel cladding, reactor coolant system pressure boundary, containment) against radioactive releases. They are defined by regulatory requirements, or proposed by the designer subject to regulatory acceptance, for use in the safety demonstration.

4.6. The radiological acceptance criteria should be expressed in terms of effective doses, equivalent doses or dose rates to nuclear power plant staff, the general public or the environment, including non-

human biota, as appropriate. The doses are required to be within prescribed limits and as low as reasonably achievable in all plant states, SSR-2/1 (Rev.1), Requirement 5 [1].

4.7. Radiological acceptance criteria expressed in terms of doses may be conveniently transformed into acceptable activity levels for different radioactive isotopes in order to decouple nuclear power plant design features from the characteristics of the environment.

4.8. Radiological acceptance criteria for normal operation should be typically expressed as effective dose limits for the plant staff and for the members of the public in the plant surroundings, or acceptable planned radioactive releases from the plant, see SSR-2/1 (Rev. 1), Requirement 5, para. 4.4 [1].

4.9. The radiological acceptance criteria for anticipated operational occurrences should be more restrictive than for design basis accidents since their frequencies are higher.

4.10. The radiological acceptance criteria for design basis accidents should ensure that Requirement 19, para. 5.25, from SSR-2/1 (Rev.1) [1], is met.

4.11. The radiological acceptance criteria for design extension conditions to be established should ensure that Requirement 20, para. 5.31A, from SSR-2/1 (Rev.1) [1] is met.

4.12. Technical acceptance criteria should be set in terms of the variable or variables that govern the physical processes that challenge the integrity of a barrier. It is a common engineering practice to make use of surrogate variables[13] related to the integrity of the barriers to establish an acceptance criterion or a combination of criteria for ensuring the integrity of the barrier. When defining these acceptance criteria, a sufficient conservatism should be included to ensure that there are adequate safety margins to the loss of integrity of the barrier.

4.13. For specification of a set of criteria depending on specific design solutions the following groups and examples of criteria should be considered as appropriate:

- Criteria related to integrity of nuclear fuel matrix: maximum fuel temperature, maximum radially averaged fuel enthalpy (both values with their dependence on burn-up and composition of fuel / additives like burnable absorbers);
- Criteria related to integrity of fuel cladding: minimum departure from nucleate boiling ratio, maximum cladding temperature, maximum local cladding oxidation;
- Criteria related to integrity of the whole reactor core: adequate subcriticality, maximum production of hydrogen from oxidation of claddings, maximum damage of fuel elements in the core, maximum deformation of fuel assemblies (as required for cooling down, insertion of absorbers, and de-assembling), calandria vessel integrity (pressurized heavy water reactor);

[13] In this Safety Guide, the use of surrogate variables refers to the use of variables providing an indirect measure of another variable which direct measure is not possible

- Criteria related to integrity of nuclear fuel located outside the reactor: adequate subcriticality, adequate water inventory above the fuel assemblies and adequate heat removal;
- Criteria related to integrity of the reactor coolant system: maximum coolant pressure, maximum temperature, pressure and temperature changes and resulting stresses-strains in the coolant system pressure boundary, no initiation of a brittle fracture or ductile failure from a postulated defect of the reactor pressure vessel;
- Criteria related to integrity of the secondary circuit (if relevant): maximum coolant pressure, maximum temperature, pressure and temperature changes in the secondary circuit equipment;
- Criteria related to integrity of the containment and limitation of releases to the environment: duration and value of maximum and minimum pressure, maximum pressure differences acting on containment walls, leakages, concentration of flammable/explosive gases, acceptable working environment for operation of systems, maximum temperature in the containment;
- Criteria related to integrity of any other component needed to limit radiation exposure, such as end shield in pressurized heavy water reactors: pressure, temperature and heat-up rate.

4.14. For postulated initiating events occurring during shutdown operational regimes or other cases with disabled or degraded integrity of any of the barriers, more restrictive criteria should be preferably used, e.g. avoiding boiling of coolant in open reactor vessel or in the spent fuel pool, or avoiding uncovering of fuel assemblies.

4.15. In particular, technical acceptance criteria related to integrity of barriers should be more restrictive for conditions with higher frequency of occurrence. For anticipated operational occurrences there should be no consequential failure of any of the physical barriers (fuel matrix, fuel cladding, reactor coolant pressure boundary or containment) and no fuel damage (or no additional fuel damage if minor fuel leakage, within operational limits, is authorized in normal operation). For design basis accidents, and for design extension conditions without significant fuel degradation barriers to the release of radioactive material from the plant should maintain their integrity to the extent required (see paras 4.10 and 4.11). For design extension conditions with core melting, containment integrity should also be maintained and containment by-pass prevented to ensure prevention of an early radioactive release or a large radioactive release.

4.16. The range and conditions of applicability of each specific criterion should be clearly specified. For example, specification of fuel melting temperature or fuel enthalpy rise should be associated with specification of fuel burn-up and content of burnable absorbers. Similarly, for limitation of radioactive releases, duration of the releases should be specified. Acceptance criteria can vary significantly depending on conditions. Therefore, acceptance criteria should be associated with sufficiently detailed conditions and assumptions to be used for safety analysis.

4.17. Although the assessment of engineering aspects important to safety may not be explicitly addressed in the safety analysis, it constitutes a relevant part of the safety assessment. Safety margins applied to the design of structures, systems and components should be commensurate with the uncertainty of the loads they have to bear, and with the consequences of their failures.

4.18. In addition to all pertinent physical quantities, the evaluation of stresses and strains should consider the environmental conditions resulting from each loading, each loading combination and appropriate boundary conditions. The acceptance criteria should adequately reflect the prevention of consequential failure of structures or components needed to mitigate the consequences of the events which are correlated to the assumed loading.

5. USE OF COMPUTER CODES FOR DETERMINISTIC SAFETY ANALYSIS

BASIC RULES FOR SELECTION AND USE OF COMPUTER CODES

5.1. According to Requirement 18 from GSR Part 4 (Rev. 1) [2], "Any calculational method and computer codes used in the safety analysis shall undergo verification and validation". The methods used in the computer codes for the calculation should be adequate for the purpose. The requirements for the validation and verification depend on the type of application and purpose of the analysis.

5.2. Regarding the selection of computer codes, it should be confirmed that:

(a) The physical models used to describe the processes are justified;

(b) The simplifying assumptions are justified;

(c) The correlations used to represent physical processes are justified and their limits of applicability are identified;

(d) The limits of application of the code are identified. This is important when the calculational method is only designed to model physical processes over a validity range and the code should not be applied outside this range;

(e) The numerical methods used in the code are robust;

(f) A systematic approach has been used for the design, coding, testing and documentation of the code;

(g) The source coding has been assessed relative to the code specification.

5.3. The assessment of the accuracy of individual codes should include a series of steps:

(a) Identifying the important phenomena in the supporting experimental data and expected plant behaviour;

(b) Estimating uncertainties associated with the numerical approaches used in the code;

(c) Estimating uncertainties in key models used in the code;

(d) Establishing sensitivities in important processes.

5.4. Regarding the outputs of the computer codes, it should be confirmed that the predictions of the code have been compared with:

(a) Experimental data for the significant phenomena modelled. This would typically include a comparison against ‘separate effect test’ (SET) and ‘integral effect test’ (IET), see para. 5.25;

(b) Whenever available, plant data, including tests carried out during commissioning or startup and operational occurrences or accidents;

(c) Outputs of other codes which have been developed independently and use different methods;

(d) Standard problems and/or numerical benchmarks whenever available and reliable;

5.5. Although there has been substantial progress in the development of more accurate and reliable computer codes for accident analysis, the user still has a significant influence on the quality of the analysis. Regarding the users of the code, it should be ensured that:

(a) The users have received adequate training and they appropriately understand the models and the methods used in the code;

(b) The users are sufficiently experienced in the use of the code and appropriately understand its uses and limitations for the application case (e.g. loss of coolant accident);

(c) The users have adequate guidance in the use of the code;

(d) The users follow the recommendation for use of the code and especially the ones relative to the application for which the analysis is carried out.

5.6. Regarding the use of the computer code, it should be confirmed that:

(a) The nodalization (see para 5.38) and the plant models provide a good representation of the behaviour of the plant;

(b) The input data are correct;

(c) The nodalization, selected models and assumptions are consistent, to the extent practicable, with the ones chosen for SET and IET used for the qualification of the application;

(d) The output of the code is evaluated and understood adequately and used correctly.

PROCESS MANAGEMENT IN CONNECTION WITH THE USE OF THE COMPUTER CODES

5.7. All activities that affect the quality of computer codes should be managed. This will require procedures that are specific to ensuring the quality of software. The appropriate software engineering practices that are applicable to the development and maintenance of software critical to safety should be applied. More specifically, formalized procedures and instructions should be put in place for the

entire lifetime of the code, including code development, verification and validation, and a continued maintenance process with special attention to the reporting and correction of errors.

5.8. Code developers should ensure that the planned and systematic actions required to provide confidence that the code meets the functional requirements have been taken. The procedures should address, as a minimum, development control, document control, configuration of the code and testing and corrective actions.

5.9. To minimize human errors in code development, only properly qualified or supervised personnel should be involved in the development, verification and validation of the code. Similarly, in user organizations, only suitably qualified personnel should use the code.

5.10. The activities in the code development and maintenance should include:

(a) Preparation and upgrading of code manuals for developers and users;

(b) Verification and validation activities and their documentation;

(c) Error reporting and corrective actions and their documentation;

(d) Acceptance testing including non-regression tests, installation of the code and upgrading of code manuals;

(e) Configuration management;

(f) Control of interfaces;

(g) Version control of the code.

5.11. If some tasks of code development, verification or validation are delegated to an external organization, those tasks should be managed to ensure quality within the external organization. The user's organization should review arrangements within the external organization and should audit their implementation.

5.12. As new versions of codes are developed, an established set of test cases should be simulated and significant differences from previous versions should be understood. Such simulations should be performed by the code developers and users, as appropriate.

Interface between safety and security regarding the use of the codes

5.13. Computer security measures should be in place to protect the code and development environment from malicious acts and the introduction of new vulnerabilities; see NSS-17 [19].

VERIFICATION OF COMPUTER CODES

5.14. Verification of the code should be performed to demonstrate that the code (source code and algorithm) conforms to the specifications. In general, the verification should ensure that the numerical

methods, the transformation of the equations into a numerical scheme to provide solutions and user options with their restrictions are appropriately implemented in accordance with the specifications.

5.15. In accordance with GSR Part 4 (Rev. 1), para. 4.60 [2], verification of the code should consist of both model verification and system code verification.

5.16. The verification of the code should be performed by means of review, inspection and audit. Checklists might be provided for review and inspection. Audits might be performed on selected items to ensure quality.

5.17. Verification of the code should be performed to review the source coding in relation to its description in the code documentation. The verification should include a review of the design concept, basic logic, flow diagrams, algorithms and computational environment.

5.18. If the code is run on a hardware or software platform (e.g. operating system) other than that the one on which the verification process was carried out, the continued validity of the code verification should be assessed.

5.19. Verification of the source code should be performed to demonstrate that it conforms to accepted programming practices, and that its logic is consistent with the design specification.

5.20. A complex code may contain the integration or coupling of simpler codes. In such cases, verification of the complex code should ensure that the links and/or interfaces between the codes are correctly designed and implemented to meet the design requirements.

VALIDATION OF COMPUTER CODES

5.21. Validation of the code should be performed to determine whether a mathematical model used in the code is an adequate representation of the real system being modelled. Outputs of the code are compared, as far as possible, with observation of the real system or experimental data.

5.22. Validation of the computer code should provide confidence in the ability of a code to predict, realistically or conservatively, the values of the safety parameter or parameters of interest. The level of confidence provided by the validation should be appropriate to the type of analysis; scope of validation might be relaxed for codes used in severe accident analysis, taking into account the limited relevant experimental data, in which case additional reliance should be placed on verification (see paras 5.14 to 5.20).

5.23. Validation of the code should be performed to assess the uncertainty of values predicted by the code. Outputs of the code are compared with relevant experimental data and with operational transients, if possible, for the important phenomena expected to occur.

5.24. For complex analysis, the validation should be performed in two phases: the development phase, in which the assessment is done by the code developer, and the independent assessment phase, in which the assessment is performed by the code user. Both phases are recommended for validation.

5.25. The validation should ideally include comparisons of code outputs with four different types of test:

(1) Basic tests. Basic tests are simple test cases that may not be directly related to a nuclear power plant. These tests may have analytical solutions or may use correlations or data derived from experiments;

(2) Separate effect tests. Separate effect tests address specific phenomena that may occur at a nuclear power plant but do not address other phenomena that may occur at the same time. Separate effect tests should ideally be performed at full scale. If not, appropriate attention should be paid to possible scaling effects (see paras 5.29 to 5.31);

(3) Integral effect tests. Integral tests are test cases that are directly related to a nuclear power plant. All or most of the relevant physical processes are represented. However, these tests may be carried out at a reduced scale, may use substitute materials or may be performed at different boundary conditions;

(4) Nuclear power plant level tests and operational transients. Nuclear power plant level tests are performed on an actual nuclear power plant, for example during the commissioning phase. Validation through operational transients together with nuclear power plant tests are important means of qualifying the plant model.

For (2), (3) and (4) above, in the absence of relevant experimental data it is possible to enhance confidence on results by means of code to code comparison or bounding engineering judgement, to cover deficiencies in the full validation.

5.26. The validation should ideally cover the range of values of parameters, conditions and physical processes that the code is intended to cover. Validation of the code is associated with specific applications.

5.27. The scope of the validation performed by the code user should be consistent with the intended purpose of the code. The scope of validation should also be in accordance with the complexity of the code and the complexity of the physical processes that it represents.

5.28. For complex applications, a validation matrix should be developed for code validation, because a code may predict one set of test data with a high degree of accuracy but may be inaccurate for other data sets. The validation matrix should be adjusted to the application for which the code is validated.

5.29. The validation matrix should include test data from different experimental facilities and different sets of conditions in the same facility, and it should ideally include basic tests, separate effect tests,

integral tests and nuclear power plant level tests. The models and associated assumptions chosen at each level of validation (from basic, separate to integral and nuclear power plant) should be consistent and not adapted depending on the type of tests. If sufficient data from full scale experiments are not available, data from reduced scale experiments should be used, with appropriate consideration of scaling effects. The number and the selection of tests in the test matrix should be justified as being sufficient for the intended application of the code.

5.30. To ensure that the code is validated for conditions that are as close as possible to those in a nuclear power plant, it should be ensured that the boundary conditions and initial conditions of the test are appropriate. Consideration should be given to scaling effects. A scaled experimental facility cannot be used to represent all the phenomena that are relevant for a full size facility. Thus, for each scaled facility that is used in the assessment process, the phenomena that are correctly represented and those that are not correctly represented should be identified. The effects of phenomena that are not properly represented should be addressed in other ways taking into account the applicable level of conservatism.

5.31. When performing a validation against experimental data, allowance for uncertainties in the measurements should be included in the determination of the uncertainty of the computer code. In addition, the evaluation of uncertainties based on scaled experimental results has to be transposed and justified to the uncertainty relative to the real power plant application.

5.32. The range of validity and the limitations of a computer code, which are established as a result of validation, should be documented in a validation report.

5.33. The results of a validation should be used to determine the uncertainty of the results obtained by a code calculation. Different methods are available for assessing the uncertainty of the results.

5.34. For point data, the difference between values calculated using the code and experimental results may be determined directly or, in the case of a set of experimental results, by using descriptive statistics. For time dependent data, as a minimum a qualitative evaluation of the uncertainty should be performed.

5.35. As a result of the validation process, the uncertainty of the code and the range of validation should be known and should be considered in any results of safety analysis calculations.

5.36. For a code intended to be conservative regarding certain acceptance criterion, it should be demonstrated that the code prediction is conservative when compared against the experimental data.

5.37. Results produced by computer codes are sensitive to decisions that are made by the user, such as the models chosen and the number and structure of nodes that are used. Such user effects could be particularly large for a specific analysis whose results cannot be compared with plant data or experimental data. The procedures, code documentation and user guidelines should be carefully followed to limit such user effects. Procedures include issues such as the way to compile the input

data set and the means of selecting the appropriate models in the code and general rules for preparing the nodalization.

5.38. The nodalization should be sufficiently detailed so that all the important phenomena of the scenario and all the important design characteristics of the nuclear power plant analysed are represented. A qualified nodalization that has successfully achieved agreement with experimental results for a given scenario should be used as far as possible for the same scenario when performing an analysis for a nuclear power plant. When scaled tests are used to assess a computer code, a consistent nodalization philosophy should be used for the test and for the full scale analysis of the plant. Sufficient sensitivity analyses should be performed on the nodalization to ensure that the calculated results are free from erratic variations.

QUALIFICATION OF INPUT DATA

5.39. The input data for a computer code include some form of model that represents all or part of the nuclear power plant. There is usually a degree of flexibility in how the plant is modelled or nodalized. The input data that are used to perform deterministic calculations should conform to the best practice guidelines for using the computer code (as in the user manual) and should be independently checked. The input data should be a compilation of information found in valid technical drawings, operating manuals, procedures, set point lists, pump performance charts, process diagrams and instrumentation diagrams, control diagrams, etc.

DOCUMENTATION OF COMPUTER CODES

5.40. Each computer code needs to be adequately documented to facilitate review of the models and correlations employed and to ensure that the models for important phenomena are appropriate and are not applied outside their range of validity. The documentation would also provide a description of the uncertainties of important models and the overall code for typical applications. The code documentation would also include user guidelines and input descriptions to ensure that the user can use the code properly. Description of the experiment or the key data used, description of the computer options used in the validation and description of the validation results should be included. The documentation should be available to all users.

5.41. Although the guidance may vary depending on the complexity of the codes and the modelling parameters available to the user, the user guidelines or validation documentation should give the user some guidance on the influence of important modelling parameters, recommendations for typical applications of the code, the type of nodalization to be used and the important trends to be expected. Typically, a complete set of documentation would include an abstract of the programme, a theory manual, a user’s manual and description of the inputs, a programmer’s manual and a validation report.

5.42. The tracking of errors and reporting of their correction status should be a continuous process and should be a part of code maintenance. The impacts of such errors on the results of analyses that have been completed and used as part of the safety assessment for a plant should be assessed.

6. GENERAL APPROACHES FOR ENSURING SAFETY MARGINS IN DETERMINISTIC SAFETY ANALYSIS

GENERAL CONSIDERATIONS

6.1. The deterministic safety analysis should demonstrate that the associated safety requirements are met and that adequate margins (depending on the plant state) exist between the real values of important parameters that could actually be reached and the threshold values at which the barriers against release of radioactivity would fail. Conservatisms might be introduced in many ways, such as in acceptance criteria or through conservative assumptions in physical models, and in initial and boundary conditions.

6.2. Uncertainties in computational predictions should be taken into account either implicitly by applicable approaches (see Table 1), or explicitly using best estimate approach with quantification of uncertainties. This is in particular important for the most limiting conditions (with the smallest margins to acceptance criteria).

6.3. To demonstrate compliance with anticipated operational occurrences acceptance criteria, two complementary approaches should be considered, the realistic approach, using plant control and limitation systems (paras 7.17 to 7.26) and a more conservative approach, using only safety systems (paras 7.27 to 7.44).

6.4. In accordance with SSR-2/1 (Rev.1), para. 5.26 [1], the deterministic safety analysis of design basis accidents should be performed using conservative analysis (see para. 2.14), including consideration of certain failures in safety systems and using other conservative assumptions, models and input parameters in the analysis.

6.5. In accordance with SSR-2/1 (Rev.1), para. 5.27 [1], the deterministic safety analysis of design extension conditions, and in particular analysis demonstrating the effectiveness of safety provisions to ensure the functionality of the containment, could be performed with a best estimate approach (although more stringent approaches may be used according to specific regulatory requirements).

6.6. When best estimate analysis is used, adequate margins to integrity of barriers should still be ensured. It should be demonstrated by sensitivity analysis that cliff edge effects[14] potentially leading

[14] Definition of a ‘cliff edge effect’ is provided in the Safety Glossary [3]. The term ‘plant parameter‘ in the definition should be interpreted in a broad sense, i.e. as any plant physical variable, design aspect, equipment condition, magnitude of a hazard, etc. that can influence equipment or plant performance.

to an early radioactive release or a large radioactive release can be reliably avoided. This demonstration is particularly important in the case of best estimate analysis used for design extension conditions and particularly for severe accidents, which have higher potential for degradation of the barriers leading to an early radioactive release or a large radioactive release.

6.7. Parameters to which the analysis results are most sensitive should be identified. A sensitivity analysis should be performed with systematic variation of the key input variables to determine their influence on the results. These analyses should be used for the determination of the most penalizing values of the parameters and for demonstration that a realistic change of the parameters does not lead to cliff edge effects. However, it should be taken into account that when sensitivity analyses are carried out with one-at-a-time parameter changes, misleading information may be obtained due to possible compensating or cumulating effects when several parameters change simultaneously.

6.8. For practical reasons, only a limited number of parameters identified as having the more significant effect on results can be involved in sensitivity analysis. Variation in parameters in a given range is also aimed to identify the values that lead to the smallest margins to a selected acceptance criterion and therefore such values are criterion dependent. Moreover, the importance of any parameter may change during the transient. Attention should be paid to the fact that, if the selected parameters are not independent, their arbitrary variation may cause problems due to inconsistency of data (e.g. violation of balance laws).

6.9. Deterministic safety analysis should incorporate a degree of conservatism which is commensurate with the safety analysis objectives and is dependent on the plant state. For conservative analysis of anticipated operational occurrences and design basis accidents (see para. 2.14), instead of the fully conservative approach, one of the two following options, or a combination of both, should be considered; either

- use of the best estimate computer code in combination with conservative input data for the analysis, or
- use of a best estimate computer code in combination with best estimate input data, however associated with quantification of uncertainties considering both uncertainties of the code models as well as uncertainties of input data for the analysis.

While in the first case the results are expressed in terms of a set of calculated conservative values of parameters limited by acceptance criteria, in the second case the results are expressed in terms of percentiles or probability distributions of the calculated parameters.

6.10. The procedures, code documentation and user guidelines should be followed carefully to limit the influence of the user in performing deterministic safety analysis

6.11. The selection of initial and boundary conditions should take account of geometric changes, fuel burnup and age-related changes to the nuclear power plant, such as boiler or steam generator fouling.

CONSERVATIVE AND COMBINED APPROACHES TO DETERMINISTIC SAFETY ANALYSIS FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENTS

6.12. In conservative or combined approaches, conservative selection of initial and boundary conditions used as input for the analysis should be made from the ranges of parameters specified in the plant limits and conditions (see Table 1). Examples of initial conditions are reactor power level, power distribution, pressure, temperature and flow in the primary circuit. Examples of boundary conditions are actuation set-point and performance characteristics of the plant systems such as pumps and power supplies, external sources and sinks for mass and energy, and other parameters changing during the course of the transient. Selection of conservative assumptions with regard to the availability of systems and operator actions is discussed separately for individual plant states in Section 7 of this Safety Guide.

6.13. Selection of input data and certain modelling assumptions applies not only to neutronic and thermal-hydraulic aspects of anticipated operational occurrences and design basis accidents, but equally also to radiological aspects. In particular, for analysis of the source term to the environment, the following factors should be addressed:

- Fission product and other radionuclide inventory in the fuel (in the core or in the spent fuel pool);
- Activity in reactor coolant system, including release of volatile fission products prior to or during the event (spiking);
- Time progression and scope of fuel damage (clad leakage);
- Fractions of radionuclides released from the fuel;
- Retention of radionuclides in the primary cooling system and in containment leakage pathways;
- Partitioning of fission products between steam and liquid phase of the coolant;
- Performance of containment systems (sprays, ventilation, filtering, deposition and resuspension);
- Containment leak rate and position of leaks from the containment;
- Timing and duration of releases;
- Chemical and physical forms of radioactive material released, in particular iodine;
- Effective elevation of release to the environment taking into account the energy of the releases.

6.14. In the case when best estimate code in combination with conservative inputs and assumptions is used, it should be ensured that the uncertainties associated with the best estimate code are sufficiently compensated by conservative inputs. To take into account uncertainties related to code models, the complete analysis should consider a combination of validation of the code, use of conservatisms and

use of sensitivity studies. These studies may be different depending on the type of transient; therefore this study should be carried out for each deterministic safety analysis.

6.15. For the purpose of conservative or combined approaches, the initial and boundary conditions should be set to values that will lead to conservative results for those safety parameters that are to be compared with the given acceptance criteria. A single set of conservative values for initial and boundary conditions does not necessarily lead to conservative results for each safety parameter or acceptance criterion. Therefore, the appropriate conservatism in initial and boundary conditions should be selected individually, depending on the specific transient and acceptance criteria. Combinations of initial conditions that cannot occur at the same time do not need to be considered.

6.16. In determination of conservative input parameters for the analysis the following should be taken into account:

- Intentional conservatisms may not always lead to conservative results, for example due to mutually contradictory effects of different assumptions leading to compensatory effects;
- The degree of conservatism can change during a course of the event, and an assumption may not be conservative throughout the whole transient;
- Due to implemented conservatisms misleading sequences of events and unrealistic time-scales may be predicted;
- If conservative values are selected based on engineering judgment, there is a high risk that such selection implemented by the user is not appropriate and that does not lead to conservative results.

Sensitivity calculations should therefore be performed to support conservative selection of inputs for each criterion. It is also advisable at least for selected scenarios with results of high importance to perform confirmatory best estimate analysis with quantification of uncertainties.

6.17. Since the use of conservative computer codes can mask certain phenomena or significantly change their chronological order, the analysis of such phenomena should be supported by adequate sensitivity analysis to demonstrate that important safety issues are not being concealed by the conservative code.

6.18. In conservative safety analysis, the most limiting initial conditions that are expected over the lifetime of the plant should be used, based on sensitivity analyses. The initiating event should be considered to occur at an unfavourable time as regards initial reactor conditions including plant mode (power or shutdown), power level, residual heat level, fission product inventory, reactivity conditions, reactor coolant system temperature, pressure and inventory.

6.19. Initial conditions that cannot occur at the same time in combination do not need to be considered. For example, the limiting decay heat and the limiting peaking factors cannot physically

occur at the same time of the fuel campaign. However the initial conditions considered should cover the most unfavourable possible combination.

6.20. Operating conditions taking place during very limited time period and with negligible frequency of occurrence may not need to be considered in selection of conservative initial conditions.

BEST ESTIMATE DETERMINISTIC SAFETY ANALYSIS WITH QUANTIFICATION OF UNCERTAINTIES FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENTS

6.21. Uncertainties in deterministic safety analysis, in particular for anticipated operational occurrences and design basis accidents, may be addressed by the use of a best estimate computer code taking into account uncertainties in models, initial and boundary conditions and other input parameters. To obtain conservative results of safety analysis, the effects of uncertainties on the results should be identified and assessed to confirm that the actual plant parameters will be bounded by the upper and lower limits of the results of calculation with an adequate confidence.

6.22. Prior to the quantification of uncertainties, it should be ensured that: (a) the best estimate computer code used for the analysis is adequately validated; (b) the user effects are properly accounted for; (c) the influence of the computational platform is minimized; and (d) the methodology to assess the uncertainties is qualified.

6.23. A reliable assessment of the uncertainties is needed to carry out acceptable best estimate analyses with quantification of uncertainties, especially for the identification and separation of aleatory and epistemic sources of uncertainties. These two different sources should be treated differently when performing the uncertainty analysis. Code-to-data comparisons are the preferred means to quantify the epistemic uncertainties. However, a combination of sensitivity studies, code to code comparisons and expert judgements may also be used as an input for the assessment (GSR Part 4 (Rev. 1), Requirement 17) [2]. For aleatory uncertainties, the preferred means is the collection of nuclear power plant data of initial and boundary conditions that are relevant to the events being considered.

6.24. Quantification of uncertainties should be based on statistically combined uncertainties in plant conditions and code models (see para. 2.7) to ensure with a specified probability, that a sufficiently large number of calculated results meet the acceptance criteria. For analysis of anticipated operational occurrences and design basis accidents it is typically required that assurance be provided at a 95% or greater probability that at least 95% of the results comply with applicable acceptance criteria for a plant. However, national regulations may require a different level of probability.

6.25. Within the uncertainty methods considered, uncertainties should be evaluated using either (a) propagation of input uncertainties or (b) extrapolation of output uncertainties. For the ‘propagation of input uncertainties’, uncertainty is obtained by performing a sufficient number of calculations varying

these input uncertain parameters. For the ‘extrapolation of output uncertainty’ approach, uncertainty is obtained from the output uncertainty based on comparison between calculation results and experimental data.

6.26. For the ‘propagation of input uncertainties’, the uncertain input parameters should include at least the most significant ones. The selected input parameters should be ranged and their probability distribution specified using relevant experiments, measurements of parameters, records of plant operational parameters, etc. If this is not feasible, conservative values from the given range should be used. Selected input parameters have to be independent or dependencies between uncertain input parameters should be identified and quantified and a specific processing should be applied.

6.27. It should be taken into account that the selection of uncertain input parameters, their ranges and probability distributions is crucial for the reliability of results, since it strongly affects the width of the uncertainty bands of the results that is essential for engineering applications.

6.28. Uncertainty methods with ‘propagation of input uncertainties’ by using regression or correlation techniques from the sets of input parameters and from the corresponding output values allow also ranking of the uncertain input parameters in relation to their contribution to output uncertainty; the ranking of parameters is therefore a result of the analysis. Such ranking indicates which of the parameters should be given the highest attention. However, attention should be given to the fact that the regression or correlation techniques might also have drawbacks, especially when the response is not linear or when the cross-correlation effects are important.

6.29. The uncertainty in parameters associated with the results of a computer code may be also determined with the assistance of phenomena identification and ranking table (PIRT) based on expert judgment for each event that is analysed. This PIRT should identify the most important phenomena for which the suitability of the code has to be assured and should be based to the extent possible on available data. The important parameters should be varied randomly in accordance with their respective probability distributions to determine the overall uncertainty. The same process can be applied to evaluate the applicability of a computer code or a computational tool to simulate a selected event.

7. DETERMINISTIC SAFETY ANALYSIS FOR DIFFERENT PLANT STATES

GENERAL CONSIDERATIONS

7.1. Deterministic safety analysis should address postulated initiating events and accident sequences corresponding to different plant states and should follow general rules for selection of acceptance criteria, use of computer codes and suggested approaches for treatment of uncertainties and ensuring safety margins, as described in the three previous sections of this Safety Guide.

7.2. In addition, deterministic safety analysis should follow more specific guidance regarding objectives of the analysis, selection of acceptance criteria, consideration of availability of various plant systems, operator actions, treatment of uncertainties and any other assumptions of the analysis for individual plant states specified further on in this section. Deterministic safety analysis should only credit structures, systems and components that meet the requirements associated with relevant plant states, with due consideration of safety classification (see SSG-30) [20].

7.3. Decisions on the level of conservatism in performing deterministic safety analysis should include the following sets of input data or assumptions on:

1) Code models;

2) Plant operating parameters;

3) Control and limitation systems;

4) Active safety systems;

5) Passive safety systems;

6) Safety features for design extension conditions;

7) Operator actions.

7.4. Separate analyses of the source term should be carried out for each type of failures for which the phenomena that would affect the source term would be different. Typical kinds of accidents include loss of coolant accident with release of reactor coolant and fission products from the core to the containment, accidents by-passing the containment or accidents taking place outside the containment, such as accidents in the spent fuel pool, accidents during manipulations with the irradiated fuel, or releases from the systems for treatment and storage of gaseous and liquid radioactive waste.

7.5. For many types of postulated accidents, the important release of radionuclides would be from the reactor core into the reactor coolant system and afterwards into the containment. Evaluation of the source term should thus involve determining the behaviour of the radioactive material along this route up to their release to the environment.

DETERMINISTIC SAFETY ANALYSIS FOR NORMAL OPERATION

Specific objectives of the analysis

7.6. Deterministic analyses of normal operation should use an iterative process to support development of operational limits and conditions and confirm their adequacy. These reflect the limiting conditions of operation in terms of values of process variables, system requirements, surveillance and testing requirements.

7.7. The limits and conditions used in normal operation, such as reactor power and coolant inventory, should cover all important initial and boundary conditions that will be subsequently used in the analysis of anticipated operational occurrences, design basis accidents and design extension conditions.

7.8. All modes of normal operation and relevant plant configuration covered by operational limits and conditions should be analysed, with particular attention paid to transient operational regimes such as changes in reactor power, reactor shutdown from power operation, reactor start up, reactor cooling down, mid-loop operation, handling of fresh and irradiated fuel and off-loading of irradiated fuel from the reactor to the spent fuel pool and loading of fuel into the core.

7.9. The safety analysis for normal operation should also include an analysis of the radiological situation in the plant and an estimate of the plant's releases of radioactive material to the environment. These are necessary inputs for determining radiation doses to the plant staff, to the public and to non-human biota around the nuclear power plant. Due to the complexity of the issue and in particular its strong dependence on the overall organization of the plant operation, the corresponding guidance is not provided in this Safety Guide.

Acceptance criteria

7.10. The analysis should assess whether normal operation of the plant can be carried out in such a way that plant parameter values do not exceed operational limits and conditions. The assessment of design in normal operation should verify that a reactor trip or initiation of the limiting and safety systems would be avoided in all the transients, as defined by the operational limits and conditions, and considering all the operating modes. Transitions from one operational state to another, as anticipated according to operational guidelines, should be also taken into account.

7.11. The safety analysis for normal operation should include an analysis of the overall design and operation of the plant to: (a) predict the radiation doses likely to be received by workers and members of the public; (b) assess that these doses are below acceptable limits (see Requirement 5 from SSR-2/1 (Rev. 1) [1]; (c) and ensure that the principle stating that these doses should be 'as low as reasonably achievable' has been satisfied. However, compliance with the radiological acceptance criteria (see [4] and [5]) is not covered by this Safety Guide.

Availability of systems

7.12. Systems credited in deterministic analysis of normal operation should be limited to normal operation systems, including plant control systems. No other plant systems should be actuated during transient normal operational modes.

Operator actions

7.13. Planned operator actions performed in accordance with normal operating procedures should be considered in the analysis.

Analysis assumptions and treatment of uncertainties

7.14. Analysis of normal operation should provide a realistic representation of the plant behaviour. However, uncertainties regarding systems performance, including instrumentation and control and mechanical systems, should be considered to assess adequacy of the available provisions.

7.15. The initial conditions considered should be representative of all expected plant authorized modes, according to operational limits and conditions. Bounding values of parameters should be considered within the whole acceptable range of the parameters.

7.16. When there are uncertainties in making the dose predictions, conservative assumptions should be made; however, the detailed guidance is beyond the scope of this Safety Guide.

REALISTIC DETERMINISTIC SAFETY ANALYSIS FOR ANTICIPATED OPERATIONAL OCCURRENCES

Specific objectives of the analysis

7.17. The main objective of the realistic analysis of anticipated operational occurrences is to check that the plant operational systems (in particular control and limitation systems) can prevent a wide range of anticipated operational occurrences from evolving into accident conditions and that the plant can return to normal operation following an anticipated operational occurrence. The realistic analyses should aim at providing a realistic response of the plant to the initiating event.

7.18. For many postulated initiating events the control and limitation systems in combination with inherent plant characteristics and operator actions will compensate for the effects of the event without a reactor trip or other demands being placed on the safety systems. Operation can resume after rectification of the fault. The anticipated operational occurrences category should include all the postulated initiating events which might be expected to occur during the lifetime of the plant.

7.19. Typically, anticipated operational occurrences should not lead to any unnecessary challenge to safety equipment primarily designed for protection in the event of design basis accidents. It is therefore advisable to demonstrate by the analysis that, in case of the operation of plant control and limitation systems as intended, these systems will be capable of preventing the initiation of the safety systems. However, it is recognized that some anticipated operational occurrences require the actuation of safety systems.

Acceptance criteria

7.20. The realistic analyses of anticipated operational occurrences should aim at proving that no induced damage is caused to any of the physical barriers (fuel matrix, fuel cladding, reactor coolant pressure boundary or containment) or the systems important to safety. In addition, they should aim at checking as far as possible, that reactor trip and safety systems are not actuated.

7.21. The realistic analyses of anticipated operational occurrences may also aim at proving that specific design criteria, more stringent than conservative anticipated operational occurrences acceptance criteria, are fulfilled when control and limitation systems are available (e.g. no actuation of safety valves).

7.22. Failures of physical barriers are typically prevented by the requirement (for light water reactors) that there should be no boiling crisis or dry out with 95 % probability at 95 % confidence level anywhere in the core, there should be no fuel melting anywhere in the core and pressure in the reactor coolant system and main steam system should not significantly (more than 10–15 %) exceed the design value.

7.23. There should be negligible radiological impact beyond the immediate vicinity of the plant. The radiological acceptance criteria for doses and correspondingly for releases for each anticipated operational occurrence should be comparable with annual limits for normal operation and more restrictive than for design basis accidents. Acceptable effective dose limits are similar to those for normal operation.

Availability of systems

7.24. For realistic anticipated operational occurrences analysis any system not affected by the postulated initiating event should be considered available. The analysis should mostly rely on control and limitation systems in addition to inherent plant characteristics.

Operator actions

7.25. Planned operator actions performed in accordance with normal and abnormal operating procedures should be considered in the analysis. Typically, when correct operation of the control and limitation systems is assumed, there is no need for any operator action during the associated transient; otherwise realistic estimates for operator action times should be used.

Analysis assumptions and treatment of uncertainties

7.26. Realistic analysis of anticipated operational occurrences should be performed with best estimate methodology covering anticipated plant initial conditions considered in determination of the postulated initiating events. Normally, uncertainties are not considered in realistic analysis of

anticipated operational occurrences. For operational considerations (such as plant reliability), treatment of uncertainties may be applied to the control and limitation systems.

CONSERVATIVE DETERMINISTIC SAFETY ANALYSIS FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENTS

Specific objectives of the analysis

7.27. Realistic analysis for design basis accidents is not permitted; one of the conservative methods[15] (Options 1, 2 or 3 from Table 1) should be used. The conservative analysis of anticipated operational occurrences and design basis accidents (see SSR-2/1 (Rev.1), para. 5.26) [1], should demonstrate that the safety systems alone in the short term, and with operator actions in the long term, are capable of achieving a safe state by fulfilling the following safety requirements:

— Shut down the reactor and achieve subcritical condition during and after anticipated operational occurrences or design basis accident conditions;

— Remove residual heat from the core after reactor shutdown from all anticipated operational occurrences or design basis accident conditions;

— Reduce the potential for the release of radioactive material and ensure that any releases are below acceptable limits during anticipated operational occurrences or design basis accident conditions;

7.28. The safety analysis should demonstrate that the acceptance criteria relevant to the event are met. In particular, it should be demonstrated that some or all of the barriers to the release of radioactive material from the plant will maintain their integrity to the extent required.

7.29. The safety analysis should establish the performance characteristics and set points of the safety systems, and operating procedures to ensure that the fundamental safety functions are always maintained. The analysis provides the basis for the design of the reactivity control systems, the reactor coolant system and the engineered safety features (for example, the emergency core cooling systems and the containment heat removal systems).

Acceptance criteria

7.30. For conservative analysis of anticipated operational occurrences the technical acceptance criteria related to fuel integrity and radiological acceptance criteria should, in principle, be the same as presented above for realistic analysis of anticipated operational occurrences.

[15] The terms ‘conservative methods’ and ‘conservative analysis’ are to be understood according to options 1, 2 and 3 from Table 1 and para. 2.14.

7.31. There should be no, or only minor, radiological impact beyond immediate vicinity of the plant, without the need for any off-site protective actions. The definition of minor radiological impact should be set by the regulatory body, but acceptable effective dose limits are typically in the order of few mSv per event.

7.32. Specific technical acceptance criteria should be defined in order to prove that the three fundamental safety functions can be ensured in any condition and that, in anticipated operational occurrences or design basis accidents, some or all of the barriers are able to limit the releases of radioactive material to the environment.

7.33. The detailed acceptance criteria should typically include the following:

— An event should not generate a subsequent more serious plant condition without the occurrence of a further independent failure (in addition to any single failure assumed to meet the single failure criterion). Thus, an anticipated operational occurrence by itself should not generate a design basis accident, and a design basis accident should not generate a design extension condition;

— There should be no consequential loss of the overall function of the safety systems needed to mitigate the consequences of an accident, although a safety system may be partially affected by the postulated initiating event;

— Systems used for accident mitigation should be designed to withstand the maximum loads, stresses and environmental conditions for the accidents analysed. This should be assessed by separate analyses covering environmental conditions and ageing (i.e. temperature, humidity radiation or chemical environment) and thermal and mechanical loads on plant structures and components. The margins considered in the design should be commensurate with the probability of the loads to be considered;

— The pressure in the reactor and main steam systems should not exceed the relevant design limits for the existing plant conditions, according to the overpressure protection rules. Additional overpressure analysis may be needed to study the influence of the plant conditions on safety and relief valves;

— The number of fuel cladding failures which could occur should be limited for each type of postulated initiating event to allow the global radiological criteria to be met and also to limit the level of radiation used for equipment qualification;

— In design basis accidents with fuel uncovering and heating up, a coolable geometry and the structural integrity of the fuel assemblies (light water reactors) should be maintained;

— No event should cause the temperature, pressure or pressure differences between containment compartments to exceed values which have been used as the containment design basis;

— Subcriticality of nuclear fuel in reactor after shutdown, in fresh fuel storage and in the spent fuel pool should be maintained. Temporary recriticality (e.g. steam line break in pressurized

water reactor) may be acceptable for certain events and plant operating modes, however without exceeding criteria associated with sufficient cooling of the fuel;

— There should be no initiation of a brittle fracture or ductile failure from a postulated defect of the reactor pressure vessel (RPV) during the plant design life for the whole set of postulated design basis accidents;

— Internal reactor components should withstand dynamic loads during design basis accidents so that safe shutdown of the reactor, reactor sub-criticality and sufficient reactor core cooling are maintained.

7.34. For postulated initiating events occurring with missing or degraded integrity of any of the barriers (such as situations with open reactor, open containment or event initiated in the spent fuel pool) more restrictive acceptance criteria (e.g. avoiding coolant boiling or fuel uncovering) should be used.

Availability of systems

7.35. The conservative considerations regarding the availability of plant systems should typically include the following:

- Normal operation systems that are in operation at the beginning of the postulated initiating event and that are not affected by the initiating event itself and by its consequences can be assumed to continue to operate;
- Any control or limitation systems should be assumed to start operating only if their functioning would aggravate the effects of the initiating event. No credit should be taken for the operation of the control systems in mitigating the effects of the initiating event;
- Safety systems designed and maintained as safety grade (in accordance with the rules for quality assurance, periodic testing, use of accepted design codes and equipment qualification) should be assumed to operate with conservative performance;
- In accordance with the single failure criterion, a single component failure should be assumed to occur in the operation of the safety groups required for the initiating event, in addition to the initiating failure and any consequential failures. Depending on the selected acceptance criterion the single failure should be put to a system/component leading to the largest challenge for the safety systems;
- Safety features specifically designed for design extension conditions should not be credited in the analysis.

7.36. If maintenance is allowed, the unavailability of the concerned train of the safety system should be taken into account.

Operator actions

7.37. For conservative safety analysis, credit should not be taken for operator diagnosis of the event and for initiating the necessary actions. The corresponding timing claimed should be justified and validated for specific reactor design; for example earlier than in 30 minutes if performed in the control room, or 60 minutes for the field actions.

7.38. The actions of the plant staff to prevent or mitigate the accident by taking correct actions should only be considered in the analysis if it can be shown that sequence and plant specific boundary conditions allow for carrying out the requested actions. The conditions to be considered include the overall context in the event sequence, working environment in the control places, ample information, written procedures and training.

7.39. In accordance with the practice in some States an additional operator error during execution of recovery actions may be considered as a single failure.

Analysis assumptions and treatment of uncertainties

7.40. The conservative assumptions used for the analysis of anticipated operational occurrences and design basis accidents should take account of uncertainties in the initial conditions and boundary conditions, availability of the plant systems and in the operator actions. The general rules specified in Section 6 should be applied in full for these categories of plant states. The aim is to ensure with high confidence that there are significant margins to the safety limits.

7.41. Conservative analysis of anticipated operational occurrences should also include the same conservative assumptions as used for the deterministic design basis accident analysis, especially those assumptions which relate to the systems for maintaining safety functions during these postulated initiating events.

7.42. If a conservative or combined methodology is applied, the safety systems should be assumed to operate at their minimum or maximum performance levels, whatever is conservative for a given acceptance criterion. For reactor trip and safety system actuation systems, this should assume that the action occurs at the worst edge of the possible range. If a best estimate plus uncertainty methodology is applied, uncertainties on safety systems performances are included in the overall uncertainty analysis.

7.43. In addition to the postulated initiating event itself, a loss of off-site power (LOOP) may be considered as additional conservative assumption. If LOOP is considered as an additional failure it may be assumed to occur at a time which has the most negative effect regarding the barrier integrity. Some acceptance criteria should be adapted taking into account the probability of this combination.

7.44. In line with the general rules for deterministic safety analysis, the source term evaluation of anticipated operational occurrences and design basis accidents would consist in taking into account all

significant physical processes occurring during an accident and using conservatively determined numerical values of initial data and coefficients on a plant specific basis.

DETERMINISTIC SAFETY ANALYSIS FOR DESIGN EXTENSION CONDITIONS WITHOUT SIGNIFICANT FUEL DEGRADATION

Specific objectives of the analysis

7.45. The objective of the safety analysis of design extension conditions without significant fuel degradation is to demonstrate that core melt can be prevented with an adequate level of confidence and that there is adequate margin to avoid cliff edge effects.

Acceptance criteria

7.46. Acceptance criteria for design extension conditions should meet the Requirement 30 of SSR-2/1 (Rev. 1), para. 5.31A [1]. 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 practicable.

Availability of systems

7.47. In general, only systems shown to be operable for this category of design extension conditions should be credited in the analysis.

7.48. Safety systems that are not affected by the failures assumed in the design extension conditions without significant fuel degradation sequence may be credited in the analysis. Special attention should be paid to other factors affecting safety systems (e.g. sump screen blockage) and support systems (electrical, ventilation, cooling) when assessing the independence of safety systems regarding the postulated failures (e.g. internal flooding).

7.49. For design extension conditions without significant fuel degradation, the single failure criterion does not need to be applied. Furthermore, unavailability of safety features for this category of design extension conditions due to maintenance does not need to be considered.

7.50. According to the independence principle between the levels of defence in depth the normal operation systems including control and limitation systems should not be credited in analysis of design extension conditions without significant fuel degradation because:

- one given sequence potentially aims at covering several kinds of postulated initiating event and it may be difficult to prove that the operational system is always available considering both the origin of the postulated initiating event and the multiple failures;
- the sequences often create degraded ambient conditions and the systems credited in the analysis should be adequately qualified for such conditions.

However, if normal operation systems have a negative impact on the course of the accident, they should be considered.

7.51. Non-permanent equipment should not be considered for demonstration of adequacy of the nuclear power plant design. Such equipment is typically considered to operate for long-term sequence and is considered available in accordance with the emergency operating procedures or accident management guidelines. The time claimed for availability of non-permanent equipment should be justified[16].

Operator actions

7.52. Best estimate assumptions might be used regarding operator actions for the analysis of design extension conditions. However, some conservative assumptions as described for design basis accidents may be used to the extent practicable.

Analysis assumptions and treatment of uncertainties

7.53. The requirements on the selection, validation and use of computer codes specified for design basis accidents should also apply in principle for analysis of design extension conditions without significant fuel degradation.

7.54. For design extension conditions without significant fuel degradation, in principle the same combined approach or even best estimate approach with quantification of uncertainties (best estimate plus uncertainty), as applicable for design basis accidents can be used. However, in line with the general rules for analysis of design extension conditions, best estimate analysis without requiring a quantification of uncertainties can be used, but see paras 7.55 and 7.67.

7.55. When best estimate analysis is performed, margins to avoid the 'cliff edge effect' should be shown, for example by sensitivity analysis demonstrating to the extent practicable that, when more conservative assumptions are considered for dominant parameters, there are still margins to the loss of integrity of physical barriers.

DETERMINISTIC SAFETY ANALYSIS FOR DESIGN EXTENSION CONDITIONS WITH CORE MELTING

Specific objectives of the analysis

7.56. The analysis of severe accidents should identify the bounding plant parameters resulting from the postulated core melting sequences, and demonstrate that:

[16] Current practice in some States is that credit is given in the safety analysis to the availability of non-permanent equipment after, for example, 8 hours for equipment stored on-site or 72 hours for equipment stored off the site.

- The plant can be brought into a state where the containment functions can be maintained in the long term;
- The plant structures, systems, and components (e.g. the containment design) and procedures are capable of preventing a large radioactive release or an early radioactive release, including containment by-pass;
- Control locations remain habitable to allow performance of required staff actions;
- Planned severe accident management measures are effective.

7.57. The safety analysis of severe accidents should demonstrate that compliance with the acceptance criteria is achieved by features implemented in the design combined with implementation of procedures or guidelines for accident management.

Acceptance criteria

7.58. Radiological acceptance criteria in terms of doses for the public (or releases to the environment) used for analysis of severe accidents should ensure that only off-site protective actions that are limited in terms of area and time are necessary and there is sufficient time for their implementation.

7.59. Technical acceptance criteria should ensure that containment integrity is maintained. Examples of acceptance criteria for design extension conditions analysis would include limitation of the containment pressure, containment water level, temperature and flammable gases concentration and stabilization of molten corium.

7.60. On site radiological acceptance criteria should ensure habitability of the control locations (i.e. control room, supplementary control room and other emergency response facilities and locations) and in the areas used to move between control locations. In particular, the radiation level (e.g. ambient equivalent dose rates and activity concentrations in the air) in the control locations of the site should allow for adequate protection of their occupants, such as emergency workers, according to requirements 11 and 24 from GSR Part 7 [8].

Availability of systems

7.61. Safety systems should not be credited in the analysis of severe accidents unless it is shown with reasonable confidence that:

- their failure is not part of any scenario that the severe accident sequence is meant to cover;
- this equipment will survive realistic severe accident conditions for the period that is needed to perform its intended function.

7.62. Consideration of availability of equipment credited to operate under severe accident conditions should include:

- Circumstances of the applicable initiating event, including those resulting from external hazards (e.g. station blackout, earthquakes); and
- Environment (e.g. pressure, temperature, radiation) and time period for which the equipment is needed

7.63. For design extension conditions with core melting, single failure criterion does not need to be applied. Furthermore, unavailability of a system or component due to maintenance does not need to be considered.

7.64. Non-permanent equipment should not be considered for demonstration of adequacy of the nuclear power plant design. Such equipment is typically considered to operate for long-term sequence and is considered available in accordance with the emergency operating procedures or accident management guidelines. The time claimed for availability of non-permanent equipment should be justified[17].

Operator actions

7.65. The same assumptions regarding operator actions should be considered as for design extension conditions without significant fuel degradation (see para. 7.52).

Analysis assumptions and treatment of uncertainties

7.66. The severe accident analysis should model (in addition to neutronic and thermal-hydraulic phenomena occurring in conditions without core melting) the wide range of physical processes that could occur following core damage and that could lead to a release of radioactive material to the environment. These should include, where appropriate:

- Core degradation processes and fuel melting;
- Fuel–coolant interactions (including steam explosions);
- In-vessel melt retention;
- Vessel melt-through;
- Direct containment heating;
- Distribution of heat inside the primary circuit;
- Generation, control, and combustion of hydrogen;
- Failure or bypass of the containment;
- Corium–concrete interaction;

[17] Current practice in some States is that credit is given in the safety analysis to the availability of non-permanent equipment after, for example, 8 hours for equipment stored on-site or 72 hours for equipment stored off the site.

- Release and transport of fission products, including venting to prevent overpressure in the containment;
- Ability to cool in-vessel and ex-vessel core melt.

7.67. Analysis of severe accidents should be performed using a realistic approach in Table 1 to the extent practicable. Since explicit quantification of uncertainties may be impractical due to complexity of the phenomena and insufficient experimental data, sensitivity analyses should be performed to demonstrate the robustness of the results and the conclusions of the severe accident analyses.

DETERMINISTIC SAFETY ANALYSIS IN SUPPORT OF 'PRACTICAL ELIMINATION' OF THE POSSIBILITY OF CERTAIN CONDITIONS ARISING

7.68. Requirements to be met include Requirement 20 from SSR-2/1 (Rev. 1), para. 5.31 [1]. It is a decision of the regulatory body to establish more specific rules describing acceptable ways for the demonstration of 'practical elimination'.

7.69. According to para. 2.1, the demonstration of 'practical elimination' of the possibility of certain conditions arising that could lead to a large radioactive release or an early radioactive release include deterministic considerations together with engineering aspects such as design, fabrication, testing, inspection and evaluation of the operating experience and supplemented by probabilistic considerations, taking into account the uncertainties due to the limited knowledge of some physical phenomena.

7.70. Demonstration of 'practical elimination' of the possibility of certain conditions arising should include, where appropriate, the following steps:

- Identification of undesired conditions (challenges) potentially endangering the containment integrity or by-passing the containment, resulting in an early radioactive release or a large radioactive release;
- Challenges should be addressed by implementing design and operational provisions in order to 'practically eliminate' the possibility of those conditions arising;
- Sensitivity studies to provide assurance that sufficient margins exist to address uncertainties regarding the demonstration with high level confidence that the possibility of the referred conditions has been 'practically eliminated';
- Final confirmation of the adequacy of the provisions by deterministic safety analysis, complemented by probabilistic safety assessment and engineering judgment.

7.71. Although probabilistic targets can be set, demonstration of the 'practical elimination' of certain event sequences arising that could lead to an early radioactive release or a large radioactive release should not be based solely on low probability numbers. Such event sequences should rather be

deterministically defined and their ‘practical elimination’ based on the performance of safety features making the events sequences extremely unlikely to arise.

7.72. Where a claim is made that the conditions potentially resulting in an early radioactive release or a large radioactive release are ‘physically impossible’, it is necessary to examine the inherent safety characteristics of the system to demonstrate that the conditions cannot, by the laws of nature, occur and that the fundamental safety functions (see Requirement 4 of SSR-2/1 (Rev. 1)) [1] of reactivity control, heat removal and limitation of accidental radioactive releases will be achieved. In practice this concept is limited to very specific cases. An example of its use could be for uncontrolled reactivity accidents, where the main protection is provided by negative reactivity coefficient with all possible combinations of the reactor power and coolant pressure and temperature, thus suppressing reactor power increase during any disturbances and eliminating the reactivity hazards with help of laws of nature (consideration of ‘practical elimination’ in terms of the physical impossibility for the conditions to arise).

8. DOCUMENTATION, REVIEW AND UPDATE OF DETERMINISTIC SAFETY ANALYSIS

DOCUMENTATION

8.1. GSR Part 4 (Rev. 1) [2] states that the results and findings of the safety assessment shall be documented, as appropriate, in the form of a safety report that reflects the complexity of the facility or activity and the radiation risks associated with it. In accordance with GSR Part 4 (Rev. 1), para. 4.64 [2], “The safety report shall document the safety assessment in sufficient scope and detail to support the conclusions reached and to provide an adequate input into independent verification and regulatory review.”

8.2. It is understood that in addition to the sufficiently comprehensive form of the safety report there are other documents which may include description and results of the deterministic safety analysis, which are used as supporting information to independent verification or regulatory review. The same rules as stated for the safety report should be used for all deterministic safety analysis intended for other submissions to the regulatory body.

8.3. The safety report should provide a list of all plant states considered in the deterministic safety analysis, appropriately grouped according to their frequencies and specific challenges to the integrity of physical barriers against releases of radioactive material. Selection of bounding scenarios in each group should be justified. ‘Practical elimination’ of the possibility of certain conditions potentially leading to an early radioactive release or a large radioactive release should be demonstrated.

8.4. A set of the most important plant data (‘data base for deterministic safety analysis’) used for development of plant models necessary for making an independent verification or for evaluating the

deterministic safety analysis performed, should be provided, conveniently compiled in a separate part of the safety report or in a separate document. Such data should include information on geometry, thermal and hydraulic parameters, material properties, characteristics of the control system and set points, and the range of uncertainties in plant instrumentation devices, including drawings and other graphical documents. If these data are not sufficiently documented in different parts of the safety report, other reliable data sources used for the preparation of the plant models should be clearly identified and referenced.

8.5. Brief description of the computer codes used in the deterministic safety analysis should be provided. In addition to the reference to the specific code documentation the description should contain convincing justification that the code is adequate for the given purpose and has been verified and validated by the user (see paras 5.14 to 5.38).

8.6. Depending on the phenomena taking place and other characteristics of each analysed scenario, a relevant acceptance criterion or a set of criteria should be selected and presented together with the safety analysis, with clear specification of conditions for applicability of the criteria (see Section 4).

8.7. The simulation models and the main assumptions used in the analysis for demonstrating compliance with each specific acceptance criterion should be described in detail, including the scope of validation of the model. This description should include potentially different approaches used for each plant state.

8.8. If deterministic analysis involves several different computer codes in sequence, the transfer of data between various stages of accident analysis and/or computer codes used in sequence should be clearly described in order to provide for traceability of calculations as a necessary condition for independent verification, understanding and acceptance of the results.

8.9. The time span of any scenario analysed and presented should extend up to the moment when the plant reaches a safe and stable end state (typically not all sensitivity calculations need to be presented over the full time scale). What is meant by a safe and stable end state should be defined. Typically it is assumed that a safe and stable end state is achieved when the core is covered and long term heat removal from both the core and the containment is achieved, and the core is and will remain subcritical by a given margin.

8.10. The results of deterministic safety analysis should be structured and presented in an appropriate format in such a way as to provide a good understanding and interpretation of the course of the accident. A standardized format is suggested for similar analyses to facilitate interpretation and inter comparison of the results.

8.11. The deterministic safety analysis results should typically contain the following information:

(a) A chronology (timing) of the main events as calculated;

(b) A description and evaluation of the accident on the basis of the parameters selected;

(c) Figures showing plots of the main parameters calculated;

(d) Conclusions on the acceptability of the level of safety achieved and a statement on compliance with all relevant acceptance criteria, including adequate margins;

(e) Results of sensitivity analysis, as appropriate.

8.12. Documentation of deterministic safety analysis should be subject to relevant quality assurance procedures and quality control [12-14].

8.13. More detailed information about documentation of deterministic safety analysis to be included in different stages of safety analysis reports can be found in GS-G-4.1 (Rev. 1) [21] (Format and Content of Safety Analysis Report for Nuclear Power Plants; in preparation).

Sensitive information in documentation

8.14. Sensitive information included in the reports regarding deterministic safety analysis which affects nuclear security should be identified and appropriately protected. This may include but is not limited to information about identification and categorization of postulated initiating events and results from deterministic safety analysis conducted. This information should be protected as per information security guidelines (Confidentiality, Integrity and Availability); see NSS-23-G [6].

REVIEW AND UPDATE OF DETERMINISTIC SAFETY ANALYSIS

8.15. In accordance with GSR Part 4 (Rev 1), para. 5.10 [2], the safety analysis used in the licensing process should be periodically updated to account for changes in nuclear power plant configuration, characteristics of plant systems and components, operating parameters, plant procedures, research findings, and advances in knowledge and understanding of physical phenomena including changes in computer codes with potential significant effects on results of safety analysis.

8.16. In addition to periodic updates, the safety analysis should also be updated following the discovery of information that may reveal a hazard that is different in nature, greater in probability, or greater in magnitude than was previously documented.

8.17. In case of need, the safety analysis should be reassessed to ensure that it remains valid and meets the objectives set for the analysis. The results should be assessed against the current requirements relevant for deterministic safety analysis, applicable experimental data, expert judgment, and comparison with similar analyses.

8.18. The outcomes of the reassessment, including new deterministic safety analyses, if necessary, should be reflected in the updated safety analysis report with an appropriate level of comprehensiveness commensurate with the extent of changes and the associated impacts.

9. INDEPENDENT VERIFICATION OF DETERMINISTIC SAFETY ANALYSIS BY THE LICENSEE

9.1. Requirements to be met include Requirement 21 of GSR Part 4 (Rev 1) [2]. The objective and scope of the independent verification are further detailed in ~~the §~~paras 4.66 to ~~–~~ ~~§~~4.71 of that Requirement.

9.2. The main purpose of the independent verification of safety analysis by the licensee (the operating organization) is to reconfirm that the safety analysis developed by other entities such as designers, manufacturers and constructors has been carried out in an acceptable way and satisfies the applicable safety requirements. As a minimum, it should be verified by the licensee that the design will comply with the relevant regulatory requirements and acceptance criteria are complied with as an essential factor of the licensee's prime responsibility for safety.

9.3. According to SF-1, para. 3.6 [22], among other duties the operating organization is responsible for verifying appropriate design and the adequate quality of facilities and activities and of their associated equipment. Adequacy of the design should be demonstrated by means of safety assessment.

9.4. As described in GSR Part 4 (Rev. 1), para. 4.13 [2], safety analysis is an essential component of safety assessment. The relevant requirements of the GSR Part 4 (Rev. 1) should therefore fully apply to deterministic safety analysis as an essential part of the safety assessment.

9.5. Throughout the design process, the safety analysis and independent verification are carried out by different groups or organizations. They are integral parts of an iterative design process with the objective of ensuring that the plant meets the safety requirements. However, the independent verification should be also carried out by or on behalf of the operating organization and should only relate to the design as submitted to the regulatory body for approval.

9.6. In accordance with GSR Part 4 (Rev. 1), para. 4.67 [2], the operating organization should ensure that an independent verification is performed by suitably qualified and experienced individuals or groups who are different from those carrying out the original safety analysis, before it is submitted to the regulatory body. The operating organization is fully responsible for the independent verification even if parts of it are entrusted to separate organizations.

9.7. Personnel performing independent verification are considered independent if they have not participated in the original safety analysis. Special attention should be paid to independence of the verification team if it is established in the same design or other closely associated organization. Use of fully independent organization should be a preferred solution.

9.8. The group performing the independent verification may take into account any quality assurance (QA) reviews which have previously been conducted in determining the extent and scope of its verification.

9.9. Special attention should be paid to independent verification of the safety analysis for nuclear power plants of older designs constructed to less rigorous standards, and of evolutionary or innovative designs with use of novel design solutions.

9.10. The conduct of the independent verification may follow the methods of the original safety analysis. However, the scope of the independent verification could be narrower since it would focus on the most significant safety issues and requirements, rather than all of them. The scope and level of detail of the independent verification should be reviewed in the independent verification itself in accordance with GSR Part 4 (Rev. 1), para. 4.68 [2].

9.11. While the verification may be conveniently subdivided in phases that are performed at various significant stages of the design, a final independent verification of the safety assessment should always be performed by the operating organization when the design has been finalized.

9.12. Independent verification usually addresses the stages before the beginning of plant construction and focuses on safety analysis originally performed by the design organization. It should be, however, applied by analogy to other subsequent verification activities.

9.13. Any findings or conclusion from the verification should be justified using one of the following methods, as appropriate:

- Comparison with requirements of the law, regulation or other legal requirements;
- Comparison with guidance documents of the regulatory body;
- Comparison with IAEA safety standards or guidance documents;
- Comparison with similar projects;
- Use of general experience from previous projects;
- Independent verification calculations.

9.14. All numerical models used in safety analysis should show their reliability through comparisons, independent analyses and qualification, with the aim of demonstrating that their intrinsic uncertainty level complies with the reliability required for the whole design project.

9.15. In accordance with GSR Part 4 (Rev.1), para. 4.69 [2], the independent verification should consist of two main parts: overall (qualitative) review focused on quality and comprehensiveness of the safety analysis, and specific review that may contain comparison of results of submitted analyses with the results of new, independent calculations. The components of verification should include as appropriate the following:

- Compliance with the requirements of reference documents;
- Completeness of documentation;
- Correctness of input data;
- Selection of initiating events or accident scenarios;

- Selection of acceptance criteria;
- Selection of safety analysis method;
- Selection of safety analysis computer codes and adequacy of code validation;
- Selection of assumptions for ensuring safety margins;
- Adequacy of description/evaluation of results.

9.16. An independent check of selected computer calculations should be conducted to ensure that the analysis is correct. If sufficient verification and validation of the original code have not been performed, then an alternative code should be used to verify its accuracy. Use of different computer codes is preferable, but use of the same codes can meet the objectives of the review if plant models (including nodalization, initial and boundary conditions) were developed independently.

9.17. If independent calculations are performed, it may be appropriate to select at least one case from each group of initiating events, usually the case with lowest margin to the acceptance criterion. Attention should be paid to the fact that independent calculation is a time and resources demanding task.

9.18. Typically, the independent safety verification of deterministic safety analysis should confirm that the:

- Safety analysis was performed in accordance with relevant regulations, safety standards and other guidance documents;
- Selected postulated initiating events or accident scenarios reflect specifics of the given design and they bound the other cases;
- Combination of individual events and identification of consequential failures was done adequately;
- Computer codes used in safety analysis have been adequately validated for the given application;
- Computational models reflect experience and applicable guidance for their development and are appropriate for reliable prediction of operational states and accident conditions;
- Assumptions and data used in each analysis have been specified in an adequate way to ensure that the relevant acceptance criteria have been fulfilled and there are sufficient margins to prevent cliff edge effects;
- Adequate sensitivity calculations or uncertainty evaluations are available in order to assure that the demonstration of safety by safety analysis is robust enough;
- Consideration of operability of plant systems in different plant states was done in accordance with established rules for deterministic safety analysis and consistently with industrial standards;

- Compliance with the relevant acceptance criteria was achieved either by means of automatic systems, or personnel actions were considered only in case of availability of contextual boundary conditions for diagnosis, decision and performing the required action;
- Independent calculations are in reasonable qualitative and quantitative agreement with the original analysis, and they both demonstrate fulfilment of the relevant acceptance criteria;
- All discrepancies found in the safety analysis are clearly understood and explained and they do not question conclusions regarding acceptability of the design.

9.19. The independent verification and its results should preferably be documented in a separate verification report which describes scope, level of detail and methodology of the verification, and findings and conclusions from the qualitative and quantitative evaluation, including detailed comments on individual parts of the safety assessment and results of independent calculations.

9.20. The plant design models and data essential for the safety analysis should be kept up to date during the design phase and throughout the lifetime of the plant. This should be the responsibility of the designer during the design phase and of the operating organization over the life of the plant. It is advisable to maintain relevant documents or data bases centrally to ensure that the same information is used by all authors as well as by reviewers.

9.21. In connection with the plant data and models, proprietary rights associated with sharing know-how between the authors and reviewers may be a sensitive issue and should be reflected in appropriate confidentiality undertakings.

REFERENCES

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

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

[3] IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2016 Revision), IAEA, Vienna (in preparation). https://www-ns.iaea.org/standards/safety-glossary.asp.

[4] EUROPEAN COMMISSION, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA SAFETY STANDARDS SERIES No. GSR Part 3, IAEA, Vienna (2014).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Prospective Radiological Environmental Impact Assessment for Facilities and Activities, *[Draft IAEA Safety Guide, DS427 (Step 14, in publication)]*.

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementing Guidance. Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, Safety Report Series No. 52, IAEA, Vienna (2008).

[8] 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).

[9] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

[10] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS,

INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, I AEA, Vienna (2011).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.15, IAEA, Vienna (2009*). [Note: Under DS483 (Step 10, February 2017), Severe Accident Management Programme for Nuclear Power Plants]*.

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3 (Rev.1), IAEA, Vienna (2016*). [Note: DS484 (Step 5 in April 2016), Site Evaluation for Nuclear Installations, complete revision of NSR-3 and establishment of SSR-1]*.

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004). *[Note: Under DS494, together with NS-G-1.11, (Step 5), Protection Against Internal Hazards in the Design of Nuclear Power Plants]*.

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection Against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004). *[Note: Under DS494, together with NS-G-1.7, (Step 5), Protection Against Internal Hazards in the Design of Nuclear Power Plants]*.

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical Guidance. Computer Security at Nuclear Facilities. Reference Manual, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Format and Content of the Safety Analysis Report for Nuclear Power Plants, IAEA Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004), *[Note: Under DS449 (Step 8a), Format and Content of the Safety Analysis Report for Nuclear Power Plants]*.

[22] 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).

ANNEX. APPLICATION OF DETERMINISTIC SAFETY ANALYSIS

AREAS OF APPLICATION

A-1 Deterministic safety analysis may be carried out for a number of applications, including:

(a) Design of nuclear power plants by the designer or verification of the design by the operating organization;

(b) Safety analysis for licensing purposes (for authorizations), including authorizations for different stages for a new plant;

(c) Independent verification of the safety analysis by the regulatory body;

(d) Updating of safety analyses in the context of a periodic safety review to provide assurance that the original assessments and conclusions are still valid;

(e) Safety analysis of plant modifications;

(f) Analysis of actual operational events, or of combinations of such events with other hypothetical faults exceeding the limits of normal operation (analysis of near misses);

(g) Development and validation of emergency operating procedures;

(h) Development of severe accident management guidelines;

(i) Demonstration of success criteria and development of accident sequences in Level 1 PSA (probabilistic safety assessment) and Level 2 PSA.

A-2 Deterministic safety analysis associated with the design and authorization (licensing) of a nuclear power plant (items (a) to (e)) may be performed to demonstrate compliance with established acceptance criteria with adequate safety margins (ensured in different ways for design basis accidents and design extension conditions). Deterministic safety analysis associated with analysis of operational events, development of procedures or guidelines and support of the probabilistic safety analysis (items (f) to (i)) are typically not aimed at demonstration of compliance with acceptance criteria and are performed in a realistic way to the extent practicable.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DESIGN OF NUCLEAR POWER PLANTS

A-3 Safety requirements to perform safety analysis of the plant design are established in SSR-2/1 (Rev.1), Requirement 42, paras 5.71 to 5.74 [A-1]. More specific requirements on the scope and objectives of deterministic safety analysis are specified in SSR-2/1 (Rev.1), para. 5.75.

A-4 Main components of the design requirements determined by deterministic safety analysis typically include nuclear power plant equipment sizing, capacity, set point values for parameters initiation, termination and control of the systems and working (environmental) conditions, which

ensures effective operation of the systems in all relevant plant states and provides for adequate operating margins. The analysis also includes assessment of radiological effects for all plant states to ensure that there is confidence in future plant authorization.

A-5 The designer typically uses the safety analysis as an integral part of the design process, which typically consists of several iterations which may continue through the manufacture and construction of the plant. The safety analysis used in the design is performed according to a quality assurance (QA) programme.

A-6 The operating organization usually performs or verifies the safety analysis to the extent necessary to ensure that the as-built design will perform as expected in operation, and to demonstrate that the design meets the safety requirements at any point in the plant's design life. This independent verification is considered as a separate additional check to ensure a safe and proper design.

A-7 Although the deterministic safety analysis for design does not represent direct input for authorization of the nuclear power plant, its results are expected to provide for sufficient margins facilitating future authorization. It is therefore performed with the same scope and following the same or even more stringent rules as applicable for the authorization itself, which are described in the main body of this Safety Guide.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE LICENSING OF NUCLEAR POWER PLANTS

A-8 Compliance with all applicable regulations and standards and other relevant safety requirements is essential for the safe and reliable operation of a nuclear power plant. This may be demonstrated by means of an initial or an updated safety analysis, typically included in safety analysis reports for different stages of the plant lifetime and other supporting safety analysis associated with various submissions to the regulatory body.

A-9 On the basis of this licensing analysis, the robustness of the design in performing safety functions during all operating regimes and all plant states may be demonstrated. In particular, the effectiveness of the safety systems in combination with prescribed operator actions for anticipated operational occurrences and design basis accident conditions and of safety features in combination with expected operator actions for design extension conditions may be demonstrated.

A-10 The analysis for licensing is typically performed in accordance with established conservative or realistic rules, and includes comparison of the results of the analysis with relevant acceptance criteria. Demonstration of compliance with the acceptance criteria is performed to take into consideration uncertainties in the analysis. The rules for performing deterministic safety analysis are described in detail in the main body of this Safety Guide.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO INDEPENDENT VERIFICATION BY THE REGULATORY BODY

A-11 A separate independent review is typically carried out by the regulatory body to check the completeness and the consistency of the deterministic safety analyses submitted for licensing purposes and to verify that the design meets their requirements. As stated in GSR Part 4 (Rev 1), para. 4.71 [A-2], "The verification by the regulatory body is not part of the operating organization's process and it is not to be used or claimed by the operating organization as part of its independent verification."

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO PERIODIC SAFETY REVIEWS

A-12 New deterministic safety analyses may be required to refine or update the previous safety analyses in the context of a periodic safety review, to provide assurance that the original assessments and conclusions are still valid. In such analyses, account is typically taken of any margins that may be reduced owing to ageing over the period under consideration.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO PLANT MODIFICATIONS

A-13 A nuclear power plant is typically upgraded on the basis of feedback from operating experience, findings of periodic safety reviews (when performed), changes in regulatory requirements, advances in knowledge or developments in technology. Plant modifications include changes in systems, structures or components, changes in plant parameters, changes in plant configuration or changes in operating procedures.

A-14 Plant modifications are often aimed at the more economical utilization of the reactor and the nuclear fuel. Such modifications encompass uprating of the reactor power, the use of improved types of fuel and the use of innovative methods for core reloads. Such modifications often imply that the safety margins to operating limits are reduced and special care is taken to ensure that the limits are not exceeded.

A-15 Deterministic safety analyses are typically performed for supporting plant modifications. The scope of deterministic safety analysis typically corresponds to the safety significance of the modification. The safety analysis is usually performed in accordance with the rules established for deterministic analysis for design and for licensing.

A-16 Changes that require significant plant modifications such as power uprating and achieving a higher burn up, longer fuel cycles and life extensions are typically addressed by comprehensive deterministic safety analysis to demonstrate compliance with acceptance criteria. Special care is taken when a combination of many changes is implemented.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE ANALYSIS OF EVENTS EXCEEDING NORMAL OPERATION LIMITS

A-17 Deterministic safety analyses are used as a tool for obtaining a comprehensive understanding of events that occur during the operation of nuclear power plants and form an integral part of the feedback from operating experience. The events are analysed with the following objectives:

(a) To check the comprehensiveness of the earlier selection of postulated initiating events;
(b) To determine whether the transients that have been analysed in the safety analysis report bound the event;
(c) To provide additional information on the time dependence of the values of parameters that are not directly observable using the plant instrumentation;
(d) To check whether the operators and plant systems performed as intended;
(e) To check and review emergency operating procedures;
(f) To identify any new safety issues and questions arising from the analyses;
(g) To support the resolution of potential safety issues identified in the analysis of an event;
(h) To analyse the severity of possible consequences in the event of additional failures (such as severe accident precursors);
(i) To validate and adjust the models in the computer codes used for analyses and in training simulators.

A-18 The analysis of events is typically performed using a realistic (best estimate) approach. Actual plant data are used where possible. If there is a lack of detailed information on the plant operating parameters, sensitivity studies, with the variation of certain parameters, may be performed.

A-19 The evaluation of safety significant events is an important aspect of the feedback from operating experience. Modern best estimate computer codes make it possible to investigate and to gain a detailed understanding of plant behaviour. Conclusions from such analyses are incorporated into the plant modifications or plant procedures that address the feedback from operating experience.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DEVELOPMENT AND VALIDATION OF EMERGENCY OPERATING PROCEDURES

A-20 Best estimate deterministic safety analyses are typically performed to confirm the recovery strategies that have been developed to restore normal operational conditions at the plant following transients due to anticipated operational occurrences and design basis accidents and design extension conditions without significant fuel degradation. These strategies are reflected in the emergency operating procedures that define the actions to be taken to recover from such events. Deterministic safety analyses provide the input that is necessary to specify the operator actions to be taken, and the analyses play an important role in the review of accident management strategies. In the development

of the recovery strategies for determining the available time period for the operator to take effective action, sensitivity calculations are carried out on the timing of the necessary operator actions, and these calculations may be used to optimize the procedures.

A-21 After the emergency operating procedures have been developed, a verification analysis is performed to confirm that the final emergency operating procedure is consistent with the simulated plant behaviour. In addition, validation of emergency operating procedures is performed. This validation is usually performed by using plant simulators. The validation is made to confirm that a trained operator can perform the specified actions within the time period available and that the plant will reach a safe end state. Possible failures of plant systems and possible errors by the operator are considered in the sensitivity analyses.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DEVELOPMENT OF SEVERE ACCIDENT MANAGEMENT GUIDELINES

A-22 Deterministic safety analyses are also typically performed to assist the development of the strategy that an operator should follow if the emergency operating procedures fail to prevent progression of a design basis accident into design extension conditions with core melting. The analyses are carried out by using one or more of the specialized computer codes that are available to model relevant physical phenomena.

A-23 The analyses are used to identify what challenges to the integrity of the barriers or alternative pathways for their by-pass can be expected during the progression of accidents and which phenomena will occur. They are used to provide the basis for developing a set of guidelines for managing accidents and mitigating their consequences.

A-24 The analysis typically starts with the selection of the accident sequences that, without intervention by the operator, would lead to core damage. A grouping of accident sequences with similar characteristics is used to limit the number of sequences that need to be analysed. Such a categorization may be based on several indicators of the state of the plant: the postulated initiating event, the shutdown status, the status of the emergency core cooling systems, the coolant pressure boundary, the secondary heat sink, the system for the removal of containment heat and the containment boundary.

A-25 The accident management measures can be broadly divided into preventive and mitigatory measures. The analyses supporting the development of severe accident management guidelines typically focus on mitigatory measures, which are strategies for managing severe accidents to mitigate the consequences of core melt. For water cooled reactors, such strategies may include: coolant injection into the degraded core; depressurization of the primary circuit; activation of the containment spray system; ex-vessel cooling of molten corium; recombiners of combustible gasses and filtered containment venting [A-3]. Possible adverse effects that may occur as a consequence of taking

mitigatory measures are taken into account, such as pressure spikes, hydrogen generation, return to criticality, steam explosions, thermal shock or hydrogen deflagration or detonation. Similar to water cooled reactors, reactors of alternate designs consider mitigatory measures applicable to the design.

A-26 Transition from the emergency operating procedures to the severe accident management guidelines, if they are separate, is to be carefully defined and analysed, so that the operator always has guidance on the necessary actions and the monitoring of accident progression, regardless of the sequence of faults.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO DEMONSTRATION OF SUCCESS CRITERIA AND DEVELOPMENT OF ACCIDENT SEQUENCES IN LEVEL 1 PSA (PROBABILISTIC SAFETY ASSESSMENT) AND LEVEL 2 PSA

A-27 Deterministic analysis and probabilistic assessment are complementary means to provide a comprehensive view of the overall safety of the plant for the entire range of the frequency–consequence spectrum. However, it is acknowledged that some residual risks will remain.

A-28 Deterministic safety analysis has an important role in support of the probabilistic safety assessment by determining so called success criteria. Deterministic safety analysis is typically used to identify challenges to the integrity of the physical barriers, to determine the failure mode of a barrier when challenged and to determine whether an accident scenario may challenge several barriers. By means of the analysis it is to be determined whether an event sequence, for various combinations of equipment failures and human errors, can prevent nuclear fuel degradation. The deterministic analysis is to be performed in a realistic way.

A-29 More specifically, the deterministic analysis is performed to specify the order of actions for both automatic systems as well as operator actions. This determines the time available for operator actions in specific scenarios, and supports the specification of success criteria for required systems for prevention and mitigation measures.

REFERENCES TO THE ANNEX

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

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

[A-3] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.15, IAEA, Vienna (2009). *[Note: DS483 (Step 10, February 2017), Severe Accident Management Programme for Nuclear Power Plants]*.

CONTRIBUTORS TO DRAFTING AND REVIEW

Boyce, T.	Nuclear Regulatory Commission, United States of America
Courtin, E.J.F.	Areva NP, France
Harwood, C.	Canadian Nuclear Safety Commission, Canada
Herer, C.	Institute for Radiological Protection and Nuclear Safety, France
Luis-Hernandez, J.	Institute for Radiological Protection and Nuclear Safety, France
Lee, S.	Korean Institute for Nuclear Safety, Republic of Korea
Misak, J.	Nuclear Research Institute Rez, Czech Republic
Ochi, H.	Nuclear Regulatory Agency, Japan
Ramon, J.	Nuclear Safety Council, Spain
Spitzer, C.	International Atomic Energy Agency
Steinrötter, T	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) ~~g~~GmbH
Villalibre, P.	International Atomic Energy Agency
Virtanen, E	Radiation and Nuclear Safety Authority, Finland
Yllera, J.	International Atomic Energy Agency