31 August 2018

IAEA SAFETY STANDARDS

for protecting people and the environment

Status: Step 12b

For submission to the CSS

Approved by the PC

Awaiting editing in MTCD

Deterministic Safety Analysis for Nuclear Power Plants

SSG-2 Rev. 1

DS491

DRAFT Revised SAFETY GUIDE

CONTENTS

1. INTRODUCTION 1
Background 1
Objective 1
Scope 2
Structure 3
2. GENERAL CONSIDERATIONS 4
Objectives of deterministic safety analysis 4
Acceptance criteria for deterministic safety analysis 5
Uncertainty analysis in deterministic safety analysis 5
Approaches to deterministic safety analysis 5
Source term FOR A RELEASE OF RADIOACTIVE MATERIAL to the environment ... 7
3. IDENTIFICATION, CATEGORIZATION AND GROUPING OF POSTULATED INITIATING EVENTS AND ACCIDENT SCENARIOS 9
Management system 10
Normal operation 10
Postulated initiating events 11
Identification of postulated initiating events for anticipated operational occurrences and design basis accidents 13
GENERAL CONSIDERATIONS FOR IDENTIFICATION OF DESIGN EXTENSION CONDITIONS 17
IDENTIFICATION OF DESIGN EXTENSION CONDITIONS WITHOUT SIGNIFICANT FUEL DEGRADATION 18
IDENTIFICATION OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING 20
IDENTIFICATION OF postulated initiating eventS DUE TO INTERNAL AND EXTERNAL HAZARDS 21
EVENT SEQUENCES AND ACCIDENT SCENARIOS TO BE ‘PRACTICALLY ELIMINATED’ 22
4. ACCEPTANCE CRITERIA FOR DETERMINISTIC SAFETY ANALYSIS 23
5. USE OF COMPUTER CODES FOR DETERMINISTIC SAFETY ANALYSIS 26
BASIC RULES FOR SELECTION AND USE OF COMPUTER CODES 26
PROCESS MANAGEMENT IN CONNECTION WITH THE USE OF THE COMPUTER CODES 28
Interface between safety and security regarding the use of the codes 29
VERIFICATION OF COMPUTER CODES 29
VALIDATION OF COMPUTER CODES 30
QUALIFICATION OF INPUT DATA 33

DOCUMENTATION OF COMPUTER CODES 33

6. GENERAL APPROACHES FOR ENSURING SAFETY MARGINS IN DETERMINISTIC SAFETY ANALYSIS 34

GENERAL CONSIDERATIONS 34

CONSERVATIVE approach AND COMBINED APPROACH TO DETERMINISTIC SAFETY ANALYSIS FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENTS 36

BEST ESTIMATE DETERMINISTIC SAFETY ANALYSIS WITH QUANTIFICATION OF UNCERTAINTIES FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENTS 38

7. DETERMINISTIC SAFETY ANALYSIS FOR DIFFERENT PLANT STATES 40

GENERAL CONSIDERATIONS 40

DETERMINISTIC SAFETY ANALYSIS FOR NORMAL OPERATION 41

Specific objectives of the analysis 41
Acceptance criteria 41
Availability of systems 42
Operator actions 42
Analysis assumptions and treatment of uncertainties 42

REALISTIC DETERMINISTIC SAFETY ANALYSIS FOR ANTICIPATED OPERATIONAL OCCURRENCES 42

Specific objectives of the analysis 42
Acceptance criteria 43
Availability of systems 43
Operator actions 43
Analysis assumptions and treatment of uncertainties 44

CONSERVATIVE DETERMINISTIC SAFETY ANALYSIS FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENTS 44

Specific objectives of the analysis 44
Acceptance criteria 45
Availability of systems 46
Operator actions 47
Analysis assumptions and treatment of uncertainties 47

DETERMINISTIC SAFETY ANALYSIS FOR DESIGN EXTENSION CONDITIONS WITHOUT SIGNIFICANT FUEL DEGRADATION 48

Specific objectives of the analysis 48
Acceptance criteria 48
Availability of systems 48
Operator actions 49
Analysis assumptions and treatment of uncertainties 50

DETERMINISTIC SAFETY ANALYSIS FOR DESIGN EXTENSION CONDITIONS WITH CORE MELTING 50

Specific objectives of the analysis 50
Acceptance criteria 50
Availability of systems 51
Operator actions 52
Analysis assumptions and treatment of uncertainties 52

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

COULD LEAD AN EARLY RADIOACTIVE RELEASE OR A LARGE RADIOACTIVE RELEASE 53

8. DOCUMENTATION, REVIEW AND UPDATING OF DETERMINISTIC SAFETY ANALYSIS 54

DOCUMENTATION 54

Sensitive information in documentation 56

REVIEW AND UPDATing OF DETERMINISTIC SAFETY ANALYSIS 56

9. INDEPENDENT VERIFICATION OF DETERMINISTIC SAFETY ANALYSIS BY THE LICENSEE 56

REFERENCES 61

ANNEX I. APPLICATION OF DETERMINISTIC SAFETY ANALYSIS 64

AREAS OF APPLICATION 64

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DESIGN OF NUCLEAR POWER PLANTS 64

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE LICENSING OF NUCLEAR POWER PLANTS 65

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO INDEPENDENT VERIFICATION BY THE REGULATORY BODY 65

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO PERIODIC SAFETY REVIEWS 66

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO PLANT MODIFICATIONS 66

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE ANALYSIS OF EVENTS EXCEEDING NORMAL OPERATION LIMITS 66

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DEVELOPMENT AND VALIDATION OF EMERGENCY OPERATING PROCEDURES 67

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DEVELOPMENT OF SEVERE ACCIDENT MANAGEMENT GUIDELINES 68

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO DEMONSTRATION OF SUCCESS CRITERIA AND DEVELOPMENT OF ACCIDENT SEQUENCES IN LEVEL 1 PSA AND LEVEL 2 PSA 69

REFERENCES FOR ANNEX I 70

ANNEX II. FREQUENCY RANGES OF ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENT CATEGORIES 71

CONTRIBUTORS TO DRAFTING AND REVIEW 72

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 SSR-2/1 (Rev. 1) [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 previous version of SSG-2[1]. The modifications incorporated in this Safety Guide reflect recent experience of deterministic safety analysis included in safety analysis reports for designs for new nuclear power plants and in the application of deterministic safety analysis to existing nuclear power plants. The Safety Guide has also been updated to maintain consistency with current IAEA safety standards, including those Safety Requirements publications updated to reflect lessons from the Fukushima Daiichi nuclear power plant accident.

OBJECTIVE

1.4. The objective of this Safety Guide is to provide recommendations and guidance for designers, operating organizations, regulatory bodies and technical support organizations on performing deterministic safety analysis and on its application to nuclear power plants. 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 provided to meet the applicable 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.

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

SCOPE

1.5. This Safety Guide applies to nuclear power plants. It addresses ways of performing deterministic safety analyses to achieve their purposes in meeting safety requirements. Such analyses are primarily required to demonstrate adequate fulfilment of safety functions by the design, to ensure that barriers to the release of radioactive material will prevent an uncontrolled release to the environment for all plant states, and validity of the operational limits and conditions. Deterministic safety analyses are also required to determine the characteristics of potential releases (source terms) depending on the status of the barriers for different plant states.

1.6. This Safety Guide focuses primarily on deterministic safety analysis for the safety of designs for new nuclear power plants and, as far as reasonably practicable or achievable, is also applicable to the safety re-evaluation or re-assessment of existing nuclear power plants when operating organizations review their safety assessment. The recommendations provided are intended to be consistent with the scope of applicability indicated in 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 recommendations provided in this Safety Guide focus 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, to design extension conditions including severe accidents.

1.8. This Safety Guide deals with human errors and failures of plant systems (e.g. systems in 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 lead 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 resulting from the hazards and potentially inducing failures in plant systems are taken into account in determining initiating events to be analysed.

1.9. This Safety Guide addresses the use of deterministic safety analysis for design or licensing purposes, aimed at demonstrating, with adequate margins, compliance with established acceptance criteria.

1.10. This Safety Guide addresses different options available for performing deterministic safety analysis, namely the conservative approach, the best estimate approach with and without quantification of uncertainty, and a combined approach.

1.11. This Safety Guide focuses on neutronic, thermohydraulic, fuel (or fuel channel for pressurized heavy water reactors) and radiological analysis. Other types of analysis, in particular structural analysis of structures and components, 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. Neutronic and thermohydraulic analysis provides necessary boundary conditions for structural analysis.

1.12. This Safety Guide covers aspects of the analysis of releases of radioactive material, up to and including the determination of the source term for releases to the environment for anticipated operational occurrences and accident conditions (paras 2.16–2.18). 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 (see GSR Part 3 [4]). 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. GSG-10 [5].

1.13. This Safety Guide describes general rules and processes to be followed in performing deterministic safety analysis. The Safety Guide does not describe specific phenomena and does not systematically identify the key factors essential for neutronic, thermohydraulic fuel (or fuel channel) and radiological analysis. When such information is provided in this Safety Guide it is intended as an illustration or example and should not be understood as a comprehensive description.

1.14. Recommendations on nuclear security are out of the scope of this Safety Guide. In general, documentation and electronic records relating to deterministic safety analysis processes and outputs provide limited information regarding equipment location and vulnerability, and practically no information on cable routes and other aspects of the plant layout. However, such information needs to be reviewed to identify any sensitive information that could be used to support malicious acts, and such information needs to be protected appropriately. Guidance on sensitive information and information security is provided in Ref. [6].

STRUCTURE

1.15. This Safety Guide consists of nine sections and two annexes. Section 2 introduces some basic concepts and terminology used in the area of deterministic safety analysis, as a basis for the specific recommendations provided in the other sections.

1.16. The sequence of subsequent sections corresponds to the general process to perform deterministic safety analysis. Section 3 describes methods of systematic identification, categorization and grouping of initiating events and accident scenarios to be addressed by deterministic safety analysis, and includes practical advice on selection of events to be analysed for the different plant states. 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. 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. Section 7 provides specific guidance on performing deterministic safety analysis for each individual plant state. Section 8 includes guidance on the documentation, review and updating of deterministic safety analysis. Section 9 provides guidance for independent verification of safety assessment, including verification of deterministic safety analysis.

1.17. Annex I indicates additional applications of the computer codes used for deterministic safety analysis, besides the nuclear power plant design and authorization. Annex II indicates the frequency ranges of anticipated operational occurrences and design basis accident categories used in some States for new reactors.

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 can be performed with the necessary reliability and that the necessary structures, systems 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 below acceptable limits. Deterministic safety analysis is aimed at demonstrating 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 information and analysis relating to fabrication, testing, inspection, evaluation of the operating experience) and by probabilistic safety analysis, is also intended to contribute to demonstrating that the source term, and the potential 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 aim of deterministic safety analyses performed for different plant states is to demonstrate the 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 of the plant to postulated initiating events, alone or in combination with additional postulated failures. A set of rules and acceptance criteria specific to each plant state is applied. Typically, these analyses focus on neutronic, thermohydraulic, thermomechanical, structural and radiological aspects, which are analysed with appropriate computational tools. Computational simulations are carried out specifically for predetermined operating modes and plant states.

2.4. The results of computations are space and time dependent values of selected 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 for a release to the environment).

ACCEPTANCE CRITERIA FOR DETERMINISTIC SAFETY ANALYSIS

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

(a) Safety criteria: criteria that relate either directly to the radiological consequences of operational states or accident conditions, or to the integrity of barriers against releases of radioactive material, with due consideration given to maintaining the safety functions;

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

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

2.6. In this Safety Guide only safety acceptance criteria 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. The use of uncertainty analysis in deterministic safety analysis is addressed in paras 6.21–6.29. Several methods for performing uncertainty analysis have been published (e.g. in Ref. [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 used (see Section 5), the assumptions made about availability of systems and the initial and boundary conditions applied for the analysis.

TABLE 1. OPTIONS FOR PERFORMING DETERMINISTIC SAFETY ANALYSIS

Option	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 in which both the assumed plant conditions and the physical models are set conservatively. In a conservative approach parameters need to be allocated values that will have an unfavourable effect in relation to specific acceptance criteria. The conservative approach was commonly adopted in the early days of safety analysis to simplify the analysis and to compensate for limitations in modelling and knowledge of physical phenomena with large conservatisms. It was assumed that such an approach would bound many similar transients in a way that the acceptance criteria would be met for all bounded transients.

2.10. Experimental research has resulted in a significant increase of knowledge of physical phenomena, 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 (e.g. potential masking of important phenomena, conservatisms in different parameters potentially cancelling each other out), option 1 is rarely used now and is not suggested for current safety analysis, except in situations when scientific knowledge and experimental support is limited. Option 1 remains relevant, however, as it may have been used in legacy analyses.

2.11. Option 2 is a combined approach based on the use of ‘best estimate’ models and computer codes instead of conservative models and codes (para. 6.12). Best estimate codes are used in combination with conservative initial and boundary conditions and with conservative assumptions regarding the

[2] For simplicity in this Safety Guide the term ‘realistic approach’ or ‘realistic analysis’ is used to mean best estimate analysis without quantification of uncertainties.

availability of systems, assuming that all uncertainties associated with the code models are well established and that plant parameters used are conservative based on plant operating experience. The complete analysis requires use of sensitivity studies to justify the selection of conservative input data. Option 2 is commonly used for design basis accidents and for conservative analysis of anticipated operational occurrences.

2.12. Option 3 is a 'best estimate plus uncertainty' approach. This allows the use of best estimate computer codes together with more realistic assumptions. A mixture of best estimate and partially unfavourable (i.e. somewhat conservative) initial and boundary conditions may be used, taking into account the very low probability that all parameters would be at their most pessimistic value at the same time. Conservative assumptions are usually made regarding availability of systems. In order to ensure the overall conservatism required in analysis of design basis accidents, the uncertainties need to be identified, quantified and statistically combined. Option 3 contains a certain level of conservatism and is currently 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 often employed. This is because the tendency is to use best estimate input data whenever extensive data are available, and to use conservative input data whenever data are scarce. The difference between these options is the statistical combination of uncertainties.

2.14. Deterministic safety analysis performed in accordance with Options 1, 2 and 3 is considered to be conservative, with the level of conservatism decreasing from Option 1 to 3 (see paras 2.9–2.13).

2.15. Option 4 allows the use of best estimate models and codes and best estimates of system availability and initial and boundary conditions. Option 4 is appropriate for realistic analysis of anticipated operational occurrences aimed at assessment of control system capability (paras 7.17–7.44) and in general for best estimate analysis of design extension conditions (paras 7.45–7.67), as well as for the purpose of justifying prescribed operator actions in realistic analysis. Deterministic analysis for operating events that may necessitate a short term relaxation of regulatory requirements may also rely on best estimate modelling. More detailed information regarding modelling assumptions applicable for different options is provided in Section 7.

SOURCE TERM FOR A RELEASE OF RADIOACTIVE MATERIAL TO THE ENVIRONMENT

2.16. Deterministic safety analysis includes as one of its essential components determination of source terms for releases of radioactive material, as a key factor for prediction of dispersion of such material in the environment and ultimately of radiation doses to the plant staff and to the public and radiological impact on the environment. The source term is "the amount and isotopic composition of radioactive material released (or postulated to be released) from a facility"; it is used "in modelling releases of

radionuclides to the environment, in particular in the context of accidents at nuclear installations or releases from radioactive waste in repositories" [3].

2.17. To evaluate the source term from a nuclear installation, it is necessary to identify the sources of radiation, to determine the inventories of radionuclides that are produced and to know the mechanisms by which radioactive material can travel from the source through the installation and be released to the environment. Under accident conditions, source term evaluation requires simulation codes that are capable of predicting fission product release from fuel elements, transport through the primary system and containment or spent fuel pool building, the related chemistry affecting this transport and the form in which the radioactive material would be released.

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

(a) To confirm that the design is optimized so that the source term is 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 support specification of the conditions for the qualification of the equipment required to withstand accident conditions;

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

(g) To support the design of safety features for the mitigation of the consequences 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 for deterministic safety analysis apply also to determination of the source term. In several places of this Safety Guide aspects associated with

[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].

determination of the source term are introduced to remind readers of the applicability of the general rules to 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 design)' from SSR-2/1 (Rev. 1) [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 address all postulated initiating events originating in any part of the plant and having the potential to lead to a radioactive release to the environment, both on their own and in combination with possible 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 radioactive material not only from the reactor core but also from other relevant sources, such as fuel elements stored at the plant and systems dealing with radioactive material.

3.3. Where applicable, the possibility should be considered that a single cause could simultaneously initiate initiating events in several or even all reactors in the case of a multiple unit nuclear power plant, or spent fuel storage units, or 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. The initial conditions should assume a steady state with normal operation equipment operating prior to the initiating event.

3.5. Each configuration of shutdown modes, including refuelling and maintenance, should be considered. For these modes, possible failures or other factors that could occur during shutdown and lead to increased risk should be considered, such as: inability to start some safety systems automatically or manually; disabled automation systems; equipment undergoing maintenance or repair; reduced amounts of coolant in the primary circuit and, for some modes, in the secondary circuit; instrumentation

[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.

switched off or non-functional so that measurements are not made; open primary circuit; and open containment.

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

3.7. Postulated initiating events taking place during plant operating modes of negligibly short duration may be excluded from deterministic safety analysis if careful analysis and quantitative assessment confirms that their potential contribution to the overall risk, including the risk of conditions arising that could lead to an early radioactive release or a large radioactive release, is also negligible. 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 of deterministic safety analysis and use of the results should take into account the recommendations of GS-G-3.1 [12] and GS-G-3.5 [13] for meeting Requirements 1–3 of SSR-2/1 (Rev.1) [1] and the requirements established in GSR Part 2 [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 startup 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 owing to transfer to different plant modes or changes in the plant power output. A major aim of the analysis for transients occurring during normal operation 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.

3.12. A list of postulated initiating events should be prepared. The list should be comprehensive to ensure 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 operating experience feedback including, depending on availability of relevant data, operating experience from the actual nuclear power plant or from similar plants.

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

(a) Failures of structures, systems and components of the plant (partial failure if relevant), including possible spurious actuation;

(b) 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;

(c) 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:

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

(b) 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 analysis for anticipated operational occurrences, design basis accidents or design extension conditions should include consideration of potential failure of the equipment that could be affected by such an event;

(c) For internal hazards such as fire or flood, or for failures caused by 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. In addition to the set of initiating failures and consequential failures, other 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 failures and the failures that are part of, or directly caused by, the postulated initiating event. Finally, some failures may be added to bound a set of similar events, so as to limit the number of analyses.

3.17. The postulated initiating events should include only those failures (either initial or consequential) that directly lead to the challenging of safety functions and ultimately to threatening the integrity of barriers to releases of radioactive material. 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, including multiple failures resulting from these hazards.

3.18. SSR-2/1 (Rev. 1) [1] states that:

> "Where the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of 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:

(a) Use of analytical methods such as hazard and operability analysis (HAZOP), failure modes and effects analysis, engineering judgement and master logic diagrams;

(b) Comparison with the list of postulated initiating events developed for safety analysis of similar plants (ensuring that previously identified deficiencies are not propagated);

(c) Analysis of operating experience data for similar plants;

(d) Use of insights and results from probabilistic safety analysis.

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) have traditionally been considered in deterministic safety analysis as design basis accidents. These accidents should be considered because they are representative of a type of accident that the reactor has to be protected against. They should not be excluded from the category of design basis accidents unless careful analysis and quantitative assessment of their potential contribution to the overall risk, including to conditions arising that could lead to an early radioactive release or a large radioactive release, indicate that they can be excluded.

3.21. Failures occurring in the supporting systems that impede the operation of systems necessary for normal operation should also be considered as postulated initiating events, if such failures ultimately 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 assessment proceed, as part of an iterative process between these two activities. The postulated initiating events should also be periodically reviewed throughout the lifetime of the plant, for example as part of a periodic safety review, to ensure that they remain valid.

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 the physical evolution of the postulated initiating events. Each group should include event sequences that lead to a similar challenge to the safety functions and barriers and need similar mitigating systems to drive the plant to a safe state. Therefore, they can be bounded by a single representative event sequence, which is usually referred to when dealing with the group (and often identified by the associated postulated initiating event itself). These groups are also categorized in accordance with 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 sequence, with focus on aspects such as 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’ would belong to the type of event sequence ‘Decrease in reactor heat removal’.

3.25. The postulated initiating events associated with anticipated operational occurrences and design basis accidents should reflect the specific characteristics 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, in accordance with the typical type of sequences listed below:

(a) Increase or decrease in the heat removal from the reactor coolant system;

(b) Increase or decrease in the flow rate of the reactor coolant system;

(c) Anomalies in reactivity and power distribution in the reactor core, or anomalies in reactivity in fresh or spent fuel in storage;

(d) Increase or decrease in the reactor coolant inventory;

(e) Leaks in the reactor coolant system with potential by-pass of the containment;

(f) Leaks outside the containment;

(g) Reduction in or loss of cooling of the fuel in the spent fuel storage pool;

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

(i) 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 groupings of postulated initiating events may be appropriate to adequately address different pathways that could lead to the release of radioactive material to the environment. Special attention should be paid to accidents in which the release of radioactive material could by-pass the containment, because of the potentially severe consequences even in the case of relatively small releases.

3.27. Within each group of postulated initiating events, the representative event sequences should also be subdivided into categories based on the frequency of the most frequent postulated initiating event in the group. The assignment of each postulated initiating event to a frequency range should be checked by an appropriate methodology. Possible anticipated operational occurrences and design basis accident categories with their indicative frequency ranges, as used in some States for new reactors, are indicated in Table II-1 of Annex II.

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 sequence. This list is broadly indicative, but the actual list will depend on the type of reactor and the actual design:

(a) Increase in heat removal from the reactor: 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;

(b) Decrease in heat removal from the reactor: feedwater 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);

(c) Increase in flow rate of the reactor coolant system: start of a main coolant pump;

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

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

(f) Anomalies in reactivity in fresh or spent fuel in storage: boron dilution in spent fuel pool;

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

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

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

(j) Reduction in or loss of cooling of the fuel in the spent fuel storage pools: loss of off-site power; malfunctions in decay heat removal system; leaking of pool coolant;

(k) Release of radioactive material due to leak in reactor coolant system, with potential containment by-pass;

(l) 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 potentially 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, i.e. demonstrating that is possible to manage them “by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator” (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 lower limit of frequency should take account of the safety targets established for the specific reactor.

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

(a) Increase in heat removal from the reactor: steam line breaks;

(b) Decrease in heat removal from the reactor: loss of feedwater;

(c) Decrease in flow rate of the reactor coolant system: seizure or shaft break of main coolant pump; trip of all coolant pumps;

(d) Anomalies in reactivity and power distribution: uncontrolled withdrawal of control rod (or control rod bank); ejection of control rod (pressurized water reactor); rod drop accident (boiling water reactor); boron dilution due to the startup of an inactive loop (pressurized water reactor);

(e) 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;

(f) Reduction in or loss of cooling of the fuel in the spent fuel storage pools: break of piping connected to the water of the pool;

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

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

(i) Release of radioactive material due to leak in reactor coolant system, with potential containment by-pass, 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;

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

3.31. Probabilistic analysis should be used in support of deterministic analysis in justifying the categorization of postulated initiating events in accordance with their frequency of occurrence. The calculation of the frequency should take account of the relative frequencies of the plant operational state(s) in which the postulated initiating event could occur, such as full power or hot shutdown. Particular care should be taken to ensure that a transient with the potential to degrade the integrity of barriers is assigned to a category consistent with its possible effect on the barriers.

3.32. A number of limiting cases, 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 collectively they include cases presenting the greatest possible challenges to each of the relevant acceptance criteria and involving limiting values for the performance parameters of safety related equipment. Several postulated initiating events may be combined, and/or their consequences amplified, within a bounding scenario in order to encompass all of 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. 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 — including degradation of core cooling, buildup of containment pressure and transport and environmental release of radioactive material — and, specifically for pressurized water reactors, also for leakage of primary coolant to the steam generator bypassing the containment, pressurized thermal shock and boron dilution (reactivity accident) due, for example, to a boiling condensing regime.

3.34. Accidents during the handling of both fresh and irradiated fuel should also be evaluated. Such accidents can occur both inside and outside the containment.

3.35. There are a number of other types of postulated initiating event that would result in a release of radioactive material outside the containment and whose source term should be evaluated. Such events 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) An increase of reactivity in the fresh or spent fuel;
(c) An accidental discharge from any of the 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 discharges of radioactive material during normal operation;
(e) An accident during reload or maintenance when the reactor or containment might be open.

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

GENERAL CONSIDERATIONS FOR IDENTIFICATION OF DESIGN EXTENSION CONDITIONS

3.37. Requirement 20 in SSR-2/1 (Rev. 1) [1] states that

> “A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant’s capabilities to withstand, without

unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences."

3.38. 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[5]. 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 sequences for design extension conditions without significant fuel degradation should be based on the consideration of single initiating events of very low frequency or multiple failures, to meet the acceptance criteria regarding prevention of core damage.

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

(a) Initiating events that could lead to situations beyond the capability of safety systems that are designed for design basis accidents. A typical example is multiple tube rupture beyond the design basis assumptions in a steam generator of a pressurized water reactor;

(b) 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 (and in particular for the most frequent anticipated operational occurrences and design basis accidents);

(c) Credible postulated initiating events involving multiple failures 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 heat removal both in accident conditions and during shutdown. The identification of these sequences should result from a

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

systematic analysis of the effects on the plant of a total failure of any safety system used in normal operation.

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

(a) Very low frequency initiating events typically not considered as design basis accidents:

- 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);

(b) 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 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;

(c) Postulated initiating events involving multiple failures:

- 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 to cause immediate or delayed consequential multiple failures in both operational and safety systems.

3.43. Sequences for different design extension conditions without significant fuel degradation that are associated with similar safety challenges should be grouped together. 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 number of specific sequences with core melting (severe accidents) should be selected for analysis in order to establish the design basis for the safety features for mitigating the consequences of such accidents, in accordance with the plant safety objectives. These sequences should be selected in order to represent all of the main physical phenomena (e.g. primary circuit pressure, reactor decay heat or containment status) involved in core melt sequences.

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

3.47. The representative sequences for design extension conditions with core melting, in accordance with each acceptance criterion, should be analysed to determine limiting conditions, particularly those sequences that could challenge the integrity of the containment. 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. Design extension conditions are, to a large extent, technology and design dependent, but the accidents below are provided as a preliminary reference of design extension conditions with core melting (severe accidents):

(a) 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 or/and the loss of the normal access to the ultimate heat sink (exact sequence is design dependent);

(b) 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. A low estimated frequency of occurrence for 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 an accident with core melting are 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 phenomena associated with a severe accident. These parameters should be used in the deterministic analyses of the plant structures, systems and components 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 assessing[6] whether the equipment used in severe accidents is capable of performing its 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 take account of effects and loads from events caused by relevant site specific internal and external hazards, individually and in combination (SSR-2/1 (Rev.1), Requirement 17, paras 5.15A–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[7]. The hazards themselves do not represent initiating events but they are associated with loads, which can initiate such events.

3.52. In accordance with paras 5.15B, 5.19 and 5.63 of SSR-2/1 (Rev.1) [1], in determining postulated initiating events caused by site specific hazards for multiple unit plant sites, the possibility of affecting 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[8], which is performed by using probabilistic methods or appropriate engineering methods, should aim to demonstrate for each hazard that either:

---

[6]. Although equipment qualification is outside the scope of this Safety Guide, it is understood that typical equipment qualification programmes for design extension conditions with core melting might not always be applicable and an assessment of the operability of structures, systems and components is acceptable. The term 'survivability assessment' is used in some States for such an assessment.

[7] The 'fundamental safety functions' are also called 'main safety functions' [3].

[8] See further guidance in NS-G-1.5 [16], NS-G-1.7 [17] and NS-G-1.11 [18].

(a) The hazard can be screened out due to its negligible contribution to risk; or

(b) The nuclear power plant design is robust enough to prevent any transition from the load caused by the hazard into an initiating event; or

(c) 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 credit only the functions of those structures, systems and components that are qualified for or protected from the hazard.

EVENT SEQUENCES AND ACCIDENT SCENARIOS TO BE 'PRACTICALLY ELIMINATED'

3.55. Paragraph 2.13(4) of SSR-2/1 (Rev. 1) [1] states that:

> "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[9] are required to be 'practically eliminated'[10]."

3.56. The event sequences for which specific demonstration of their 'practical elimination' is required should be classified as follows:

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

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

  (ii) Uncontrolled reactivity accidents;

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

  (i) Highly energetic direct containment heating;

  (ii) Large steam explosion;

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

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

[10] "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" [1].

(c) Severe accident sequences that could lead to late containment failure[11]:

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

(ii) Long term loss of containment heat removal;

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

(d) Severe accident with containment bypass;

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

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 7.68–7.72).

4. ACCEPTANCE CRITERIA FOR DETERMINISTIC SAFETY ANALYSIS

4.1. Paragraph 4.57 of GSR Part 4 (Rev. 1) [2] states that: "Criteria for judging safety, sufficient to meet … the requirements of the designer, the operating organization and the regulatory body, shall be defined for the safety analysis."

4.2. Paragraph 5.75 of SSR-2/1 (Rev.1) [1] states that: "The deterministic safety analysis shall mainly provide: … (d) Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection". 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 to the release of radioactive material in order to prevent releases (and hence consequences) above acceptable limits. Selection of the criteria should ensure sufficient margin between the criterion and the physical limit for loss of integrity of a barrier.

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:

[11] These conditions need to be analysed during the identification of situations to be practically eliminated. Nevertheless, consequences from (i) and (ii) could generally be mitigated with the implementation of reasonable technical means.

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

(b) Detailed (derived) technical criteria, which relate to integrity of barriers to releases of radioactive material (e.g. the fuel matrix, fuel cladding, reactor coolant system pressure boundary, containment). These are defined in 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 dose, equivalent dose or dose rate to workers at the nuclear power plant, members of the public or the environment, including non-human biota, as appropriate. Radiological acceptance criteria regarding doses should be defined in accordance with the applicable safety requirements (see Requirements 5 and 81 [1] of SSR-2/1 (Rev.1)).

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

4.8. Radiological acceptance criteria for normal operation should typically be expressed as effective dose limits for the workers at the plant and for members of the public in the vicinity of the plant, or as authorized limits on the activity in planned discharges from the plant (see SSR-2/1 (Rev. 1), Requirement 5 [1]).

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

4.10. The radiological acceptance criteria for design basis accidents should ensure that Requirement 19 and the requirements in para. 5.25 of SSR-2/1 (Rev.1) [1] are met.

4.11. The radiological acceptance criteria for design extension conditions to be established should ensure that Requirement 20 and the requirements in para. 5.31A of SSR-2/1 (Rev.1) [1] are met.

4.12. Technical acceptance criteria should be set in terms of the variables that govern the physical processes that challenge the integrity of a barrier. It is common engineering practice to use surrogate variables[12] relating 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, sufficient conservatism should be included to ensure that there are adequate safety margins to the loss of integrity of the barrier.

[12] In this Safety Guide, a surrogate variable is a measurable variable that provides an indirect measure of another variable that cannot be directly measured.

4.13. The following groups and examples of criteria should be considered, as appropriate depending on specific design solutions, in the specification of a set of technical acceptance criteria:

(a) Criteria relating to integrity of nuclear fuel matrix: maximum fuel temperature and maximum radially averaged fuel enthalpy (taking into account burnup, fuel composition and additives, such as burnable absorbers, in both values);

(b) Criteria relating to integrity of fuel cladding: minimum departure from nucleate boiling ratio; maximum cladding temperature; maximum local cladding oxidation;

(c) Criteria relating to integrity of the whole reactor core: adequate subcriticality; maximum production of hydrogen from oxidation of cladding; maximum damage of fuel elements in the core; maximum deformation of fuel assemblies (as required for cooling, insertion of control rods and removal of control rods); calandria vessel integrity (for pressurized heavy water reactors);

(d) Criteria relating to integrity of nuclear fuel located outside the reactor: adequate subcriticality; adequate water level above the fuel assemblies and adequate heat removal;

(e) Criteria relating to integrity of the reactor coolant system: maximum coolant pressure; maximum temperature, pressure and temperature changes and resulting stresses and 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;

(f) Criteria relating to integrity of the secondary circuit (if relevant): maximum coolant pressure; maximum temperature, pressure and temperature changes in the secondary circuit equipment;

(g) Criteria relating to integrity of the containment and limitation of releases to the environment: value and duration of maximum and minimum pressure; maximum pressure differences acting on containment walls; maximum leakages; maximum concentration of flammable or explosive gases; acceptable working environment for operation of systems; maximum temperature in the containment;

(h) Criteria relating to integrity of any other component necessary to limit radiation exposure, such as the end shield in pressurized heavy water reactors: maximum pressure, temperature and heat-up rate.

4.14. For postulated initiating events occurring during shutdown modes or other cases with disabled or degraded integrity of any of the barriers, more restrictive criteria should be used if possible, 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 general, technical acceptance criteria relating 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 be maintained and containment bypass should be 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 burnup and content of burnable absorbers. Similarly, for limitation of radioactive releases, the 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 might 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 in the loads they may have to bear, and with the consequences of their failure.

4.18. In addition to all relevant physical quantities, the evaluation of stresses and strains should take account of 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 that are necessary 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. Requirement 18 of GSR Part 4 (Rev. 1) [2] states that: “Any calculational methods and computer codes used in the safety analysis shall undergo verification and validation.” The models and methods used in the computer codes for deterministic safety analysis should be appropriate and adequate for the purpose. The extent of the validation and verification necessary and the means for achieving it should 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 made in the models 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 model or calculational method is only designed to model physical processes in a particular range of conditions, and the code should not be applied outside this range.

(e) The numerical methods used in the code are accurate and robust.

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

(g) Compliance of the source coding with its description in the system code documentation has been assessed.

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 the main models used in the code;

(d) Establishing sensitivities of important processes to values of the main variables.

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 comparison with ‘separate effect tests’ and ‘integral effect tests’, as described in para. 5.25;

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

(c) Outputs from other codes that have been developed independently and use different methods;

(d) Results from standard problems and/or numerical benchmarks, when these are 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. It should be ensured that:

(a) All users of the code have received adequate training and have sufficient understanding of the models and the methods used in the code;

(b) The users or their supervisors are sufficiently experienced in the use of the code and have sufficient understanding of its uses and limitations for the specific 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, especially those relevant to the specific 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 5.39) 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 those chosen for separate effect tests and integral effect tests 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, using procedures that are specific to ensuring the quality of software. Established software engineering practices that are applicable to the development and maintenance of software critical to safety should be applied. 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 error in code development, only suitably qualified or supervised personnel should be involved in the development, verification and validation of the code. Similarly, in user organizations, only suitably qualified or supervised personnel should use the code.

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

5.12. When new versions of codes are developed, an established set of test cases should be simulated and run with the new version and any significant differences in the results compared to previous versions should be identified and 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. Guidance on computer security for nuclear facilities is provided in the IAEA Nuclear Security Series [19].

VERIFICATION OF COMPUTER CODES

5.14. Paragraph 4.60 of GSR Part 4 (Rev. 1) [2] indicates that verification of the code is required to include both model verification and system code verification.

5.15. Verification of the code should include demonstration that the code (source code and algorithm) accurately represents the mathematical model of the real system (model verification) and conforms to the code documentation (system code verification). In general, the verification should ensure that the numerical methods, the transformation of the equations into a numerical scheme to provide solutions, and the user options and restrictions are appropriately implemented in accordance with the specifications.

5.16. The verification of the code should be performed by means of review, inspection and audit. Checklists may be provided for review and inspection. Audits may 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 validity of the code verification for the intended platform should be assessed.

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

5.20. A complex code may include 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 code documentation.

VALIDATION OF COMPUTER CODES

5.21. Validation of the code should be performed to determine whether the mathematical models used in the code are an adequate representation of the real system being modelled. Outputs of the code should be compared, as far as possible, with observations 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 as required, 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. For example, the scope of validation may be relaxed for codes used in severe accident analysis, in view of the limited experimental data available, in which case additional reliance should be placed on verification (see paras 5.14–5.20).

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

5.24. The validation of the codes used in complex analysis should be performed in two phases: the development phase, in which the validation assessment is performed by the code developer, and the independent assessment phase, in which the validation assessment is performed by the code user.

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

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

(b) Separate effect tests. These are designed to highlight 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 5.30–5.32).

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

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

5.26. Validation against test data is the primary means of validation. However, in cases where no means to achieve appropriate data for validation are available for test cases of the types (b), (c) or (d) above, it is possible to enhance confidence in results by means of code–to-code comparisons or the use of bounding engineering judgement, to compensate for limitations in the full validation. The approach taken to validation and the use of the code should be justified.

5.27. The validation should ideally cover the full range of values of parameters, conditions and physical processes that the code is intended to model, in the specific applications for which it is to be used.

5.28. The scope of the validation performed by the code user should be consistent with the intended use 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.

5.29. For complex applications, a code might predict one set of test data with a high degree of accuracy but be inaccurate for other data sets. For such cases, a validation matrix should be developed for code validation, tailored to the application(s) for which the code is to be validated.

5.30. The validation matrix should include test data from different experimental facilities and from different sets of conditions in the same facility, and should ideally include basic tests, separate effect tests, integral effect tests and nuclear power plant level tests. The models and associated assumptions chosen at each level of validation should be consistent with one another and should not be different for different types of test. 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 validation matrix should be justified as being sufficient for the intended application(s) of the code.

5.31. 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 for each test are

appropriate. If data relating to other conditions are used, consideration should be given to scaling effects. A scaled experimental facility cannot be used to represent all of the phenomena that are relevant for a full size facility. Thus, for each scaled facility that is used in the validation 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.

5.32. When performing validation against experimental data, allowance for uncertainties in the measured data should be included in the determination of the uncertainty in the computer code's predictions. In addition, the evaluation of uncertainties based on scaled experimental results should be transposed to the real power plant application and this transposition should be evaluated and justified in assessing the overall uncertainty in the results.

5.33. The range of validity and the limitations of a computer code, established from its validation, should be documented in a validation report.

5.34. The results of validation should be used to determine the uncertainty in the results provided by code calculations. Different methods are available for assessing the uncertainty in the results.

5.35. 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.

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

5.37. For a code intended to be conservative regarding a particular acceptance criterion, it should be demonstrated that the code prediction for that criterion is conservative when compared with the experimental data (i.e. that predictions of negative consequences are worse than the likely actual consequences).

5.38. 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 in cases where results cannot be compared with plant data or experimental data. The procedures, code documentation and user guidelines should be carefully elaborated and followed to minimize such user effects. For example, user's procedures should include guidance on issues such as how to compile input data sets, selecting the appropriate models in the code, and general rules for preparing the nodalization.

5.39. The nodalization should be sufficiently detailed that all important phenomena of the scenario and all important design characteristics of the nuclear power plant are represented. A qualified nodalization that has successfully provided code outputs in 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

5.40. 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 and 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 and other plant documentation.

DOCUMENTATION OF COMPUTER CODES

5.41. Each computer code should 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 should also provide a description of the uncertainties in important models and in the overall code for typical applications. The code documentation should also include user guidelines and input descriptions to ensure that the user can use the code properly. A description of the experimental data or other key data used, a description of the computer options considered in the validation and a description of the validation results should also be included. The documentation should be available to all users.

5.42. 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 a description of the inputs, a programmer’s manual and a validation report.

5.43. 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 radioactive material would fail. Conservatisms might be introduced in many ways, such as in acceptance criteria or through conservative assumptions in physical models or in initial and boundary conditions.

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

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

6.4. Paragraph 5.26 of SSR-2/1 (Rev.1) [1] states that "The design basis accidents shall be analysed in a conservative manner. This approach involves postulating certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis." (See para. 2.14 of this Safety Guide.)

6.5. Paragraph 5.27 of SSR-2/1 (Rev.1) [1] states, in relation to the deterministic safety analysis of design extension conditions, that: "The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach" (although more stringent approaches may be used in accordance with specific regulatory requirements).

6.6. When best estimate analysis is used, adequate margins to the loss of integrity of barriers should still be ensured. It should be demonstrated by sensitivity analysis that cliff edge effects[13] potentially leading 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

[13] A 'cliff edge effect' is defined in the Safety Glossary as "An instance of severely abnormal conditions caused by an abrupt transition from one status of a facility to another following a small deviation in a parameter or a small variation in an input value" [3]. The term 'parameter' in this definition can 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.

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 values of parameters that represent the greatest challenges to safety, and for demonstration that realistically foreseeable changes in parameters do not lead to cliff edge effects. It should be taken into account that when sensitivity analyses are carried out by changing one parameter at a time, misleading results may be obtained because the possible compensatory or cumulative effects when several parameters change simultaneously are not necessarily reflected.

6.8. For practical reasons, only a limited number of parameters — those identified as having the more significant effect on results — can be considered in sensitivity analysis. Variation in the values of these parameters within a given range aims to identify the values that lead to the smallest margins to a selected acceptance criterion, and such values are criterion dependent. Moreover, the importance of any parameter may change during transients. Care should be taken to avoid situations in which arbitrary variations in selected parameters that are not independent may cause problems due to inconsistency of data (e.g. violation of mass balance).

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

(a) Use of the best estimate computer code in combination with conservative input data; or

(b) Use of a best estimate computer code in combination with best estimate input data, irrespective of how it is associated with the quantification of uncertainties both in the code models and in input data.

In the former case, the results are expressed in terms of a set of calculated conservative values of parameters that are limited by the acceptance criteria; in the latter 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 fouling of boilers or steam generators.

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

6.12. In the conservative approach or combined approach, conservative initial and boundary conditions should be selected from the ranges of parameters specified in the plant's operational 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 points and performance characteristics of plant systems such as pumps and power supplies, external sources and sinks for mass and energy, and other parameters that change 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.

6.13. Input data and modelling assumptions should be selected not only for neutronic and thermohydraulic aspects of anticipated operational occurrences and design basis accidents, but also for radiological aspects. In particular, for analysis of the source term for releases to the environment, the following factors should be addressed:

(a) Inventory of fission products and other radionuclides in the fuel (in the core or in the spent fuel pool);

(b) Activity in the reactor coolant system, including release of volatile fission products prior to or during the event (spiking);

(c) Time progression and scope of fuel damage (clad leakage);

(d) Fractions of radionuclides released from the fuel;

(e) Retention of radionuclides in the primary cooling system and in containment leakage pathways;

(f) Partitioning of fission products between steam and liquid phases of the coolant;

(g) Performance of containment systems (sprays, ventilation, filtering, deposition and resuspension);

(h) Leak rate and position of leaks from the containment;

(i) Timing and duration of releases;

(j) Chemical and physical forms of radioactive material released, in particular iodine;

(k) Effective height of release to the environment taking into account the energy of the releases.

6.14. When a best estimate code is used in combination with conservative inputs and assumptions, it should be ensured that the uncertainties associated with the best estimate code are sufficiently

compensated for by conservative inputs. The analysis should include a combination of validation of the code, use of conservatisms and use of sensitivity studies to evaluate and take into account the uncertainties relating to code models. These studies may be different depending on the type of transient, and therefore should be carried out for each deterministic safety analysis.

6.15. For the conservative or combined approaches, the initial and boundary conditions should be set to values that will lead to conservative results for the safety related parameters that are to be compared with the acceptance criteria. A single set of conservative values for initial and boundary conditions does not necessarily lead to conservative results for each safety related parameter or acceptance criterion. Therefore, the appropriate conservative initial and boundary conditions should be selected individually, depending on the specific transient and acceptance criteria.

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

(a) Intentional conservatisms might not always lead to the intended conservatism in the results, for example if different assumptions lead to compensatory effects and 'cancel out' conservatisms;

(b) The degree of conservatism can change during the course of the event, and an assumption might not remain conservative throughout the whole transient;

(c) The use of some conservative assumptions might lead to misleading or unrealistic predicted sequences of events and timescales;

(d) If conservative values are selected based on engineering judgment, there is a high risk that such selection is not properly implemented by the user and that it does not lead to conservative results.

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

6.17. Since the use of conservative computer codes can conceal the effects of 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 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 with respect to initial reactor conditions such as plant mode (power or shutdown), power level, residual heat level, fission product inventory, reactivity conditions, and 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 include the most unfavourable combinations that are possible.

6.20. Operating conditions occurring with negligibly low frequency and having a very limited duration might not need to be considered in the 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 particular for anticipated operational occurrences and design basis accidents, may be addressed in deterministic safety analysis 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 such 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 level of confidence.

6.22. Before quantification of uncertainties, it should be ensured that: the best estimate computer code used for the analysis is adequately validated; user effects (e.g. possible improper selection of values) are properly accounted for; the influence of the computational platform (hardware and software) on the results is minimized; and the methodology to assess the uncertainties is qualified.

6.23. A reliable assessment of the uncertainties is necessary to carry out robust 'best estimate with quantification of uncertainties' analyses, especially for the identification and separation of aleatory and epistemic sources of uncertainties[14]. These different sources of uncertainty 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), para. 4.59 [2]). The preferred means for assessing aleatory uncertainties is the collection of data from nuclear power plants on initial and boundary conditions that are relevant to the events being considered.

6.24. Quantification of uncertainties should be based on statistical combination of uncertainties in plant conditions and in code models (see para. 2.7) to ensure that, with a specified probability, a sufficiently large number of calculated results meet the acceptance criteria. For analysis of anticipated operational

[14] Aleatory uncertainty is uncertainty inherent in a phenomenon, and is of relevance for events or phenomena that occur in a random manner, such as random failures of items of equipment. Epistemic uncertainty is uncertainty attributable to incomplete knowledge about a phenomenon, which affects the ability to model it [3].

occurrences and design basis accidents it is typically required that assurance be provided at a 95% confidence level or greater that at least 95% of the results comply with applicable acceptance criteria for a plant. However, national regulations may require different levels of probability.

6.25. Within the uncertainty methods considered, uncertainties should be evaluated using either propagation of input uncertainties or extrapolation of output uncertainties. In the former approach, overall uncertainty in outputs is evaluated by performing a sufficient number of calculations, varying uncertain input parameters. In the latter approach, overall uncertainty in outputs is evaluated based on comparison between the outputs (calculation results) and experimental data.

6.26. For the 'propagation of input uncertainties' approach, the uncertain input parameters that are varied should include at least the most significant ones. Ranges should be assigned to the values of selected input parameters and the probability distributions within those ranges specified based on data from relevant experiments, measurements of parameters, records of plant operational parameters, or other appropriate sources. If this is not feasible, conservative values from the range should be used. Either the selected input parameters should be independent of each other or dependencies between uncertain input parameters should be identified and quantified; specific processing of these results should be applied.

6.27. The selection of uncertain input parameters to be varied, and the ranges and probability distributions used, are crucial for the reliability of results, since they strongly affect 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 also allow ranking of the uncertain input parameters in accordance with their contribution to output uncertainty. Such ranking indicates which of the parameters should be given the greatest attention. However, it should be taken into account that regression or correlation techniques might also give unclear or misleading results, 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 also be estimated based on expert judgment with the assistance of "phenomena identification and ranking tables" for each event that is analysed. Each such table should identify the most important phenomena for which the suitability of the code has to be assured, based to the extent possible on available data. The important parameters should be varied randomly in accordance with their respective probability distributions to estimate 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 the selection of acceptance criteria, use of computer codes, suggested approaches for treatment of uncertainties and ensuring safety margins, as described in Sections 4, 5 and 6.

7.2. Deterministic safety analysis should also be conducted following more specific guidance regarding the objectives of the analysis, selection of acceptance criteria, consideration of availability of various plant systems, operator actions, treatment of uncertainties and other assumptions of the analysis for individual plant states, as described in this section. In deterministic safety analysis, credit should be only given to those structures, systems and components that meet the requirements associated with relevant plant states, with due consideration of their safety classification (see SSG-30 [20]).

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

(a) Code models;

(b) Plant operating parameters;

(c) Control and limitation systems;

(d) Active safety systems;

(e) Passive safety systems;

(f) Safety features for design extension conditions;

(g) Operator actions.

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

7.5. For many types of postulated accident, the important release of radionuclides would be from the reactor core into the reactor coolant system and subsequently into the containment. Evaluation of the source term should therefore include predicting the behaviour of the radionuclides through this route, until their release to the environment.

Specific objectives of the analysis

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

7.7. The limits and conditions used in deterministic safety analyses of normal operation, such as those of reactor power and coolant inventory, should include 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 configurations covered by operational limits and conditions should be analysed, with particular attention paid to associated transients such as changes in reactor power, reactor shutdown from power operation, reactor startup, reactor cooling down, mid-loop operation and handling of fresh and irradiated fuel, including offloading of irradiated fuel from the reactor to the spent fuel pool and loading of fuel into the core.

7.9. The deterministic safety analysis for normal operation should 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 workers at the plant, and to members of the public and non-human biota around the nuclear power plant. Owing to the complexity of radiological analysis, and in particular its strong dependence on the overall organization of the plant operation, the corresponding guidance is not provided in this Safety Guide (see for example GSG-10 [5]).

Acceptance criteria

7.10. The deterministic safety analysis should provide an assessment of 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 transients, as defined by the operational limits and conditions, and taking account of all operating modes. Transitions from one operational state to another, as anticipated in operational guidelines, should also be 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: predict the radiation doses likely to be received by workers and members of the public; assess that these doses are below dose limits (see Requirement 5 of SSR-2/1 (Rev. 1) [1]); and ensure that the principle that these doses should be as low as reasonably achievable has been

satisfied. However, compliance with 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 transients associated to normal operational modes.

Operator actions

7.13. Planned operator actions performed in accordance with normal operating procedures should be credited 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 system performance, including that of instrumentation and control and mechanical systems, should be considered in order to assess the adequacy of the available provisions.

7.15. The initial conditions considered should be representative of all expected and authorized plant modes, in accordance with the operational limits and conditions. Bounding values of parameters used should take into account the whole acceptable range of the parameters.

7.16. When there are uncertainties in making predictions of doses, conservative assumptions should be made. However, detailed guidance in this area 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 verify that the plant's 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 response of the plant to the initiating event that is realistic.

7.18. The anticipated operational occurrences category of postulated initiating events considered in the analysis should include all those that might be expected to occur during the lifetime of the plant. 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. In such cases, operation can resume after rectification of the fault.

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, if the plant control and limitation systems operate as intended, they will be capable of preventing the need for actuation of the safety systems. However, it is recognized that some anticipated operational occurrences themselves require the actuation of safety systems.

Acceptance criteria

7.20. The realistic analyses of anticipated operational occurrences should aim to demonstrate 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 to verify, 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 to demonstrate that specific design criteria, more stringent than acceptance criteria for conservative analysis of anticipated operational occurrences, 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 providing assurance (for light water reactors) that, with 95 % probability at 95 % confidence level, there will be no boiling crisis or dry out anywhere in the core, no fuel melting anywhere in the core, and pressure in the reactor coolant system and main steam system will not significantly (i.e. by more than 10–15%) exceed the design value.

7.23. There should be negligible radiological impact beyond the immediate vicinity of the plant from any anticipated operational occurrence. 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 analysis of anticipated operational occurrences, any system not affected by the postulated initiating event should be assumed to be 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 operating procedures for normal and abnormal operation should be credited 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 a best estimate methodology covering the anticipated initial conditions of the plant that are considered in the determination of postulated initiating events. Normally, uncertainties are not considered in realistic analysis of anticipated operational occurrences. For operational considerations (such as analysis of 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. Paragraph 5.26 of SSR-2/1 (Rev.1) [1] requires that "design basis accidents shall be analysed in a conservative manner." One of the conservative methods[15] (Option 1, 2 or 3 from Table 1) should therefore be used; realistic analysis should not be applied for design basis accidents. The conservative analysis of anticipated operational occurrences and design basis accidents should demonstrate that the safety systems alone in the short term, along with operator actions in the long term, are capable of achieving a safe state by fulfilling the following safety conditions:

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

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

(c) 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 applicable events 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

[15] The terms 'conservative methods' and 'conservative analysis' are to be understood to refer to any of Options 1, 2 and 3 from Table 1 and para. 2.14.

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 relating to fuel integrity and radiological acceptance criteria should, in principle, be the same as for realistic analysis of anticipated operational occurrences.

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

7.32. Specific technical acceptance criteria should be defined such that their fulfilment allow demonstration 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 technical acceptance criteria should typically include the following:

(a) An event should not generate a 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;

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

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

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

(e) The number of fuel cladding failures should be limited for each type of postulated initiating event to allow the global radiological criteria to be met and to limit the level of radiation to below that used for equipment qualification;

(f) 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;

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

(h) Subcriticality of nuclear fuel in the reactor after shutdown, in fresh fuel storage and in the spent fuel pool should be maintained. Temporary returns to criticality (e.g. steam line break in pressurized water reactor) may be acceptable for certain events and plant operating modes, provided that criteria for sufficient cooling of the fuel continue to be met;

(i) There should be no initiation of a brittle fracture or ductile failure from a postulated defect of the reactor pressure vessel during the plant design life for any postulated design basis accident;

(j) Internal reactor components should withstand dynamic loads during design basis accidents so that safe shutdown of the reactor, reactor subcriticality and sufficient reactor core cooling are maintained.

7.34. For postulated initiating events occurring when the integrity of any of the barriers is missing or degraded (such as situations with an open reactor, open containment or an 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 assumptions to be made in the analysis regarding the availability of plant systems should typically include the following:

(a) 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, continue to operate;

(b) Any control or limitation systems 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;

(c) 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) operate with conservative performance (see para. 7.42);

(d) 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 postulated in a system or component that leads to the greatest challenge to the safety systems;

(e) 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 until after a conservatively specified time. The timing assumed in analysis should be justified and validated for the specific reactor design; for example the minimum specified time may be 30 minutes for control room actions or 60 minutes for field actions.

7.38. The actions of the plant staff to prevent an accident or mitigate its consequences by taking correct actions should only be taken into account in the analysis if it can be shown that the event sequence and the plant specific boundary conditions allow for carrying out the assumed actions. The conditions to be considered include the overall context in which the event sequence takes place, the working environment in the control places, written procedures, and the relevant staff's training status and access to necessary information.

7.39. In accordance with the practice in some States, an additional operator error during performance 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, in the 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 state. The aim is to demonstrate with a high level of confidence that there are significant margins to the safety limits.

7.41. Conservative analysis of anticipated operational occurrences should include the same conservative assumptions as used for the deterministic analysis of design basis accidents, especially those

assumptions that 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, whichever is conservative for a given acceptance criterion. For reactor trip and safety system actuation systems, it should be assumed that the initiating action occurs at the worst end of the possible range of conditions. 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 may be considered as additional conservative assumption. If such a loss is considered as an additional failure, it may be assumed to occur at a time that has the most negative effect for the barrier integrity; in this case 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 for anticipated operational occurrences and design basis accidents should take into account all significant physical processes occurring during an accident and use conservative 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 any cliff edge effects.

Acceptance criteria

7.46. Acceptance criteria for design extension conditions should meet the requirement established in para. 5.31A of SSR-2/1 (Rev. 1) [1], namely: “The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures.”. The same or similar technical and radiological criteria as those for design basis accidents may be considered for these conditions to the extent practicable. Radioactive releases should be minimized as far as reasonably achievable.

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 and 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 may not need to be considered.

7.50. To ensure independence 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. This is because:

(a) One given sequence is potentially intended to cover several kinds of postulated initiating event, and it may be difficult to demonstrate that the operational system is always available considering both the origin of the postulated initiating event and the multiple failures;

(b) 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 in demonstrating the adequacy of the nuclear power plant design. Such equipment is typically considered to operate for long-term sequences and is assumed to be 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 may 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.

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

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 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 combined approach or the best estimate approach with quantification of uncertainties (best estimate plus uncertainty), as applicable for design basis accidents, may be used. However, in line with the general rules for analysis of design extension conditions, best estimate analysis without a quantification of uncertainties may also be used, subject to consideration of the caveats and conditions indicated in paras 7.55 and 7.67.

7.55. When best estimate analysis is performed, margins to avoid cliff edge effects should be demonstrated to be adequate. This may be done, for example by means of sensitivity analysis demonstrating, to the extent practicable, that when more conservative assumptions are made 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:

(a) The plant can be brought into a state where the containment functions can be maintained in the long term;

(b) The plant structures, systems and components (e.g. the containment) and procedures are capable of preventing a large radioactive release or an early radioactive release, including containment bypass;

(c) Control locations remain habitable to allow performance of required staff actions;

(d) 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 to members of the public (or releases to the environment) used for analysis of severe accidents should represent levels such that only off-site

protective actions that are limited in terms of lengths of time and areas of application are necessary, and that there is sufficient time for their implementation early enough for them to be effective.

7.59. Technical acceptance criteria should represent conditions such that containment integrity is maintained. Examples of acceptance criteria for analysis of design extension conditions include limitation of the containment pressure, containment water level, temperature and flammable gas concentrations 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 them. In particular, the radiation levels (e.g. ambient 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, consistent with Requirements 11 and 24 of 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:

(a) Their failure is not part of any scenario that the severe accident sequence is meant to cover;

(b) This equipment will survive realistic severe accident conditions for the period that is necessary to perform its intended function.

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

(a) The circumstances of the applicable initiating event, including those resulting from external hazards (e.g. station blackout, earthquakes);

(b) The environment (e.g. pressure, temperature, radiation) and time period for which the equipment is needed.

7.63. For design extension conditions with core melting, the 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 in the deterministic safety analysis. Appropriate rules should be defined for testing and maintenance of systems or components necessary for design extension conditions to ensure their availability.

7.64. Non-permanent equipment should not be considered in demonstrating the adequacy of the nuclear power plant design. For some design extension conditions such equipment is typically considered to operate for long-term sequences and is assumed to be 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

7.65. The same assumptions regarding operator actions should be considered as for design extension conditions with core melting as for those 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 thermohydraulic 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:

(a) Core degradation processes and fuel melting;

(b) Fuel–coolant interactions (including steam explosions);

(c) In-vessel melt retention;

(d) Vessel melt-through;

(e) Direct containment heating;

(f) Distribution of heat within the primary circuit;

(g) Generation, control, and combustion of hydrogen;

(h) Failure or bypass of the containment;

(i) Corium–concrete interaction;

(j) Release and transport of fission products, including venting to prevent overpressure in the containment;

(k) Ability to cool in-vessel core melt and ex-vessel core melt.

7.67. Analysis of severe accidents should be performed using a realistic approach (Option 4 in Table 1) to the extent practicable. Since explicit quantification of uncertainties may be impractical due to the complexity of 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 CONDITIONS ARISING THAT COULD LEAD AN EARLY RADIOACTIVE RELEASE OR A LARGE RADIOACTIVE RELEASE

7.68. Paragraph 5.31 of SSR-2/1 (Rev. 1) [1] states that: "The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'." The regulatory body may establish more specific rules describing acceptable ways to demonstrate 'practical elimination'.

7.69. The demonstration of 'practical elimination' of the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release include deterministic considerations, and engineering aspects such as design, fabrication, testing and inspection of structures, systems and components and evaluation of operating experience, 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 conditions arising that could lead to an early radioactive release or a large radioactive release should include, where appropriate, the following steps:

(a) Identification of conditions that potentially endanger the integrity of the containment or allow bypassing of the containment, resulting in an early radioactive release or a large radioactive release;

(b) Implementation of design and operational provisions in order to 'practically eliminate' the possibility of those conditions arising. The design of these provisions should include sufficient margins to cope with uncertainties;

(c) Final confirmation of the adequacy of the provisions by deterministic safety analysis, complemented by probabilistic safety assessment and engineering judgement.

7.71. Although probabilistic targets can be set, demonstration of the 'practical elimination' of conditions arising that could lead to an early radioactive release or a large radioactive release should not be based solely on low probability values. Such event sequences should be deterministically defined and their 'practical elimination' should be demonstrated based on the performance of safety features making the event 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 — control of reactivity, removal of heat and confinement of radioactive material, including limitation of accidental radioactive releases (see Requirement 4 of SSR-2/1 (Rev. 1) [1]) — will be achieved. In practice this approach is limited to very specific cases. An

example of its use may be for uncontrolled reactivity accidents for which the main protection is provided by ensuring a negative reactivity coefficient with all possible combinations of the reactor power and coolant pressure and temperature.

8. DOCUMENTATION, REVIEW AND UPDATING OF DETERMINISTIC SAFETY ANALYSIS

DOCUMENTATION

8.1. Paragraph 4.62 of 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." Paragraph 4.64 of GSR Part 4 (Rev. 1) [2] states that: "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. While the safety report itself should be sufficiently comprehensive for these purposes, typically there are other documents, which may include description and results of the deterministic safety analysis, that are used as supporting information to independent verification or regulatory review. Similar rules to those for the safety report should apply to all documentation of deterministic safety analysis intended for submission 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 in accordance with their frequencies and the specific challenges to the integrity of physical barriers against releases of radioactive material that are addressed. The selection of the bounding scenarios in each group should be justified. 'Practical elimination' of the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release should be demonstrated.

8.4. A set of the most important plant data used for the development of plant models (effectively the 'database for deterministic safety analysis'), and considered necessary for independent verification or evaluation of the deterministic safety analysis performed, should be provided 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, and should include relevant drawings and other graphical documentation. If these data are not sufficiently documented and justified in the safety report itself, other reliable data sources used for the preparation of the plant models should be clearly identified and referenced in the safety report.

8.5. A brief description of the computer codes used in the deterministic safety analysis should be provided. In addition to a reference to the specific code documentation, the description should include justification that the code is adequate for the given purpose and has been verified and validated by the user (see paras 5.14–5.39).

8.6. Depending on the phenomena modelled and other characteristics of each analysed scenario, a relevant acceptance criterion or set of criteria should be selected for each scenario and presented together with the safety analysis of that scenario, 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. Different approaches that may have been used for each plant state should be described (see Section 6).

8.8. If the deterministic analysis involves using different computer codes in sequence, the transfer of data between the different stages of accident analysis and/or computer codes used in the 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 covered by any scenario analysed and presented should extend up to the moment when the plant reaches a safe and stable end state (although not all sensitivity calculations need necessarily 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 documentation of the results of the deterministic safety analysis should be structured and presented in an appropriate format in such a way as to provide a clear description and interpretation of the course of the accident. A standardized format may be adopted for similar analyses to facilitate interpretation and intercomparison of the results.

8.11. The documentation of the results of the deterministic safety analysis should typically include the following information:

(a) A chronological description of the main events as they have been 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 the adequacy of margins;

(e) Results of sensitivity analyses, 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 parts of the safety analysis report can be found in DS449 [21].

Sensitive information in documentation

8.14. Sensitive information included in reports describing deterministic safety analysis the unauthorized disclosure of which could compromise 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. Such information should be protected in accordance with guidance on information security [6].

REVIEW AND UPDATING OF DETERMINISTIC SAFETY ANALYSIS

8.15. In accordance with the requirement established in para. 5.10 of GSR Part 4 (Rev. 1) [2], deterministic safety analysis used in the licensing process should be periodically updated to take into account 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 potentially significant effects on the results of the analysis.

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

8.17. In such cases, 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 judgement, 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 level of documentation commensurate with the extent of changes and the associated impacts.

9. INDEPENDENT VERIFICATION OF DETERMINISTIC SAFETY ANALYSIS BY THE LICENSEE

9.1. Requirement 21 of GSR Part 4 (Rev. 1) [2] states that: “The operating organization shall carry out an independent verification of the safety assessment before it is used by the operating organization or

submitted to the regulatory body." The objective and scope of such independent verification are further described in paras 4.66–4.71 of GSR Part 4 (Rev. 1) [2].

9.2. The main purpose of the independent verification of safety analysis by the licensee (the operating organization) is to confirm that the safety analysis, and particularly parts developed by other groups or organizations 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 met, in accordance with the licensee's prime responsibility for safety.

9.3. Among the responsibilities set out in para. 3.6 of the Fundamental Safety Principles [22], the licensee is responsible for "Verifying appropriate design and the adequate quality of facilities and activities and of their associated equipment". The adequacy of the design should be demonstrated by means of safety assessment.

9.4. Paragraph 4.13 of GSR Part 4 (Rev. 1) [2] makes clear that safety analysis is an essential component of safety assessment. The relevant requirements of GSR Part 4 (Rev. 1) therefore apply fully to deterministic safety analysis performed 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 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 para. 4.67 of GSR Part 4 (Rev. 1) [2], the operating organization should ensure that independent verification of the deterministic safety analysis is performed by suitably qualified and experienced individuals or a group different from those who carried 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 the work are delegated 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 organization or other closely associated organization. Use of a fully independent organization should be the preferred solution.

9.8. The group performing the independent verification may take into account any quality assurance 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 using 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, focusing on the most significant safety issues and requirements rather than all of them. “The decisions made on the scope and level of detail of the independent verification shall be reviewed in the independent verification itself” (GSR Part 4 (Rev. 1), para. 4.68 [2]).

9.11. While the verification may be conveniently subdivided into phases that are performed at different 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 the safety analysis originally performed by the design organization. The same approach should, however, be applied to other subsequent verification activities.

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

(a) Comparison with requirements of the law, regulations or other legal requirements;

(b) Comparison with guidance from the regulatory body;

(c) Comparison with IAEA safety standards or guidance;

(d) Comparison with similar projects;

(e) Use of general experience from previous projects;

(f) Independent verification calculations.

9.14. The reliability of all numerical models used in safety analysis should be shown 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 para. 4.69 of GSR Part 4 (Rev.1) [2], the independent verification should consist of two main parts: an overall (qualitative) review focused on the quality and comprehensiveness of the safety analysis, and specific detailed reviews of important aspects of the analysis, which may include comparison of results of submitted analyses with the results of new, independent calculations. The components of verification should include, as appropriate, the following:

(a) Compliance with the requirements of reference documents (see para. 9.13);

(b) Completeness of the documentation;

(c) Correctness of input data;

(d) Selection of initiating events or accident scenarios;

(e) Selection of acceptance criteria;

(f) Selection of the safety analysis method;

(g) Selection of safety analysis computer codes and adequacy of code validation;

(h) Selection of assumptions for ensuring safety margins;

(i) Adequacy of description and evaluation of the analysis results.

9.16. An independent check of selected computer calculations should be conducted to verify that they are correct. If sufficient verification and validation of the original code have not been performed, then a different code should be used to verify the accuracy of the computer calculations. Use of different computer codes for independent verification is preferred, but use of the same codes may meet the objectives of the review if the plant models (including nodalization, initial and boundary conditions) are 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, typically the case with smallest margin to the acceptance criterion. However, it should be taken into account that independent calculation is a time and resource demanding task.

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

(a) The safety analysis was performed in accordance with relevant regulations, safety standards and other relevant guidance;

(b) The selected postulated initiating events or accident scenarios reflect specific features of the given design and bound the other cases;

(c) The combination of individual events and identification of consequential failures was done adequately;

(d) The computer codes used in safety analysis have been adequately verified and validated for the given application;

(e) The computational models reflect experience and applicable guidance for their development and are appropriate for reliable prediction of operational states and accident conditions;

(f) The assumptions and data used in each analysis have been specified in an adequate way to demonstrate that the relevant acceptance criteria have been met and there are sufficient margins to prevent cliff edge effects;

(g) Adequate sensitivity calculations or uncertainty evaluations are available in order to assure that the demonstration of safety by safety analysis is sufficiently robust;

(h) Consideration of the operability of plant systems in different plant states was in accordance with established rules for deterministic safety analysis and consistent with industrial standards;

(i) Compliance with the relevant acceptance criteria was achieved either by means of automatic systems, or personnel actions were assumed only in cases where contextual boundary conditions for diagnosis, decision and performing the required action were available;

(j) Independent calculations are in reasonable qualitative and quantitative agreement with the original analysis, and both demonstrate that relevant acceptance criteria are met;

(k) Any discrepancies found in the safety analysis are clearly understood and explained and do not call into 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 the scope, level of detail and methodology of the verification, and the 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 databases centrally to ensure that the same information is used by all assessors, authors and reviewers.

9.21. In relation to the sharing of plant data, information on models and other know-how between assessors, authors and reviewers, proprietary rights should be addressed through 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] INTERNATIONAL ATOMIC ENERGY AGENCY, 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, IAEA Safety Standards Series No. GSG-10, IAEA, Vienna (in preparation).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, Implementing Guide, 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 Reports 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, IAEA, 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*).* (A revision of this publication is in preparation.)

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

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

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

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

[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 I. APPLICATION OF DETERMINISTIC SAFETY ANALYSIS

AREAS OF APPLICATION

I–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.

I–2. Deterministic safety analysis associated with the design and authorization (licensing) of a nuclear power plant (items (a)–(e) in the above list) 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)–(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

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

I–4. Main components of the design requirements determined by deterministic safety analysis typically include: equipment sizing; capacity; set point values for parameters regarding initiation, termination and

control of systems; and working (environmental) conditions. These ensure effective operation of the systems in all relevant plant states and provide for adequate operating margins. The analysis also includes assessment of radiological effects for all plant states to ensure that there is confidence in the future authorization of the plant.

I–5. The designer typically uses the safety analysis as an integral part of the design process, which typically consists of several iterations that may continue through the manufacture and construction of the plant. The safety analysis used in the design is performed in accordance with a quality assurance programme.

I–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.

I–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 to facilitate 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 text.

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

I–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.

I–9. On the basis of this analysis for licensing, the robustness of the design in performing safety functions during all operational modes 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.

I–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 text.

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

I–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 [I–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

I–12. New deterministic safety analyses may be necessary 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 due to ageing over the period under consideration.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO PLANT MODIFICATIONS

I–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 structures, systems or components, changes in plant parameters, changes in plant configuration or changes in operating procedures.

I–14. Plant modifications are often aimed at 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 mean that the safety margins to operating limits are reduced and special care is taken to ensure that the limits are not exceeded.

I–15. Deterministic safety analyses are typically performed to support plant modifications. The scope of such 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.

I–16. Changes that require significant plant modifications such as power uprating and achieving higher burnup, 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 several changes are implemented at the same time.

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

I–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 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.

I–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 selected parameters, may be performed.

I–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

I–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 t 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.

I–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. Validation of emergency operating procedures is also performed. This validation is usually performed 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

I–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 using one or more of the specialized computer codes that are available to model relevant physical phenomena.

I–23. The analyses are used to identify the challenges to the integrity of the barriers or alternative pathways for their bypass that can be expected during the progression of accidents and the phenomena that will occur. They are used to provide the basis for developing a set of guidelines for managing accidents and mitigating their consequences.

I–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; or 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.

I–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 melting. 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; recombination of combustible gases; and filtered containment venting [I–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. For reactors of other designs, consideration is given to the mitigatory measures applicable to the design.

I–26. Transition from the emergency operating procedures to the severe accident management guidelines, if they are separate, needs 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 AND LEVEL 2 PSA

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

I–28. Deterministic safety analysis has an important role in support of the probabilistic safety assessment by determining ‘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. The aim of such studies supporting probabilistic safety assessment is to identify, for various combinations of equipment failures and human errors, a minimum set of safety features that can prevent nuclear fuel degradation. The deterministic analysis is performed in a realistic way although uncertainties are quantified where it is necessary.

I–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 FOR ANNEX I

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

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

[I–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). (A revision of this publication is in preparation.)

ANNEX II. FREQUENCY RANGES OF ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENT CATEGORIES

II–1. Possible anticipated operational occurrences and design basis accident categories used in some States for new reactors are indicated in Table II–1.

TABLE II–1. EXAMPLE OF ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENT CATEGORIES USED IN SOME STATES

Plant state	Alternative names used in some States[1]	Indicative frequency (f) range ($year^{-1}$) [2]
Anticipated operational occurrences	Faults of moderate frequency, DBC-2, PC-2	$f > 10^{-2}$
Design basis accidents	Infrequent faults, DBC-3, PC-3	$10^{-2} > f > 10^{-4}$
	Limiting faults, DBC-4, PC-4	$10^{-4} > f > 10^{-6}$

[1] DBC stands for ‘design basis condition’; PC stands for ‘plant condition’. The designations DBC-1 and PC-1 are used for normal operation.

[2] Some other accidents for which the frequency is lower than 10^{-6} need to be considered because they are representative of a type of risk the reactor has to be protected from.

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 Regulation Authority, Japan
Ramon, J.	Nuclear Safety Council, Spain
Spitzer, C.	International Atomic Energy Agency
Steinrötter, T.	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) GmbH, Germany
Villalibre, P.	International Atomic Energy Agency (TO)
Virtanen, E.	Radiation and Nuclear Safety Authority, Finland
Yllera, J.	International Atomic Energy Agency