Version: 20 April 2016

IAEA SAFETY STANDARDS

for protecting people and the environment

Step 7

Preparing draft publication

Deterministic Safety Analysis for Nuclear Power Plants. (SSG-2 Rev. 1)

DS491

DRAFT Revised SAFETY GUIDE

CONTENTS

1. INTRODUCTION

BACKGROUND

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

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

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

OBJECTIVE

1.4. The objective of this Safety Guide is to provide recommendations and guidance on performing deterministic safety analysis for designers, operators, regulators and technical support organizations. It also provides recommendations on the use of deterministic safety analysis in:

(a) Demonstrating or assessing compliance with regulatory requirements;

(b) Identifying possible enhancements of safety and reliability;

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

SCOPE

1.5. This Safety Guide applies to nuclear power plants. It addresses the ways for performing deterministic safety analyses that are required to demonstrate adequate fulfilment of safety functions in order to ensure that barriers to the release of radioactive material will prevent an uncontrolled

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

release to the environment for all plant states. Deterministic safety analyses are required to determine the characteristics of the releases (source term) depending on the status of the barriers for different plant states.

1.6. This Safety Guide focuses primarily on the deterministic safety analysis for the design safety of new nuclear power plants and, as far as reasonably practicable or achievable, also the safety re-evaluation or assessment of existing nuclear power plants when operating organizations review their safety assessment. The guidance provided is intended to be as much as possible technology neutral, although it is particularly based on experience with deterministic safety analysis for water cooled reactors.

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

1.8. This Safety Guide deals with those failures in the reactor core, reactor coolant system (RCS), fuel storage, systems containing radioactive substances or any other system that affect performance of safety functions potentially leading to loss of physical barriers against releases of radioactive substances. Analysis of hazards, either internal or external (natural or human induced) is not covered by this Guide, although the loads potentially inducing the failures in plant systems are taken into account in determining initiating events to be analysed.

1.9. This Safety Guide is devoted to the deterministic safety analysis for design or licensing purposes, which are aimed at demonstration of compliance with acceptance criteria with adequate margins. However, computer codes used for deterministic safety analysis as analytical tools have broader range of applications.

1.10. This Safety Guide addresses both conservative and realistic deterministic safety analysis.

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

1.12. Radiological analysis in this Safety Guide includes transport of radioactive substances inside the nuclear power plant, in particular in anticipated operational occurrences and accident conditions, as one of the inputs for determining the radiation doses to the nuclear power plant staff (see GSR Part 3) [4]). It is however recognized that minimization of the staff exposures and keeping the doses ALARA is a much more complex issue of radiation protection, which primarily includes such measures as minimization of radiation sources, appropriate nuclear power plant configuration, shielding and ventilation design, limitation of staff exposure time and monitoring of staff exposure, etc. Determination of the doses to the nuclear power plant staff is therefore not covered by this Safety Guide.

1.13. This Safety Guide also covers radiological aspects associated with different plant states with potential releases of radioactive substances to the environment as the source term evaluation for determining radiation doses to the public. However, these aspects are only covered up to the determination of the source term to the environment for anticipated operational occurrences and accident conditions. Radioactive gaseous and liquid effluents and discharges during normal operation are primarily controlled by operational measures and are not covered by this Guide. Similarly, dispersion of radioactive substances in the environment and prediction of the radiological effects on population and non-human biota is outside the scope of this Safety Guide. While general rules for deterministic safety analysis apply also to 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 Guide, for example in [5].

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

INTERFACE BETWEEN SAFETY AND SECURITY REGARDING DETERMINISTIC SAFETY ANALYSIS

1.15. Recommendations about Security are out of the scope of this Safety Guide. From this point of view it can be noted that documentation and electronic records related to deterministic safety analysis process and outputs provide, in general, limited information regarding equipment location and susceptibility and practically no information on cable routes and other aspects of the plant layout. However, both documentation and electronic records include sensitive information about initiating events and their combinations or safety limits. According to that, deterministic safety analysis can provide valuable insights regarding the identification of plant items having relevance for security considerations and information for the identification of vital areas; see NSS 4 [6], NSS 13 [7], NSS 16 [8] and NSS 17 [9].

STRUCTURE

1.16. Besides this introduction, this Safety Guide consists of nine additional sections and one annex. Section 2 introduces some basic concepts and terminology used in the area of deterministic safety analysis. It includes general statements necessary as basis to provide specific guidance by other sections of this Safety Guide. Section 3 describes methods of systematic identification, categorization and grouping of initiating events and accident scenarios to be addressed by deterministic safety analysis. The section includes practical advice on selection of events to be analysed for the different plant states. 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 DBAs. The guidance provided covers conservative and best estimate approaches for addressing uncertainties and for ensuring adequate margins in safety analysis. Section 7 provides specific guidance on performing deterministic safety analysis for each individual plant state. Section 8 includes guidance on documentation, review and update of deterministic safety analysis. Section 9 provides guidance for independent verification of safety assessment, including verification of deterministic safety analysis. The Annex indicates additional applications of the computer codes used for deterministic safety analysis, besides the nuclear power plant design and authorization. Some terms and explanations for consideration in the preparation or revision of safety standards and so for possible inclusion in the IAEA Safety Glossary are provided at the end, under Definitions.

2. GENERAL CONSIDERATIONS

OBJECTIVES OF DETERMINISTIC SAFETY ANALYSIS

2.1. The objective of deterministic safety analysis for nuclear power plants is to confirm that plant systems, in combination where relevant with operator actions, are capable and sufficient, with adequate safety margins, to keep the radiological releases from the plant under acceptable limits. Deterministic safety analysis is aimed to demonstrate that barriers to the release of radioactive material from the plant will maintain their integrity to the extent required. Deterministic safety analysis, supplemented by a number of investigations such as those related to fabrication, testing, inspection, evaluation of the operating experience and by PSA, is also aimed to contribute to demonstrate that the source term and eventually radiological consequences of different plant states are acceptable and that early or large releases are practically eliminated.

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

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

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

ACCEPTANCE CRITERIA FOR DETERMINISTIC SAFETY ANALYSIS

2.5. The acceptance criteria can be expressed either in general, qualitative terms or as quantitative limits. Three categories of criteria can be recognized: (a) design criteria: design limits for individual systems, structures and components, which are part of the design basis as important preconditions for meeting criteria in the two following categories; (b) operational criteria: these are rules to be followed by operator during normal operation and anticipated operational occurrences, they need to be consistent with design criteria and provide preconditions for meeting safety criteria; (c) safety criteria: these are criteria either directly related to the consequences of operational states or accident conditions or to the integrity of barriers against releases of radioactive materials.

2.6. In this Safety Guide only the safety criteria are used in connection with the deterministic safety analysis and the wording acceptance criteria then refers to safety criteria.

UNCERTAINTY ANALYSIS IN DETERMINISTIC SAFETY ANALYSIS

2.7. Several methods for performing uncertainty analysis have been published (e.g. in Safety Report Series No. 52 [10] para 6.21-6.29 and 7.43). They include:

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

(b) Use of scaled experimental data;

(c) Use of bounding scenario calculations.

CONSERVATIVE AND BEST ESTIMATE APPROACHES TO DETERMINISTIC SAFETY ANALYSIS

2.8. Table 2 lists different options currently available for performing deterministic safety analyses, with different levels of conservatism associated with the computer code, availability of systems and initial and boundary conditions for the analysis.

Table 2. Options for performing deterministic safety analysis

Option number and title	**Computer code type**	**Assumptions on systems availability**	**Type of initial and boundary conditions**
1. Conservative	Conservative	Conservative	Conservative
2. Combined	Best estimate	Conservative	Conservative
3. Best estimate + uncertainty (BEPU)	Best estimate	Conservative	Best estimate; partly most unfavourable conditions
4. Realistic	Best estimate	Best estimate	Best estimate

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

2.10. At present, experimental research has resulted in a significant increase of knowledge and the development of computer codes has improved the ability to achieve calculated results that correspond more accurately to experimental results. Due to the improved capabilities of computer codes and the possible drawbacks of the conservative approach (potential masking of important phenomena, counter effects of various parameters) option 1 is rarely used now and not suggested for current safety analysis unless situations when scientific knowledge and experimental support is limited. Option 1 remains also in legacy analysis.

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

2.12. Option 3 is so called best estimate plus uncertainty (BEPU) approach which allows the use of a best estimate computer code together with more realistic, that means best estimate and partially most unfavourable, initial and boundary conditions. However, in order to ensure the conservatism required in analysis of DBAs the uncertainties need to be identified, quantified and statistically combined. Availability of systems is usually assumed in a conservative way. Option 3 contains a certain level of conservatism and is at present accepted for some DBA and conservative anticipated operational occurrences analyses (e.g. para 6.21). Option 3 requires sound justification of the ranges and probability distributions of parameters that are applied.

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

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

2.15. Option 4 allows the use of best estimate modelling, as well as use of best estimate values for parameters and initial conditions. Option 4 may be appropriate for realistic analysis of anticipated operational occurrences aimed at assessment of control system capability and in general for best estimate design extension conditions analysis (see paras 7.17 and 7.54). More detailed information regarding modelling assumptions applicable for different options is provided in section 8 of this Safety Guide.

SOURCE TERM TO THE ENVIRONMENT

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

2.17. To evaluate the source term from a nuclear installation, it is necessary to identify the sources of radiation, to evaluate the inventories of radionuclides that are produced and to know the mechanisms of transmission of radioactive material from the source through the installation and released to the environment.

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

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

(b) To support by means of its quantification the demonstration that early or large releases can be considered as 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[2] that are required to protect human life, health, property and the environment in case of an emergency at the nuclear power plant;

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

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

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

MANAGEMENT SYSTEM

3.1. The performance and use of deterministic safety analysis should be conducted taking into account the recommendations of GS-G-3.1 [15] and GS-G-3.5 [16] to meet the requirements 1 to 3 of SS-R 2/1 (Rev.1) [1] and GSR Part 2 requirements-[17].

3.2. The plant states considered in the deterministic safety analysis should cover:

(a) Normal operation;

[2] 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) [11] and recommendations are provided in GS-G-2.1 (Arrangements for Preparedness for a Nuclear or Radiological Emergency, 2007) [12] and GSG-2 (Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, 2011) [13].

(b) Anticipated operational occurrences;

(c) DBAs;

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

3.3. The deterministic safety analysis should consider the postulated initiating events (PIEs) originated in any part of the plant requesting the actuation of the control and limitation systems[3] as well as the safety functions and potentially leading to a radioactive release to the environment in case of failures. This includes events that can lead to a release of radioactivity not only from the reactor core but from other relevant sources such as fuel elements stored at the plant and systems dealing with radioactive materials.

3.4. Where applicable, interactions between all reactors, spent fuel storages and any other sources of potential radioactive releases on the given site should be taken into account (SSR 2/1, § 5.32) [1].

3.5. The deterministic safety analysis should be performed for PIEs that can occur in all planned modes of the plant during normal operation at full power and low power, including operation during shutdown.

3.6. Every configuration of shutdown modes including refuelling and maintenance should be considered. For these modes of operation, contributors potentially increasing risk should be considered, such as the inability to start some safety systems automatically or manually; disabled automation systems; equipment in maintenance or in repair; reduced amounts of coolant in the primary circuit as well as in the secondary circuit for some modes; instrumentation switched off or non-functional and measurements not made; open primary circuit and open containment.

3.7. For PIEs initiated in the spent fuel pool, specific operating modes related to fuel handling (e.g. emergency core unloading) should be also considered.

3.8. PIEs potentially taking place during plant operating modes with negligible duration in time may not be considered after careful analysis and assessment of the potential contribution to early or large releases.

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 conditions such as:

[3] 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

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

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

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

(d) Reactor shutdown from power operation;

(e) Hot shutdown;

(f) Cooling down process;

(g) Refuelling during normal operation at power, where applicable;

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

(i) Normal operation of the spent fuel pool;

(j) Storage and handling of fresh fuel.

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

POSTULATED INITIATING EVENTS

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

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

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

3.14. The set of PIEs should be comprehensive and should be defined in such a way that covers all credible failures, including:

- failures of structures, systems and components of the plant (partial failure if relevant), including possible spurious actuation,

- failures initiated by operator errors, this could range from faulty or incomplete maintenance operations to incorrect settings of control equipment limits or wrong operator actions,
- failures of structures, systems and components of the plant arising from internal and external hazards.

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

— If the initiating event is a failure of part of an electrical distribution system, the DBA or design extension conditions analysis should assume the unavailability of all the equipment powered from that part of the distribution system.

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

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

3.16. Additional failures are assumed in deterministic safety analysis for conservatism (eg. single failure criteria) or DiD purpose (eg. common cause failure). Distinction should be made between these additional failures and failures that are part of, or directly caused by, the PIE. Further failures may be added to bound a set of similar events, limiting the number of analyses.

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

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

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

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

- Comparison with the list of PIEs developed for safety analysis of similar plants (ensuring that prior flaws or deficiencies are not propagated);
- Analysis of operating experience data for similar plants;
- Use of PSA insights and results.

3.20. Certain limiting faults (e.g. large break loss of coolant accidents, secondary pipe breaks, control rod ejection in pressurized water reactors or rod drop in boiling water reactors) traditionally considered in deterministic safety analysis as DBAs should not be excluded from this category of accidents without careful analysis and assessment of the potential impact on early or large releases.

3.21. Failures occurring in the supporting systems that impede the operation of systems necessary for normal operation should be also considered PIEs if such failures eventually require the actuation of the reactor protection systems.

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

IDENTIFICATION OF PIES FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DBAS

3.23. All PIEs should be subdivided into representative groups of event sequences taking into account the expected frequency of occurrence and its effect on the nuclear power plant. This approach allows the selection of the same acceptance criteria and/or initial conditions in each group, applying the same assumptions/methodologies, and identification of the worst accident (bounding case) in each group.

3.24. The postulated initiating events associated with anticipated operational occurrences and DBAs should reflect specifics of the design, but typically should belong to the following types of transients:

- Increase or decrease of the heat removal from the RCS;
- Increase or decrease of the RCS flow rate;
- Anomalies in reactivity and power distribution in the reactor core or in the fresh or spent fuel storage;
- Increase or decrease of the reactor coolant inventory;
- Leaks in RCS with potential containment by-pass;
- Reduction or loss of cooling of the fuel in the spent fuel storage pool;
- Release of radioactive material from a subsystem or component (typically from treatment or storage systems for radioactive waste).

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

3.26. Within each type of PIE, the transients should also be subdivided into categories depending on the frequency of the PIE. Possible anticipated operational occurrences and DBA categories are the following:

Plant state	**Alternative names used in some Member States**	**Indicative frequency range (year^{-1})**
AOO	Faults of Moderate Frequency, DBC-2, PC-2	1E-2 <
DBA	Infrequent Faults, DBC-3, PC-3	1E-4 < f < 1E-2
	Limiting Faults, DBC-4, PC-4	1E-6 < f < 1E-4

3.27. Typical examples of PIEs categorised as anticipated operational occurrences could include those given below. This list is broadly indicative. The actual list will depend on the type of reactor and the actual design:

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

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

—Decrease in RCS flow rate: trip of one main coolant pump; inadvertent isolation of one main coolant system loop (if applicable).

—Reactivity and power distribution anomalies: inadvertent control rod withdrawal; boron dilution due to a malfunction in the chemical and volume control system (for a PWR); wrong positioning of a fuel assembly.

—Increase in reactor coolant inventory: malfunctions of the chemical and volume control system; excessive feedwater flow in BWRs.

—Decrease in reactor coolant inventory: very small loss of coolant accident (LOCA) due to the failure of an instrument line.

— Failures of systems ensuring normal operation of fuel pools: loss of off-site power; malfunctions in decay heat removal system; leaking of pool coolant; malfunctions of the ventilation system.

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

3.28. The subset of PIEs which are considered as leading to DBAs should be identified. All PIEs identified as initiators of anticipated operational occurrences should also be considered as potential initiators for DBAs. Although it is not usual to include PIEs with a very low frequency of occurrence, the establishment of any threshold limit should consider the safety targets established for the specific reactor.

3.29. Typical examples of PIEs leading to DBAs should include those given below. This list is broadly indicative. The actual list will depend on the type of reactor and actual design:

—Increase in reactor heat removal: steam line breaks.

—Decrease in reactor heat removal: feedwater line breaks.

—Decrease in RCS flow rate: main coolant pump seizure or shaft break.

—Reactivity and power distribution anomalies: uncontrolled control rod withdrawal; control rod ejection; boron dilution due to the startup of an inactive loop (for a PWR).

—Increase in reactor coolant inventory: inadvertent operation of emergency core cooling.

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

—Sudden loss of heat removal from irradiated fuel in the fuel pools: a break of piping connected to the water in the pool.

—Release of radioactive material 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.

3.30. Groups of PIE should be further subdivided according the mechanisms affecting the performance of the safety functions and integrity of the physical barriers. Special groups of sequences can be thus formed with focus on reduced core cooling and RCS pressurization, containment pressurization, radiological consequences, or pressurized thermal shocks.

3.31. Probabilistic analysis should be used as a support to justify the categorization of PIE according to their frequency of occurrence. It should especially be checked that a transient with potential effects on integrity of barriers has a category consistent with the possible damages on the barriers.

3.32. A reasonable number of limiting cases, which are referred to as bounding or enveloping scenarios, should be selected from each category of events. These bounding or enveloping scenarios should be chosen so that they present the greatest possible challenge to the relevant acceptance criteria and are limiting for the performance parameters of safety related equipment. Note that a bounding scenario may combine or amplify the consequences of several PIEs in order to encompass all the possible PIEs grouped together. The safety analysis should confirm that the grouping and bounding of initiating events is acceptable.

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

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

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

(a) A reduction in or loss of cooling of the fuel in the spent fuel pool;

(b) Reactivity anomalies in the fresh or spent fuel;

(c) An accidental discharge from any of the other auxiliary systems that carry liquid or gaseous radioactive material;

(d) A failure in systems or components such as filters or delay tanks that are intended to reduce the level of discharges of radioactive material during normal operation.

(e) An accident during reload or maintenance where the reactor or containment might be open.

3.36. The frequency associated to a type of anticipated operational occurrences or DBA should combine the frequencies of all PIEs that have been grouped together.

GENERAL CONSIDERATIONS FOR IDENTIFICATION OF DESIGN EXTENSION CONDITIONS

3.37. In accordance with SSR-2/1 Rev. 1, Req. 20 [1], design extension conditions which are either more severe than DBA or that involve additional failures should be identified using engineering judgment, as well as deterministic and probabilistic assessment with the objective of identifying design provisions to prevent as far as possible such conditions or mitigate their consequences.

3.38. Two separate categories of design extension conditions should be identified, using different acceptance criteria and different rules for deterministic safety analysis: design extension conditions without significant fuel degradation and design extension conditions progressing into core melt, i.e. severe accidents[4].

IDENTIFICATION OF DESIGN EXTENSION CONDITIONS WITHOUT SIGNIFICANT FUEL DEGRADATION

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

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

- Initiating events that could lead to situations beyond the capability of safety systems that are designed for a single initiating event. A typical example is the multiple tube rupture in a steam generator of a PWR.
- Anticipated operational occurrences or DBAs 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 PIE. A typical example is a LOCA without actuation of the high pressure 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 occurrences or DBA (at least for the most frequent ones).
- Multiple failure PIEs that cause the loss of a safety system while this system is used to fulfil its function as part of normal operation. This applies to those designs that use, for example, the same system for the heat removal in accident conditions and during shutdown. The identification of these sequences should result from a systematic analysis of the effects on the plant of a total failure of any safety system used in normal operation.

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

- very low frequency initiating events typically not considered as DBA
  - uncontrolled level drop during mid-loop operation (PWR) or during refuelling

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

    - uncontrolled boron dilution (PWR)
    - multiple steam generator tube ruptures (PWR, PHWR)
    - main steam line break and induced steam generator tube ruptures (PWR, PHWR)
- anticipated operational occurrences or DBA combined with multiple failures on safety systems
    - anticipated transient without scram (ATWS): anticipated operational occurrences combined with the failure of rods to drop (does not apply to PHWRs)
    - station black out (SBO): loss of offsite power combined with the failure of the emergency diesel generators
    - total loss of feed water: loss of main feedwater combined with total loss of emergency feedwater
    - LOCA together with the complete loss of one type of emergency core cooling feature (either the high pressure or the low pressure part of the emergency core cooling system)
    - loss of required safety systems in the long term after a postulated initiating event
- multiple failure PIEs
    - total loss of the component cooling water system or of the essential service water system
    - total loss of core cooling in the residual heat removal mode
    - total loss of normal fuel pool cooling and potential subsequent loss of inventory
    - loss of normal access to the ultimate heat sink

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

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

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

IDENTIFICATION OF DESIGN EXTENSION CONDITIONS WITH CORE MELTING

3.45. A selection of specific sequences with core melting (severe accidents) should be made in order to establish the design basis for the safety features for mitigating core melt accidents, according to the plant safety objectives. These sequences should be selected in order to represent all main physical phenomena involved in core melt sequences.

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

3.47. The specific scenarios to be considered as well as the mitigation safety features are design dependent. Out of the representative sequences with core melt (design extension conditions with core melting), the enveloping one should be postulated to provide input to the design of the containment and of those safety features necessary to mitigate the consequences of such design extension conditions.

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

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

3.49. The low probability of occurrence of an accident with core melting is not sufficient reason for failing to protect the containment against the conditions generated by such accident. Core melt conditions should be postulated regardless of the provisions implemented in the design and some very energetic phenomena that may result from the core melt accident should be prevented (practically eliminated) to exclude containment failure.

3.50. Severe accident sequences should be selected to identify the most severe plant parameters resulting from the severe accident phenomena to be considered in the design of the plant structures, systems, and components.

IDENTIFICATION OF PIES DUE TO INTERNAL AND EXTERNAL HAZARDS

3.51. Determination of PIEs should consider events caused by relevant site specific internal and external hazards (SSR-2/1 Rev.1, Req. 17, § 5.15A-5.21A [1]. A list of examples external hazards can be found in NS-R-3 [14]. 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. The hazards themselves do not represent initiating events but they are associated with loads which can initiate such events.

3.52. In accordance with Ref. [SSR-2/1 Rev.1, § 5.15b, 5.19, and 5.63] in determination of PIEs caused by site specific hazards for multiple unit plant sites a possibility to impact several or even all units on the site simultaneously should be taken into account.

3.53 The analysis of hazards performed by using probabilistic methods or appropriate engineering methods should demonstrate that either:

- such hazard can be screened out due to its negligible contribution to risk, or
- the nuclear power plant design is robust enough to prevent any transition from the load into an initiating event, or
- the hazard causes an initiating event considered in the design, or
- the protection of plant equipment provides guaranties that the hazard will not result in an accident condition

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

EVENT SEQUENCES AND ACCIDENT SCENARIOS TO BE PRACTICALLY ELIMINATED

3.55. According ref. [SSR-2/1 Rev.1, § 2.13(4)], "The safety objective in the case of a severe accident is that only protective actions that are limited in terms of times and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that lead to early or large radioactive releases[5] are required to be practically eliminated[6]"

3.56. The event sequences requiring specific demonstration of their "practical elimination" should be classified as follows, if need be with a design specific adaption:

1) Events that could lead to prompt reactor core damage and consequent early containment failure:

   a. Failure of a large pressure-retaining component in the RCS

   b. Uncontrolled reactivity accidents

2) Severe accident phenomena which could lead to early containment failure:

   a. Direct containment heating

[5] SSR-2/1, Rev.1 [1] 'Large radioactive release': 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. 'Early radioactive release': radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time.

[6] SSR-2/1, Rev.1 [1] The possibility of certain conditions occurring is considered to have been 'practically eliminated' if it is physically impossible for the conditions to occur or if the conditions can be considered with a high level of confidence to be extremely unlikely to arise.

b. Large steam explosion

c. Hydrogen detonation

3) Severe accident phenomena which could lead to late containment failure:

a. Molten core concrete interaction (MCCI)

b. Loss of containment heat removal

4) Severe accident with containment bypass

5) Significant fuel degradation in a storage pool

3.57. Consequences of event sequences that have been ‘practically eliminated’ do not need themselves to be deterministically analysed. Nevertheless, severe accident management guidance for “not postulated scenario’ should be provided, but their ‘practical elimination’ should be demonstrated, including relevant deterministic analysis, as presented in paragraphs 7.68 to 7.72 of this Safety Guide.

4. ACCEPTANCE CRITERIA FOR DETERMINISTIC SAFETY ANALYSIS

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

4.2. The Safety Requirements SSR-2/1 (Rev.1), § 5.75 [1] state that the deterministic safety analysis among other objectives shall mainly provide “comparison of the results of the analysis with acceptance criteria, design limits, regulatory dose limits and acceptable doses”. Compliance with the deterministic 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, including severe accidents. These criteria should aim at limiting damage to barriers against the release of radioactive material in order to prevent unacceptable radiological releases. Selection of the criteria should ensure sufficient margin between the criterion and the physical limit for loss of integrity of a barrier against release of radioactive material.

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

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

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

—Detailed/derived technical criteria which relate to integrity of barriers (fuel matrix, fuel cladding, RCS pressure boundary, containment) against radioactive releases. They are typically proposed by the designer and subsequently approved by the regulatory body for use in the safety demonstration.

4.6. The radiological acceptance criteria should be expressed in terms of effective doses, equivalent doses or dose rates to nuclear power plant staff, general public or environment, including non-human biota. The doses are required to be within prescribed limits and as low as reasonably achievable in all plant states, SSR-2/1 (Rev.1), Req. 5 [1].

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

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

4.9. The radiological acceptance criteria for anticipated operational occurrences are typically comparable with annual dose limits for normal operation. They should be more restrictive than for DBAs since their frequencies are higher.

4.10. The radiological acceptance criteria for DBAs to be established should ensure that very restrictive dose limits, according to Req. 19 § 5.25 from SSR-2/1 (Rev.1) [1], are met.

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

4.12. Technical acceptance criteria should be set in terms of the variable or variables that govern the physical processes that challenge the integrity of a barrier. It is a common engineering practice to make use of surrogate variables to establish an acceptance criterion or combination of criteria that, if not exceeded, will ensure the integrity of the barrier. Examples of surrogate variables are: peak cladding temperature, departure from nucleate boiling ratio or fuel pellet enthalpy rise. When defining these acceptance criteria, a sufficient conservatism should be included to ensure that there are adequate safety margins to the loss of integrity of the barrier.

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

- Criteria related to integrity of nuclear fuel matrix: maximum fuel temperature, maximum radially averaged fuel enthalpy (both values with their dependence on burn-up and composition of fuel / additives like burnable absorbers)
- Criteria related to integrity of fuel cladding: minimum departure from nuclear boiling ratio, maximum cladding temperature, maximum local cladding oxidation
- Criteria related to integrity of the whole reactor core: adequate subcriticality, maximum production of hydrogen from oxidation of claddings, maximum damage of fuel elements in the core, maximum deformation of fuel assemblies (as required for cooling down, insertion of absorbers, and de-assembling)
- Criteria related to integrity of nuclear fuel located outside the reactor: adequate subcriticality and adequate heat removal
- Criteria related to integrity of the RCS: maximum coolant pressure, maximum temperature, pressure and temperature changes and resulting stresses-strains in the coolant system pressure boundary, no initiation of a brittle fracture or ductile failure from a postulated defect of the reactor pressure vessel
- Criteria related to integrity of the secondary circuit (if relevant): maximum coolant pressure, maximum temperature, pressure and temperature changes in the secondary circuit equipment
- Criteria related to integrity of the containment and limitation of releases to the environment: duration and value of maximum and minimum pressure, maximum pressure differences acting on containment walls, leakages, concentration of flammable/explosive gases, and acceptable working environment for operation of systems.

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

4.15. In particular, technical acceptance criteria related to integrity of barriers should be more restrictive for conditions with higher probability 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 DBA, and for design extension conditions without significant fuel degradation there should be no (or limited) consequential damage to the RCS, containment integrity should be preserved, and damage of the reactor fuel should be limited. For design extension conditions with core melting, containment integrity should also be maintained and containment by-pass prevented to ensure prevention of early or large releases.

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

4.17. Although the assessment of engineering aspects important to safety may not be explicitly addressed in the safety analysis, it constitutes a relevant part of the safety assessment. Safety margins applied to the SSCs design should be commensurate with the probability of the loads they have to bear.

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

5. USE OF COMPUTER CODES FOR DETERMINISTIC SAFETY ANALYSIS

BASIC RULES FOR SELECTION AND USE OF COMPUTER CODES

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

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

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

(b) The simplifying assumptions are justified

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

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

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

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

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

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

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

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

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

(d) Establishing sensitivities in important processes.

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

(a) Experimental data for the significant phenomena modelled. This would typically include a comparison against ‘separate effects’ (SET) and ‘integral effects’ (IET) experiments.

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

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

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

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

(a) The users have received adequate training and that they understand the code,

(b) The users are sufficiently experienced in the use of the code and fully understand its uses and limitations,

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

(d) The users follow the recommendation for use of the code and especially the ones relative to the application the user are carrying out the analysis

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

(a) The nodalization 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 match the ones chosen for SET and IET used for the qualification of the application

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

PROCESS MANAGEMENT IN CONNECTION WITH THE USE OF THE COMPUTER CODES

5.7. All activities that affect the quality of computer codes should be managed. This will require procedures that are specific to ensuring the quality of software. The appropriate software engineering practices that are applicable to the development and maintenance of software critical to safety should be applied. More specifically, formalized procedures and instructions should be put in place for the entire lifetime of the code, including code development, verification and validation, and a continued maintenance process with special attention to the reporting and correction of errors.

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

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

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

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

(b) Verification and validation activities and their documentation;

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

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

(e) Configuration management;

(f) Control of interfaces;

(g) Version control of the code

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

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

VERIFICATION OF COMPUTER CODES

5.13. Verification of the code should be performed to demonstrate that the code (source code and algorithm) conforms to the specifications. In general, the verification should ensure that the numerical methods, the transformation of the equations into a numerical scheme to provide solutions and user options with their restrictions are appropriately implemented in accordance with the specifications.

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

5.15. 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.

5.16. If the code is run on a hardware or software platform other than that the one on which the verification process was carried out, the continued validity of the code verification should be assessed.

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

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

VALIDATION OF COMPUTER CODES

5.19. Validation of the computer code should provide confidence in the ability of a code to predict, realistically or conservatively, the values of the safety parameter or parameters of interest. The level of confidence provided by the validation should be appropriate to the type of analysis; scope of validation might be relaxed for codes used in severe accident analysis, taking into account the limited relevant experimental data.

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

5.21. Validation of the code should be performed to assess the uncertainty of values predicted by the code. Outputs of the code are compared with relevant experimental data for important phenomena expected to occur.

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

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

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

(2) Separate effect tests. Separate effect tests address specific phenomena that may occur at a nuclear power plant but do not address other phenomena that may occur at the same time. Separate effect tests should ideally be performed at full scale. In the absence of analytical solutions or experimental data, sufficient conservatisms, based for example on code-to-code comparison or bounding engineering judgement, should be allowed to cover the deficiencies in the means to support a full validation.

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

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

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

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

5.26. For complex applications, a validation matrix should be developed for code validation, because a code may predict one set of test data with a high degree of accuracy but may be inaccurate for other data sets.

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

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

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

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

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

5.32. 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.

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

5.34. For a code intended to be conservative regarding certain acceptance criterion, it should be demonstrated that the code prediction bounds the experimental data.

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

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

QUALIFICATION OF INPUT DATA

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

DOCUMENTATION OF COMPUTER CODES

5.38. Each computer code needs to be adequately documented to facilitate review of the models and correlations employed and to ensure that the models for important phenomena are appropriate and are not applied outside their range of validity. The documentation would also provide a description of the uncertainties of important models and the overall code for typical applications. The code documentation would also include user guidelines and input descriptions to ensure that the user can use the code properly.

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

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

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

GENERAL CONSIDERATIONS

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

6.2. Uncertainties in computational predictions should be taken into account either implicitly by bounding them using conservative, combined or even best estimate approach, associated with sensitivity analysis as appropriate, or explicitly using best estimate approach with quantification of uncertainties. This is in particular important for the most limiting conditions (with the smallest margins to acceptance criteria).

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

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

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

6.6. When best estimate analysis is used, adequate margins to integrity of barriers should still be ensured. It should then be demonstrated by sensitivity analysis that cliff-edge effects[7] (abrupt change in the result of the analysis for a realistic variation of inputs) potentially leading to early or large radioactive releases can be reliably avoided. This demonstration is particularly important in the case of best estimate analysis used for design extension conditions and particularly for severe accidents, which have higher potential for degradation of the barriers to early or large radioactive releases.

[7] Definition of a ‘cliff-edge effect’ is provided in SSR-2/1 (Rev 1), § 5.21 [1]. The term „plant parameter“ in the definition should be interpreted in a broad sense, i.e. as any plant physical variable, design aspect, equipment condition, magnitude of a hazard, etc. that can influence equipment or plant performance.

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

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

6.9. For conservative deterministic safety analysis of anticipated operational occurrences and DBAs, in addition to the fully conservative approach, one of two following options, or a combination of both should be considered: either:

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

While in the first case the results are expressed in terms of a set of calculated conservative values of parameters limited by acceptance criteria, in the second phase the results are expressed in terms of ranges of the calculated parameters.

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

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

CONSERVATIVE AND COMBINED APPROACHES TO DETERMINISTIC SAFETY ANALYSIS FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DBAS

6.12. In conservative or combined approaches, conservative selection of initial and boundary conditions used as input for the analysis should be made from the ranges of parameters specified in the plant limits and conditions (see Table 2). Examples of initial conditions are reactor power level, power distribution, pressure, temperature and flow in the primary circuit. Examples of boundary conditions are actuation set-point and performance characteristics of the plant systems such as pumps and power supplies, external sources and sinks for mass and energy, and other parameters changing during the course of the transient. Selection of conservative assumptions with regard to the availability of systems and operator actions is discussed separately for individual plant states in Section 7 of this Safety Guide.

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

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

6.14. In the case when best estimate code in combination with conservative inputs and assumptions is used, it should be ensured that the uncertainties associated with the best estimate code are sufficiently compensated by conservative inputs. To take into account uncertainties related to code models, the complete analysis should consider a combination of validation of the code, use of conservatisms and use of sensitivity studies. These studies may be different depending on the type of PIE ; therefore this study should be carried out for each deterministic safety analysis.

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

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

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

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

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

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

6.19. Initial conditions that cannot occur at the same time in combination need not be considered. For example, the limiting decay heat and the limiting peaking factors cannot physically occur at the same time of the fuel campaign. However the initial conditions considered should cover the most unfavourable possible combination.

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

BEST ESTIMATE DETERMINISTIC SAFETY ANALYSIS WITH QUANTIFICATION OF UNCERTAINTIES FOR ANTICIPATED OPERATIONAL OCCURRENCES AND DBAS

6.21. Uncertainties in deterministic safety analysis, in particular for anticipated operational occurrences and DBAs, may be addressed by the use of a best estimate computer code in combination with best estimate initial and boundary conditions. To achieve conservative safety analysis, uncertainties should be identified and assessed to confirm that the actual plant parameters will be bounded by the results of calculation plus uncertainty with an adequate confidence.

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

6.23. A reliable assessment of the uncertainties is needed to carry out acceptable best estimate analyses with quantification of uncertainties, especially for the identification of aleatory and epistemic sources of uncertainties. Code-to-data comparisons are the preferred means to quantify the uncertainties. However, a combination of sensitivity studies, code to code comparisons and expert judgements may also be used as an input for the assessment.

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

6.25. Within the uncertainty methods considered, uncertainties should be evaluated using either (a) propagation of input uncertainties or (b) extrapolation of output uncertainties. For the ‘propagation of input uncertainties’, uncertainty is obtained by performing a sufficient number of calculations varying these input uncertain parameters. For the ‘extrapolation of output uncertainty’ approach, uncertainty is obtained from the output uncertainty based on comparison between calculation results and experimental data.

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

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

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

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

7. DETERMINISTIC SAFETY ANALYSIS FOR DIFFERENT PLANT STATES AND ACCIDENT SCENARIOS

GENERAL CONSIDERATIONS

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

7.2. In addition, deterministic safety analysis should follow more specific guidance regarding objectives of the analysis, selection of acceptance criteria, consideration of availability of various plant systems, operator actions, treatment of uncertainties and any other assumptions of the analysis for individual plant states specified further on in this section.

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

1) Code models;

2) Plant operating parameters;

3) Control and limitation systems;

4) Active safety systems;

5) Passive safety systems;

6) Safety features for design extension conditions;

7) Operator actions.

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

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

DETERMINISTIC SAFETY ANALYSIS FOR NORMAL OPERATION

Specific objectives of the analysis

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

7.7. The limits and conditions used in normal operation should cover all important initial and boundary conditions that will be subsequently used in the analysis of anticipated operational occurrences, DBAs and design extension conditions.

7.8. All possible operating modes of normal operation should be analysed, with particular attention paid to transient operational regimes such as changes in reactor power, reactor shutdown from power operation, reactor cooling down, handling of irradiated fuel and off-loading of irradiated fuel from the reactor to the spent fuel pool.

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

Acceptance criteria

7.10. The analysis should assess whether normal operation of the plant can be carried out in such a way that plant parameter values do not exceed 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.

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 within acceptable limits; and ensure that the principle that these doses should be as low as reasonably achievable has been satisfied. However, demonstration of compliance with the radiological acceptance criteria for normal operation is not covered by this Safety Guide.

Availability of systems

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

Operator actions

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

Analysis assumptions and treatment of uncertainties

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

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

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

REALISTIC DETERMINISTIC SAFETY ANALYSIS FOR ANTICIPATED OPERATIONAL OCCURRENCES

Specific objectives of the analysis

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

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

7.19. In addition, the anticipated operational occurrences should not lead to any unnecessary challenges to safety equipment primarily designed for protection in the event of DBAs. It is therefore advisable to demonstrate by the analysis that, in case of the operation of the plant control and limitation systems as intended, these systems will be capable of preventing the initiation of the safety systems.

Acceptance criteria

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

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

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

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

Availability of systems

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

Operator actions

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

Analysis assumptions and treatment of uncertainties

7.26. Realistic analysis of anticipated operational occurrences should be analysed with best estimate methodology covering anticipated plant initial conditions considered in determination of the PIEs.

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

Specific objectives of the analysis

7.27. Conservative analysis[8] of anticipated operational occurrences and DBAs should demonstrate that the safety systems alone are capable of fulfilling the following safety requirements

—Shut down the reactor and achieve subcritical condition during and after anticipated operational occurrences or DBA conditions.

—Remove residual heat from the core after reactor shutdown from all anticipated operational occurrences or DBA conditions.

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

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

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

Acceptance criteria

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

[8] The term “conservative analysis” is to be understood according to para 2.14

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

7.32. Specific decoupling criteria should be defined in order to prove that the three main safety functions can be ensured in any condition and that, in an anticipated operational occurrences or DBA, at least one safety barrier remains able to limit the radiological releases to the environment.

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

—An event should not generate a subsequent more serious plant condition without the occurrence of a further independent failure. Thus an anticipated operational occurrence by itself should not generate a DBA, and a DBA (in combination with a single failure) should not generate design extension conditions.

—There should be no consequential loss of function of the safety systems needed to mitigate the consequences of an accident.

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

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

—The number of fuel cladding failures which could occur should be limited for each type of PIE to allow the global radiological criteria to be met.

—In accidents with fuel uncovering and heatup, a coolable geometry and structural integrity of the fuel rods should be maintained.

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

—Subcriticality of nuclear fuel in reactor after shutdown, in fresh fuel storage and in the spent fuel pool should be maintained. Temporary recriticality may be acceptable for certain events and plant operating modes, however without exceeding criteria associated with sufficient cooling of the fuel.

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

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

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

Availability of systems

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

— For anticipated operational occurrences, normal operation systems that are in operation at the beginning of the event and that are not affected by the initiating event and the consequences of the PIE, can be assumed to continue to operate.

— For DBAs:

- Safety systems designed and maintained as safety grade (in accordance with the rules for quality assurance, periodic testing, use of accepted design codes and equipment qualification) should be assumed to operate with conservative performances.
- Any control or limitation systems should be assumed to start operating only if their functioning would aggravate the effects of the initiating event. No credit should be taken for the operation of the control systems in mitigating the effects of the initiating event.
- Single 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. If the single failure is applied to the reactor scram system, the insertion of the control rod that has the greatest effect on reactivity should be assumed to fail.

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 starting the actions, typically earlier than in 30 minutes if performed in the control room, or 60 minutes for the field actions.

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

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

Analysis assumptions and treatment of uncertainties

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

7.41. Conservative analysis of anticipated operational occurrences should also include the same conservative assumptions as used for the deterministic DBA analysis, especially those assumptions which relate to the systems for maintaining safety functions during these PIEs.

7.42. If a conservative methodology is applied, the safety systems should be assumed to operate at their minimum or maximum performance levels, whatever is conservative for a given acceptance criterion. For reactor trip and safety system actuation systems, this should assume that the action occurs at the worst edge of the possible range. Otherwise, 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 should be considered as additional conservative assumption. LOOP should be considered as an additional failure occurring at a time which has the most negative effect regarding the barrier integrity, then some acceptance criteria should be adapted taking into account the probability of this combination.

7.44. In line with the general rules for deterministic safety analysis, the source term evaluation of anticipated operational occurrences and DBAs would consist in taking into account all significant physical processes occurring during an accident and introducing to the modelling the conservatively determined numerical values of initial data and coefficients (which reflects the conservative approach) 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 cliff-edge effects.

Acceptance criteria

7.46. The same or similar technical and radiological criteria as those for DBAs should be considered for these conditions to the extent practicable.

Availability of systems

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

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

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

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

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

7.50. The single failure criterion need not be applied in the analysis of design extension conditions without significant fuel degradation.

7.51. Non-permanent systems and equipment should not be considered for demonstration of adequacy of the nuclear power plant design. Such equipment is typically considered to operate for long-term sequence and is considered available in the development of emergency operating procedures or accident management guidelines.

Operator actions

7.52. Conservative assumptions as described for DBAs should be used to the extent practicable. A more realistic approach that considers the information available and the inherent uncertainties in the data might be acceptable but should also consider the additional challenges of design extension conditions.

Analysis assumptions and treatment of uncertainties

7.53. Since the physical phenomena taking place in design extension conditions without significant fuel degradation do not qualitatively differ from those present in DBAs, the requirements on the selection, validation and use of computer codes specified for DBAs should also apply in principle for analysis of design extension conditions without significant fuel degradation.

7.54. For design extension conditions without significant fuel degradation, in principle the same combined approach or even best estimate approach with quantification of uncertainties (BEPU), as applicable for DBAs can be used. However, in line with the general rules for analysis of design extension conditions the best estimate analysis not always requiring a quantification of uncertainties can be used, but see 7.55 and 7.67.

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

7.56. For design extension conditions without significant fuel degradation, single failure criterion does not need to be applied.

DETERMINISTIC SAFETY ANALYSIS FOR DESIGN EXTENSION CONDITIONS WITH CORE MELTING

Specific objectives of the analysis

7.57. The analysis of severe accidents should identify the most severe plant parameters resulting from the core melt sequences, and demonstrate that:

- the plant can be brought into a state where the containment functions can be maintained in the long term
- the plant structures, systems, and components (e.g., the containment design) are capable of preventing large or early releases, including containment by-pass
- control locations remain habitable to allow performance of required staff actions.

7.58. The safety analysis of severe accidents should demonstrate that compliance with the acceptance criteria is achieved by features implemented in the design and not by implementation of accident management guidelines.

Acceptance criteria

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

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

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

Availability of systems

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

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

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

- Circumstances of the applicable initiating event, including those resulting from external hazards (e.g. station blackout, earthquakes) and

- Environment (e.g. pressure, temperature, radiation) and time period for which the equipment is needed

7.64. Single failure criterion need not be considered in severe accident analysis.

Operator actions

7.65. Operator actions should be considered as for design extension conditions without significant fuel degradation.

Analysis assumptions and treatment of uncertainties

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

- Core degradation processes and fuel melting;
- Fuel–coolant interactions (including steam explosions);
- In-vessel melt retention;
- Vessel melt-through;
- Distribution of heat inside the primary circuit;
- Generation, control, and combustion of hydrogen;
- Failure or bypass of the containment;
- Corium–concrete interaction;
- Release and transport of fission products, including venting to prevent overpressure in the containment;
- Ability to cool in-vessel and ex-vessel core melt.

7.67. Analysis of severe accidents should be performed using a realistic approach in Table 2, (to the extent possible). Since explicit quantification of uncertainties may be impractical due to complexity of the phenomena and insufficient experimental data, sensitivity analyses should be performed to demonstrate the robustness of the results and the conclusions of the severe accident analyses.

DETERMINISTIC SAFETY ANALYSIS IN SUPPORT OF PRACTICAL ELIMINATION OF CERTAIN CONDITIONS

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

7.69. According to 2.8, the demonstration of "practical elimination" of accident situations which could lead to large or early releases include deterministic considerations supplemented by a number of investigations such as those related to fabrication, testing, inspection and evaluation of the operating experience and by probabilistic considerations, taking into account the uncertainties due to the limited knowledge of some physical phenomena.

7.70. Demonstration of practical elimination of certain conditions (unless such conditions are judged as physically impossible) should include the following steps:

- Identification of undesired conditions (challenges) potentially endangering the containment integrity or by-passing the containment, resulting in early or large releases,

- Assessment of the ability of the design and operational provisions with high confidence to eliminate or to address the challenges
- Sensitivity studies to provide assurance that sufficient margins exist to address uncertainties and to avoid cliff-edge effects
- Final confirmation of the adequacy of the provisions by deterministic safety analysis, complemented by probabilistic safety assessment and engineering judgment.

7.71. Although probabilistic targets can be set, demonstration of practical elimination should not be based solely on low probability numbers. The achievement of any probabilistic value cannot be considered a justification for not implementing reasonable design or operational measures.

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

8. DOCUMENTATION, REVIEW AND UPDATE OF DETERMINISTIC SAFETY ANALYSIS

DOCUMENTATION

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

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

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

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

8.5. Brief description of the computer codes used in the deterministic safety analysis should be provided. In addition to the reference to the specific code documentation the description should contain convincing justification that the code is adequate for the given purpose and has been validated by the user to a reasonable extent.

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

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

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

8.9. The time span of any scenario analysed and presented should extend up to the moment when the plant reaches a safe and stable end state. 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 the core is achieved, and the core is subcritical by a given margin.

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

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

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

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

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

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

(e) Results of sensitivity analysis, as appropriate.

8.12. Documentation of deterministic safety analysis should be subject to relevant quality assurance procedures and quality control [15-17].

8.13. More detailed information about documentation of deterministic safety analysis to be included in different stages of safety analysis reports can be found in GS-G-4.1 (Rev. 1) [18] (Format and Content of Safety Analysis Report for Nuclear Power Plants; in preparation).

REVIEW AND UPDATE OF DETERMINISTIC SAFETY ANALYSIS

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

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

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

8.17. The outcomes of the reassessment including new deterministic safety analyses if necessary should be reflected in updated the safety report with the same level of comprehensiveness as the original safety report.

9. INDEPENDENT VERIFICATION OF DETERMINISTIC SAFETY ANALYSIS BY THE LICENSEE

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

9.2. The main purpose of the independent verification of safety analysis by the licensee (the operating organization) is to reconfirm that the safety analysis developed by other entities such as designers, manufacturers and constructors satisfies the applicable safety requirements. As a minimum, it should be verified by the licensee (but not necessarily limited to) that the design will comply with the relevant regulatory requirements and acceptance criteria are complied with as an essential factor of the licensee's prime responsibility for safety.

9.3. According to SF-1, §. 3.6 [19] among other duties the operating organization is responsible for verifying appropriate design and the adequate quality of facilities and activities and of their associated equipment. Adequacy of the design should be demonstrated by means of safety assessment.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Selection of acceptance criteria
- Selection of assumptions for ensuring safety margins
- Adequacy of description/evaluation of results

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

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

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

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

- Independent calculations are in reasonable qualitative and quantitative agreement with the original analysis, and they both demonstrate fulfilment of the relevant acceptance criteria
- All discrepancies found in the safety analysis are clearly understood and explained and they do not question conclusions regarding acceptability of the design.

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

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

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

REFERENCES

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

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

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition), IAEA, Vienna (2007).

[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, A General Framework for Prospective Radiological Environmental Impact Assessment and Protection of the Public, Draft IAEA Safety Guide, DS427 Draft Version 7, August 2015

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical Guidance. Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007)

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/REVISION 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011)

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012)

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

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

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015)

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007)

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011)

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

[15] 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)

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

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (in publication under DS456, to supersede GS-R-3)

[18] 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 (Rev. 1), NOTE: This Safety Guide is in preparation as DS449

[19] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006)

ANNEX. APPLICATION OF DETERMINISTIC SAFETY ANALYSIS

AREAS OF APPLICATION

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

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

(b) Safety analysis for licensing purposes (for regulatory authorizations), including regulatory 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 maintenance of emergency operating procedures

(h) Development of severe accident management guidelines.

(i) Demonstration of success criteria and development of accident sequences in the PSA. Levels 1 and 2.

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

APPLICATION OF DSA TO THE DESIGN OF NUCLEAR POWER PLANTS

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

A.4. Main components of the design requirements determined by deterministic safety analysis typically include nuclear power plant equipment sizing, capacity, set point values for parameters initiation, termination and control of the systems and working (environmental) conditions, which ensures effective operation of the systems in all relevant plant states and provide for adequate operating margins. The analysis also includes assessment of radiological effects for all plant states to ensure that there is confidence in future plant authorization.

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

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

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

APPLICATION OF DSA TO THE LICENSING OF NUCLEAR POWER PLANTS

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

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

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

APPLICATION OF DSA TO INDEPENDENT VERIFICATION BY THE REGULATORY BODY

A.11. A separate independent review is typically carried out by the regulatory body to check the completeness and the consistency of the deterministic safety analyses submitted for licensing purposes and to satisfy themselves that the design meets their requirements. As stated in GSR Part 4 (Rev 1), § 4.71 [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 DSA TO PERIODIC SAFETY REVIEWS

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

APPLICATION OF DSA TO PLANT MODIFICATIONS

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

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

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

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

APPLICATION OF DSA TO THE ANALYSIS OF EVENTS EXCEEDING NORMAL OPERATION LIMITS

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

To check the comprehensiveness of the earlier selection of postulated initiating events;

To determine whether the transients that have been analysed in the safety analysis report bound the event;

To provide additional information on the time dependence of the values of parameters that are not directly observable using the plant instrumentation;

To check whether the plant operators and plant systems performed as intended;

To check and review emergency operating procedures;

To identify any new safety issues and questions arising from the analyses;

To support the resolution of potential safety issues that are identified in the analysis of an event;

To analyse the severity of possible consequences in the event of additional failures (such as severe accident precursors);

To validate and adjust the models in the computer codes that are used for analyses and in training simulators.

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

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

APPLICATION OF DSA TO THE DEVELOPMENT AND VALIDATION OF EMERGENCY OPERATING PROCEDURES

A.20. Best estimate deterministic safety analyses are typically performed to confirm the recovery strategies that have been developed to restore normal operational conditions at the plant following transients due to anticipated operational occurrences and DBAs and design extension conditions without core melt. These strategies are reflected in the emergency operating procedures that define the actions to be taken to recover from such events. Deterministic safety analyses provide the input that is necessary to specify the operator actions to be taken, and the analyses play an important role in the review of accident management strategies. In the development of the recovery strategies for determining the available time period for the operator to take effective action, sensitivity calculations are carried out on the timing of the necessary operator actions, and these calculations may be used to optimize the procedures.

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

APPLICATION OF DSA TO THE DEVELOPMENT OF SEVERE ACCIDENT MANAGEMENT GUIDELINES

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

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

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

A.25. The accident management measures can be broadly divided into preventive and mitigatory measures. The analysis supporting the development of severe accident management guidelines typically focus on mitigatory measures, which are strategies for managing severe accidents to mitigate the consequences of core melt. For light water reactors, such strategies include: coolant injection into the degraded core; depressurization of the primary circuit; operation of containment sprays; and use of the fan coolers, hydrogen recombiners and filtered venting that are available in the reactors of different types that are in operation or being constructed. Possible adverse effects that may occur as a consequence of taking mitigatory measures are taken into account, such as pressure spikes, hydrogen generation, return to criticality, steam explosions, thermal shock or hydrogen deflagration or detonation. Similar to light water reactors, reactors of alternate designs consider mitigatory measures applicable to the design.

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

APPLICATION OF DSA TO DEMONSTRATION OF SUCCESS CRITERIA AND DEVELOPMENT OF ACCIDENT SEQUENCES IN THE PSA (LEVELS 1 AND 2)

A.27. Deterministic analysis and probabilistic assessment are complementary means to provide a comprehensive view of the overall safety of the plant for the entire range of the frequency–consequence spectrum.

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

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

LIST OF CONTRIBUTORS TO DRAFTING AND REVIEW

Boyce, T.	Nuclear Regulatory Commission, United States of America
Courtin, E. J. F.	Areva NP, France
Harwood, C.	Canadian Nuclear Safety Commission, Canada
Herer, C.	Institute for Radiological Protection and Nuclear Safety, France
Luis-Hernandez, J.	Institute for Radiological Protection and Nuclear Safety, France
Lee, S.	Korean Institute for Nuclear Safety, Republic of Korea
Misak, J.	Nuclear Research Institute Rez, Czech Republic
Ochi, H.	Nuclear Regulatory Agency, Japan
Ramon, J.	Nuclear Safety Council, Spain
Spitzer, C.	International Atomic Energy Agency
Villalibre, P.	International Atomic Energy Agency
Yllera, J.	International Atomic Energy Agency