Proceedings of the ASME 2010 3rd Joint US-European Fluids Engineering Summer Meeting and
8th International Conference on Nanochannels, Microchannels, and Minichannels
FEDSM-ICNMM2010
August 1-5, 2010, Montreal, Canada

FEDSM-ICNMM2010-31285

IAEA SSG-2: DETERMINISTIC SAFETY ANALYSIS FOR NPP

M. Dusic
IAEA
Vienna, Austria

F. D'Auria, A. Petruzzi
University of Pisa
Pisa, Italy

L.M.C. Dutton
Mark Dutton and Associates
United Kingdom

H. Glaeser
Gesellschaft für Anlagen- und
Reaktorsicherheit mbH,
Munich, Germany

B. Mavko
Jožef Stefan Institute,
Slovenia

F. Pelayo
Consejo de Seguridad Nuclear
Madrid, Spain

ABSTRACT

Regulating safety is a national responsibility. However, radiation risks may transcend national borders, and international cooperation serves to promote and enhance safety globally by exchanging experience and by improving capabilities to control hazards, to prevent accidents, to respond to emergencies and to mitigate any harmful consequences. International safety standards provide support for States in meeting their obligations under general principles of international law, such as those relating to environmental protection.

The objective of the Safety Guide SSG-2 "Deterministic Safety Analysis for Nuclear Power Plants (NPP)" is to provide harmonized guidance to designers, operators, regulators and providers of technical support on deterministic safety analysis for nuclear power plants.

1. INTRODUCTION

Current developments for ensuring the stable, safe and competitive operation of nuclear reactors are closely related to the advances that are being made in safety analysis. Deterministic safety analyses for anticipated operational occurrences, Design Basis Accidents (DBAs) and Beyond Design Basis Accidents (BDBAs), as defined in Refs [1, 2], are essential instruments for confirming the adequacy of safety provisions.

Safety analyses play an important role throughout the lifetime of a nuclear power plant. The stages of and occasions in a plant's lifetime in which the use of safety analyses is relevant include: (a) Design; (b) Commissioning; (c) Operation and shutdown; (d) Modification of design or operation; (e) Periodic safety review; (f) Life extension, in States where licences are issued for a limited duration.

Initially, rigorous conservative approaches to anticipated operational occurrences and design basis accidents were used in deterministic safety analyses. Licensing calculations used conservative codes with conservative input data, mostly owing to the difficulty of modelling complicated physical phenomena with limited computer capacity and a lack of adequate data. As more experimental data have become available, and with advances in code development, for Loss Of Coolant Accidents (LOCAs) in particular, the practice in many States has moved towards a more realistic approach together with an evaluation of uncertainties. This is termed a best estimate approach.

The use of best estimate analysis together with an evaluation of the uncertainties is increasing for the following reasons:

a) The use of conservative assumptions may sometimes lead to the prediction of an incorrect progression of events or unrealistic timescales, or it may exclude some important physical phenomena. The sequences of events that constitute the accident scenario, which are important in assessing the safety of the plant, may thus be overlooked.
b) In addition, the use of a conservative approach often does not show the margins to the acceptance criteria that apply in reality, which could be taken into account to improve operational flexibility.
c) A best estimate approach provides more realistic information about the physical behaviour of the plant, assists in identifying the most relevant safety parameters and allows more realistic comparison with acceptance criteria.

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

1) Demonstrating or assessing compliance with regulatory requirements;
2) Identifying possible enhancements of safety and reliability;
3) Obtaining increased operational flexibility within safety limits for nuclear power plants.

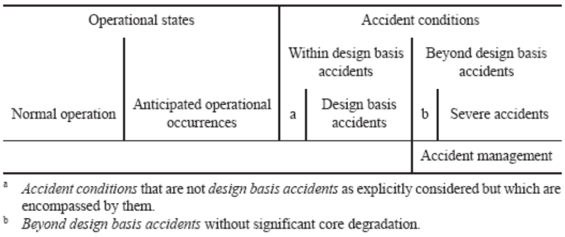
The recommendations are based on current good practices at nuclear power plants around the world and derive mainly from experience in performing transient analyses and accident analyses for nuclear power plants.

Section 2 addresses the plant states and the classification of conditions that should be considered. Deterministic safety analysis and acceptance criteria are described in Section 3 together with the difference between a conservative and a best estimate plus uncertainty analysis. The quality of the analysis of computer codes and their verification and validation are described in Section 4. The relationship of deterministic safety analysis to engineering aspects of safety and to probabilistic safety analysis is presented in Section 5. The application of deterministic safety analysis is described in Section 6. Source term evaluation for operational states of and accident conditions for nuclear reactors is described in Section 7.

2. GROUPING OF INITIATING EVENTS AND ASSOCIATED TRANSIENTS RELATING TO PLANT STATES

Plant states for nuclear power plants are specified in Ref. [1], as shown in Table 1. The plant states are divided into operational states and accident conditions. Normal operation is defined as operation within specified operational limits and conditions. An anticipated operational occurrence is an operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions (it may result in a reactor scram, however). Design basis accidents are accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits (see Ref. [2]).

Table 1: Plant Status.



Operational states		Accident conditions			
		Within design basis accidents		Beyond design basis accidents	
Normal operation	Anticipated operational occurrences	a	Design basis accidents	b	Severe accidents
				Accident management	

[a] *Accident conditions* that are not *design basis accidents* as explicitly considered but which are encompassed by them.

[b] *Beyond design basis accidents* without significant core degradation.

For all plant states, a comprehensive listing of Postulated Initiating Events (PIEs) should be prepared for ensuring that the analysis of the behaviour of the plant is complete. An initiating event is an event that leads to anticipated operational occurrences or accident conditions. This includes operator errors and equipment failures (both within and external to the facility), human induced or natural events, and internal or external hazards that, directly or indirectly, challenge one or more of the systems required to maintain the safety of the plant.

When performing deterministic safety analyses for anticipated operational occurrences, design basis accidents and beyond design basis accidents, all postulated initiating events and associated transients should be grouped into categories. One approach is to group events according to the principal effects that could result in the degradation of safety systems. Anticipated operational occurrences typically include loss of normal power, turbine trip, failure of control equipment and loss of power to the main coolant pump. The categories of postulated initiating events for design basis accidents typically include the following transients: (a) Increase or decrease of the removal of heat from the reactor coolant system; (b) Increase or decrease of the flow rate for the reactor coolant system; (c) Anomalies in reactivity and power distribution; (d) Increase or decrease of the reactor coolant inventory; (e) Release of radioactive material from a subsystem or component.

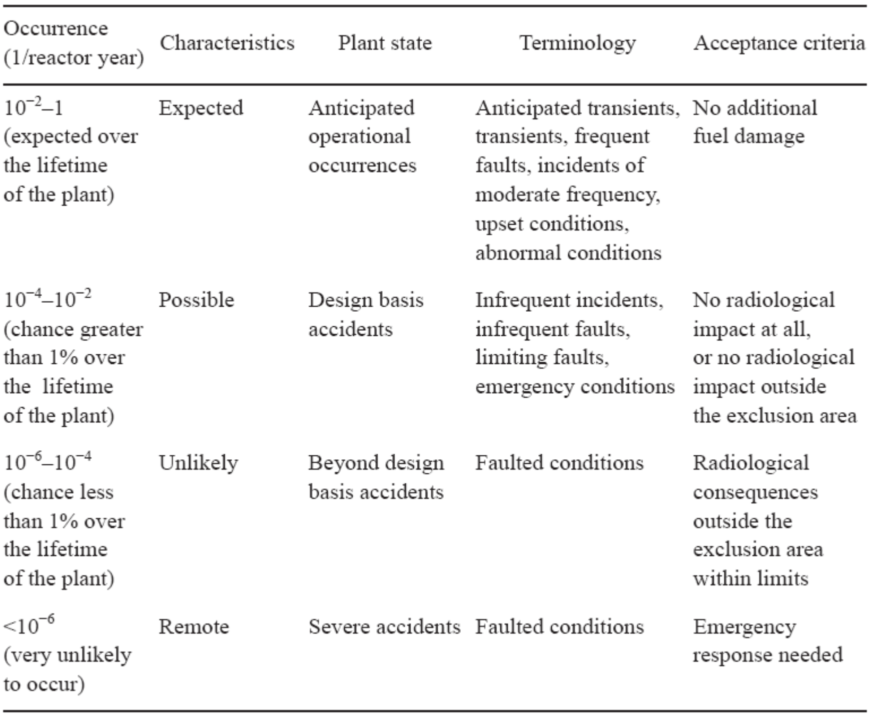
Computational analysis of all possible design basis accident scenarios may not be practicable. Bounding or enveloping scenarios shall be chosen so that they present the greatest possible challenge to the relevant acceptance criteria and are limiting for the performance parameters of safety related equipment. In addition to design basis accidents, Anticipated Transients Without Scram (ATWS) have traditionally been analysed for light water reactors.

There are two alternative approaches to grouping postulated initiating events and their associated transients. Currently, the most common approach is to group initiating events and their associated transients according to the expected frequency of the initiating events, as indicated in Table 2. The second approach is to group according to the frequency of the accident scenarios. One way of quantifying the frequency of each accident scenario is to perform a probabilistic safety analysis. Probabilistic safety analysis identifies not only the sequences that lead to core degradation, but also the more frequent sequences that do not lead to plant damage or that lead to limited damage.

3. DETERMINISTIC SAFETY ANALYSIS AND ACCEPTANCE CRITERIA

Safety analyses are analytical evaluations of physical phenomena occurring at nuclear power plants, made for the purpose of demonstrating that safety requirements, such as the requirement for ensuring the integrity of barriers against the release of radioactive material and various other acceptance criteria, are met for all postulated initiating events that could occur over a broad range of operational states, including

Table 2: Possible Subdivision of Postulated Initiating Events.



Occurrence (1/reactor year)	Characteristics	Plant state	Terminology	Acceptance criteria
10^{-2}–1 (expected over the lifetime of the plant)	Expected	Anticipated operational occurrences	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions	No additional fuel damage
10^{-4}–10^{-2} (chance greater than 1% over the lifetime of the plant)	Possible	Design basis accidents	Infrequent incidents, infrequent faults, limiting faults, emergency conditions	No radiological impact at all, or no radiological impact outside the exclusion area
10^{-6}–10^{-4} (chance less than 1% over the lifetime of the plant)	Unlikely	Beyond design basis accidents	Faulted conditions	Radiological consequences outside the exclusion area within limits
$<10^{-6}$ (very unlikely to occur)	Remote	Severe accidents	Faulted conditions	Emergency response needed

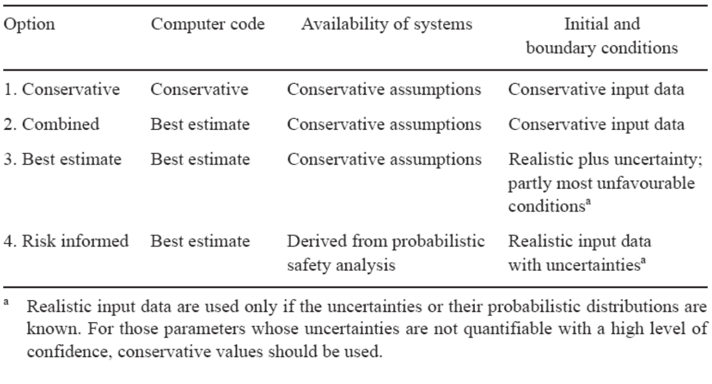
different levels of availability of the safety systems. There are two basic types of safety analysis: deterministic safety analysis and probabilistic safety analysis.

Deterministic safety analyses for a nuclear power plant predict the response to postulated initiating events. A specific set of rules and acceptance criteria is applied. Typically, these should focus on neutronic, thermohydraulic, radiological, thermomechanical and structural aspects, which are often analysed with different computational tools. Deterministic safety analyses for design purposes should be characterized by their conservative assumptions and bounding analysis. This is achieved by an iterative process in the design phase, when the limiting case(s) in terms of the minimum margin to the acceptance criteria is (are) determined for each group of postulated initiating events and sequences. To determine the limiting case for a given transient or set of transients, the consequential failures that are caused by the initiating event (internal or external) should be taken into account.

The time span of any scenario that is analysed 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. In some cases 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.

To guarantee an adequate degree of defence in depth, all credible failure mechanisms of the different barriers should be analysed. Certain limiting faults (e.g. large break loss of coolant accidents, secondary breaks, rod ejection in pressurized water reactors or rod drop in boiling water reactors) should also be part of the deterministic safety analysis and should not be excluded merely on the grounds of their low frequency. Table 3 lists different options for performing deterministic safety analyses, whose options 1 to 3 are described with more details in the following sub- sections. Option 4 is not yet widely used. It includes a realistic analysis, on the basis of a probabilistic safety analysis, to quantify the availability of systems that are significant for safety and the success of mitigatory actions. Option 4 is also relevant to the development of risk informed decision making, and it may be used as a means of verifying the deterministic design basis envelope.

Table 3: Options for Combination of a Computer Code and Input Data.



Option	Computer code	Availability of systems	Initial and boundary conditions
1. Conservative	Conservative	Conservative assumptions	Conservative input data
2. Combined	Best estimate	Conservative assumptions	Conservative input data
3. Best estimate	Best estimate	Conservative assumptions	Realistic plus uncertainty; partly most unfavourable conditions[a]
4. Risk informed	Best estimate	Derived from probabilistic safety analysis	Realistic input data with uncertainties[a]

[a] Realistic input data are used only if the uncertainties or their probabilistic distributions are known. For those parameters whose uncertainties are not quantifiable with a high level of confidence, conservative values should be used.

3.1 Conservative Deterministic Safety Analysis

A conservative approach usually means that any parameter that has to be specified for the analysis should be allocated a value that will have an unfavourable effect in relation to specific acceptance criteria. The concept of conservative methods was introduced in the early days of safety analysis to take account of uncertainties due to the limited capability of modelling and the limited knowledge of physical phenomena, and to simplify the analysis.

In a traditional conservative analysis, both the assumed plant conditions and the physical models used are set conservatively. The reasoning is that such an approach would demonstrate that the calculated safety parameters are within the acceptance criteria and would ensure that no other transient of that category would exceed the acceptance criteria. In particular, Option 1 in Table 3 implies: a) the code is conservative, as it is intended to produce pessimistic results; b) the selected initial and boundary conditions, including the time available for the operator to act, are assumed to have pessimistic values; c) no credit is taken for non-safety-grade equipment unless it is conservative to do so; d) the most severe single failure of the safety systems that are designed to mitigate the consequences of the accident is assumed.

Option 2 in Table 3 is also considered to be a conservative approach. Currently, it is being used for safety analyses in many States, that is, the use of a ‘best estimate’ computer code instead of a conservative code. However, conservative initial and boundary conditions are used, as well as conservative assumptions with regard to the availability of systems. Conservative initial and boundary conditions should be used to ensure that all uncertainties associated with the code models and plant parameters are bounded. The complete analysis requires a combination of validation of the code, use of conservatism in the data and use of sensitivity studies.

However, for both Options 1 and 2, it should also be demonstrated that the calculated results are conservative for each application. The interaction with the set points for activation of the relevant safety systems or the plant control systems should be reviewed to ensure that the conservatism of the results is adequate.

For the purpose of conservative calculations, 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 acceptance criteria. One set of conservative values for initial and boundary conditions does not necessarily lead to conservative results for every safety parameter. Therefore, the appropriate conservatism should be selected for each initial and boundary condition, depending on the specific transient and the associated acceptance criterion. 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 acceptance criteria. One set of conservative values for initial and boundary conditions does not necessarily lead to conservative results for every safety parameter. Therefore, the appropriate conservatism should be selected for each initial and boundary condition, depending on the specific transient and the associated acceptance criterion. Moreover, conservative assumptions should be made with respect to the timing of operator actions.

3.2 Best Estimate Plus Uncertainty Analysis

The use of a conservative methodology may be so conservative that important safety issues may be masked. In addition, a conservative approach often may not show margins to acceptance criteria which, in reality, could be used to obtain greater operational flexibility. To overcome these deficiencies, it may be preferable to use a best estimate approach together with an evaluation of the uncertainties to compare the results of calculations with acceptance criteria. This type of analysis is referred to as a best estimate plus uncertainties approach. A best estimate approach provides more realistic information about the physical behaviour of the reactor, identifies the most relevant safety issues and provides information about the existing margins between the results of calculations and the acceptance criteria.

For a best estimate analysis [3], best estimate codes that realistically describe the behaviour of physical processes in a component or system should be used. This requires sufficient data to be able to ensure that all important phenomena have been taken into account in the modelling or that their effects are bounded. Establishing that all important phenomena have been taken into account in the modelling or that their effects are bounded should be part of the validation programme (see Section 4). Because the results of best estimate codes are not designed to bound experimental data, best estimate codes are not intended to provide conservative results. Uncertainties in the results due to unavoidable approximations in the modelling should therefore be quantified using experimental results.

Best estimate plus uncertainty analysis, i.e. Option 3 in Table 3, requires a combination of a best estimate computer code and realistic assumptions for the initial and boundary conditions. Such an approach should be based on statistically combined uncertainties for plant conditions and code models to establish, with a specified high probability, that the calculated results do not exceed the acceptance criteria. It is common practice to require that assurance be provided of a 95% or greater probability that the applicable acceptance criteria for a plant will not be exceeded.

In a deterministic safety analysis, the most limiting initial conditions that are expected over the lifetime of the plant should be used, and these are usually based on sensitivity analyses. As an example, the following unfavourable deterministic requirements may also be valid in a ‘best estimate’ approach for the safety analysis of a loss of coolant accident:

a) Most unfavourable single failure and unavailability due to preventive maintenance during operation, if allowed, should be included in the analysis;
b) Most unfavourable break location and range of break sizes that results in the highest peak cladding temperature or

other limiting values of the relevant safety variables that are to be compared with acceptance criteria.

c) Loss of off-site power;
d) Initial core power should be specified for the most unfavourable conditions and values that may occur in normal operation,
e) Conservative values for the reactivity feedback coefficients (in case of point kinetic calculation);
f) Time within the fuel cycle (i.e. beginning of cycle, end of cycle, burnup);
g) The rod that has the greatest effect on reactivity is assumed to be stuck (in certain reactor designs);
h) Values of thermohydraulic parameters such as pressure, temperature, flow rates and water levels in the primary circuit and secondary circuit that result in the shortest time to uncovering of the core.

The licensing requirements with regard to the availability of systems should be the same regardless of whether a conservative approach or a best estimate approach is to be used. They are currently the ‘most unfavourable single failure’ criterion and the assumption of a coincident loss of off-site power in the analysis of design basis accidents. With improvements in the development of methods for realistic analyses, these traditional assumptions might not always be applied in the future; for example, the most unfavourable single failure criterion might be relaxed by introducing probabilistic arguments for the availability of systems. This is governed by risk informed safety analysis, using Option 4 in Table 3.

With respect to the nodalization, 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. The nodalization should be sufficiently detailed that all the important phenomena of the scenario and all the important design characteristics of the nuclear power plant that is being analysed are represented. Different input data sets may be necessary for different scenarios. Sufficient sensitivity analyses should be performed on the nodalization to ensure that the calculated results are free from erratic variations.

Sensitivity and uncertainty analysis are part of Option 3 in Table 3. A sensitivity analysis includes systematic variation of the individual code input variables and of the individual parameters that are used in models, to determine their influence on the results of the calculations. An uncertainty analysis should be performed to address the uncertainties in the code models, in the plant model and in plant data, including uncertainties in measurements and uncertainties in calibration, for the analysis of each individual event. The overall uncertainty in the results of a calculation should be obtained by combining the uncertainties associated with each individual input. Studies to quantify the scaling effect between an experimental arrangement and the actual plant size should also be considered.

For licensing purposes, sensitivity analyses are performed to identify the conditions that lead to the smallest margin to acceptance criteria. Subsequently, uncertainty analyses should be performed for the most limiting conditions. The combined effect of uncertainties due both to the models and to the numerical methods can be evaluated using experimental data or by comparison with validated codes, as discussed in the next Section 4.

3.3 Acceptance Criteria

Basic acceptance criteria are usually defined as limits and conditions set by a regulatory body, and their purpose is to ensure the achievement of an adequate level of safety. These criteria are supplemented by other requirements known as acceptance criteria (sometimes termed derived acceptance criteria) to ensure defence in depth by, for example, preventing the consequential failure of a pressure boundary in an accident.

To demonstrate the safety of the plant, the following basic acceptance criteria should be fulfilled:

a) The individual doses and collective doses to workers and the public are required to be within prescribed limits and as low as reasonably achievable in all operational states by ensuring mitigation of the radiological consequences of any accident [1];
b) The integrity of barriers to the release of radioactive material (i.e. the fuel itself, the fuel cladding, the primary and/or secondary reactor coolant system, the primary and/or secondary containment) should be maintained, depending on the categories of plant states for the accidents for which their integrity is required;
c) The capabilities of systems that, and operators who, are intended to perform a safety function, directly or indirectly, should be ensured for the accidents for which performance of the safety function is required;
d) In some designs, it is required that early large releases of radioactive material be practically excluded.

Acceptance criteria should be established for the entire range of operational states and accident conditions and may be related to the frequency of the event. Events that occur frequently, such as anticipated operational occurrences, should have acceptance criteria that are more restrictive than those for less frequent events such as design basis accidents. Acceptance criteria should be set in terms of the variable or variables that directly govern the physical processes that challenge the integrity of a barrier. Nevertheless, it is a common engineering practice to make use of surrogate variables to establish an acceptance criterion 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 sufficiently high degree of conservatism should be included to ensure that there are adequate safety margins beyond the acceptance criterion to allow for uncertainties. Acceptance criteria for design basis accidents may be supplemented by criteria that relate to severe accidents. These are typically core damage frequency, prevention of consequential damage to the containment, large early release frequency, etc...

4. VERIFICATION AND VALIDATION OF COMPUTER CODES

Procedures should be implemented to ensure that the code correctly performs all the intended functions and does not perform any unintended function. The necessary activities can be categorized as follows: (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 and installation of the code and upgrading of code manuals; (e) Configuration management; (f) Control of interfaces.

Verification of the code design should be performed to demonstrate that the code design conforms to the design requirements. In general, the verification of the code design should ensure that the numerical methods, the transformation of the numerical equations into a numerical scheme to provide solutions, and user options and their restrictions are appropriately implemented in accordance with the design requirements. The code design may contain the integration or coupling of codes. In such cases, verification of the code design should ensure that the links and/or interfaces between the codes are correctly designed and implemented to meet the design requirements

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. A review and inspection of the entire code may not be practicable for verification purposes owing to its large size. In such cases, verification of individual modules or parts of the code should be conducted, and this should include a careful inspection of all interfaces between the modules.

Validation should be performed on all computer codes that are used for the deterministic safety analysis of nuclear power plants. The purpose of validation (code assessment) is to provide confidence in the ability of a code to predict, realistically or conservatively, the values of the safety parameter or parameters of interest. It should also quantify the accuracy with which the values of parameters can be calculated.

For complex analysis, the validation process 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 someone who is independent of the developer of the code. Both phases are necessary for an adequate assessment. If possible, the data that are used for the independent validation of the code and the data that are used for the validation by the code developers should be derived from different experiments.

The validation process should ideally include four different types of test calculation: 1) Basic tests; 2) Separate effect tests; 3) Integral tests and 4) Nuclear power plant level tests and operational transients. The validation tests should ideally cover the entire range of values of parameters, conditions and physical processes that the code is intended to cover. 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 extremely inaccurate for other data sets. 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. 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. 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.

As validation tests should be mostly based on experimental data, and only occasionally with analytical solutions or with results obtained by other codes (code to code comparisons can be used for validation purposes provided that at least one of the codes has been validated), it therefore follows that the uncertainty in the code is directly related to the uncertainty in the experimental data. Care should therefore be exercised when planning an experiment to ensure that the measured data are as suitable as possible for the purposes of code validation: the safety parameters that will ultimately be calculated using the code should be considered when the experiment and its instrumentation are planned and the uncertainty in the experimental data should be reported in the documentation of the experiment.

5. DETERMINISTIC SAFETY ANALYSIS, ENGINEERING SAFETY ASPECTS AND PROBABILISTIC SAFETY ANALYSIS

A key element of the safety analysis for a nuclear power plant is the demonstration that defence in depth is adequate, and deterministic safety analyses play a vital role in this demonstration. The objective of deterministic safety analyses is to demonstrate that, in normal operational conditions and accident conditions, a sufficient number of barriers are retained. The following relations between deterministic safety analysis and engineering safety aspects can be characterized:

- The requirements for each safety system and its supporting systems to fulfil its safety function, including their reliability, and the safety classification should be determined in accordance with the requirement to provide defence in depth;
- To determine the adequacy of the assumed initial and boundary conditions, a careful analysis should be made of the process that links the original cause, all the consequential failures and the initiating event itself;
- Analyses should be performed for each category of postulated initiating event to demonstrate that safety margins are adequate for design basis accidents. Regulatory requirements that include a frequency and/or dose relationship for design basis accidents may accept the failure of some barriers for less frequent accidents, provided that

any release of radioactive material to the environment is acceptably low.

- Account should be taken of the redundancy that is provided for in the design of safety systems and support systems that are designed to prevent, limit or mitigate the consequences of an initiating event;
- Account should be taken of the independence, diversity and physical separation that have been incorporated into the design to avoid possible common cause failures;
- The time period that is assumed in the analysis for temporary inoperability should be based on the maintenance and repair activities that have been specified;
- For each plant modification that may have an impact on safety, an analysis should be performed to demonstrate compliance with the acceptance criteria;
- Deterministic safety analyses are also performed to develop a set of rules, namely, the operational limits and conditions. These reflect the limiting conditions of operation in terms of values of process variables, system requirements, system operability, surveillance and testing requirements, etc., as well as the necessary actions to take when the conditions of the plant are degraded or are not covered by the safety analysis.

As already stated, the objectives of the safety analysis are to identify issues that are important to safety and to demonstrate that the plant is capable of meeting any authorized limits on the release of radioactive material and on the potential exposure to radiation for each plant state. Thus a deterministic safety analysis alone does not demonstrate the overall safety of the plant, and it should be complemented by a probabilistic safety analysis to determine the probability of damage for each barrier, as stated in Ref. [1]. Probabilistic safety analysis is a suitable tool for evaluation of the risk that arises from low frequency sequences that lead to barrier damage, whereas a deterministic analysis is adequate for events of higher frequency for which the acceptance criteria are set in terms of the damage allowed. To verify that defence in depth is adequate, certain very low frequency design basis accidents, such as large break loss of coolant accidents or rod ejection accidents, are evaluated deterministically despite the low frequency of the initiating event. Thus deterministic analysis and probabilistic analysis provide a comprehensive view of the overall safety of the plant for the entire range of the frequency–consequence spectrum.

A probabilistic safety analysis fault tree is a powerful tool that can be used to confirm assumptions that are commonly made in the deterministic calculation about the availability of systems; for example, to determine the potential for common cause failures or the minimum system requirements, to identify important single failures and to determine the adequacy of technical specifications.

6. APPLICATION OF DETERMINISTIC SAFETY ANALYSIS

Deterministic safety analyses should be carried out for the following areas:

a) Design of nuclear power plants.

b) Production of new or revised safety analysis reports for licensing purposes, including obtaining the approval of the regulatory body for modifications to a plant and to plant operation.

c) Assessment by the regulatory body of safety analysis reports.

d) Analysis of incidents that have occurred or of combinations of such incidents with other hypothetical faults.

e) Development and maintenance of emergency operating procedures and accident management procedures.

f) Refinement of previous safety analyses in the context of a periodic safety review to provide assurance that the original assessments and conclusions are still valid.

Analyses at bullets a), b) and c) require either a conservative approach or a best estimate analysis together with an evaluation of uncertainties. Analyses at bullets d) and e) would normally require best estimate methods, in particular for complex occurrences that require a realistic simulation.

Regarding with item b), 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 should be demonstrated by means of an initial or an updated safety analysis report. “The safety analysis of the plant design … shall be consistent with the current or ‘as built’ state” (Ref. [1], para. 5.72). The safety analysis examines:

- All planned modes of the plant in normal operation;
- Plant performance in anticipated operational occurrences;
- Design basis accidents;
- Event sequences that may lead to beyond design basis accidents.

On the basis of this analysis, the robustness of the engineering design in performing its safety functions during postulated initiating events and accidents should be established. In addition, the effectiveness of the safety systems and safety related systems should be demonstrated, and guidance for emergency response should be provided. Analyses should be performed for transients that can occur in all planned modes of the plant in normal operation, including operations during shutdown. The range of scenarios should be evaluated to determine whether abrupt changes in the results of the analysis occur for a realistic variation of inputs (usually termed bifurcation or cliff edge effects).

A nuclear power plant may be modified on the basis of feedback from operating experience, the findings of periodic safety reviews, regulatory requirements, advances in knowledge or developments in technology. A revision of the safety analysis of the plant design should be made when major modifications or modernization programmes are implemented, when advances in technical knowledge and understanding of physical phenomena are made, when changes in the described plant configuration are implemented or when changes in operating procedures are made owing to operating experience. The modification of existing nuclear power plants is normally undertaken to counteract the ageing of the plant, to justify the continued operation of the plant, to take advantage of developments in technology or to comply with changes to the applicable rules and regulations. Other important applications of deterministic safety analysis are aimed at the more economical utilization of the reactor and the nuclear fuel. Such applications encompass uprating of the reactor power, the use of improved types of fuel and the use of innovative methods for core reloads. Such applications often imply that the safety margins to operating limits are reduced and special care should be taken to ensure that the limits are not exceeded.

With respect to plant operation, accident analyses may be used as a tool for obtaining a full understanding of events that occur during the operation of nuclear power plants and should form an integral part of the feedback from operating experience. Operational events may be analysed with several objectives, like to check the adequacy of the selection of postulated initiating events, or to determine whether the transients that have been analysed in the safety analysis report bound the event, etc… Actual plant data should be used in the best estimate approach for the analysis of operational events. If there is a lack of detailed information on the plant state, sensitivity studies, with the variation of certain parameters, should be performed.

Regarding with item e), best estimate deterministic safety analyses should be performed to confirm the strategies that have been developed to restore normal operational conditions at the plant following transients due to anticipated operational occurrences and design basis accidents. These strategies are reflected in the emergency operating procedures that define the actions that should be taken during such events. Deterministic safety analyses are required to provide the input that is necessary to specify the operator actions to be taken in response to some accidents, and the analyses should be an important element of the review of accident management strategies. In the development of the recovery strategies, to establish the available time period for the operator to take effective action, sensitivity calculations should be carried out on the timing of the necessary operator actions, and these calculations may be used to optimize the procedures. When the predictions of a computer code that has been used to support or to verify an emergency operating procedure do not agree with observed plant behaviour during an event, the code and the procedure should be reviewed. Any changes that are made to the emergency operating procedure should be consistent with the observed plant behaviour.

Deterministic safety analyses should also be performed to assist the development of the strategy that an operator should follow if the emergency operating procedures fail to prevent a severe accident from occurring. The analyses should be used to identify what challenges can be expected during the progression of accidents and which phenomena will occur. The analysis should start with the selection of the accident sequences that, without intervention by the operator, would lead to core damage and it should be used to provide the basis for developing a set of guidelines for managing accidents and mitigating their consequences. The measures can be broadly divided into preventive measures and mitigatory actions. Preventive measures are recovery strategies to prevent core damage. They should be analysed to investigate what actions are possible to inhibit or delay the onset of core damage. Mitigatory measures are strategies for managing severe accidents to mitigate the consequences of core melt. Possible adverse effects that may occur as a consequence of taking mitigatory measures should be taken into account.

With respect to item f) new deterministic analyses may be required to refine 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 should be taken of any margins that may have become reduced and that continue to be reduced owing to ageing over the period under consideration. Best estimate analyses together with an evaluation of the uncertainties may be appropriate to demonstrate that the remaining margins are adequate.

7. SOURCE TERM EVALUATION FOR OPERATIONAL STATES AND ACCIDENT CONDITIONS

To evaluate the source term from a nuclear power plant, it is necessary to know the sources of radiation, to evaluate the inventories of radionuclides that may occur at the plant and to know the mechanisms by means of which radioactive material can be transmitted through the plant and released to the environment.

An evaluation of the behaviour of fission products, radioactive corrosion products, activation products in coolant and impurities, and actinides following possible accidents of each type at the plant should be carried out early in the design stage. This is required to identify the most important phenomena that affect their behaviour and to identify the possible design features that could increase their retention in the plant. Source terms may be evaluated to support also software for use in emergency planning that employs theoretical source terms related to the damage to the plant to provide an early indication of what emergency measures are required. This allows decisions to be made early, before measurements of the activity levels of released radioactive material outside the plant can be made.

The levels of dose or of risk that should not be exceeded following design basis accidents should be specified in the regulatory regime under which a nuclear power plant is licensed or in the requirements of the associated environmental assessment (Ref. [1], para. 2.4). Such regulatory requirements usually become less restrictive as the frequency of the postulated accidents decreases. There are also requirements that refer to beyond design basis accidents. To demonstrate compliance with regulatory numerical limits that are expressed in terms of dose, the evaluation of the source terms should be followed by an evaluation of the radiological consequences, as described in Ref. [4]. To demonstrate compliance with a risk target, Level 1, 2 and 3 probabilistic safety analyses should be carried out.

The evaluation before a plant is operated of the source terms for normal operational states should include all the radionuclides that, owing to either liquid discharges or gaseous discharges, may make a significant contribution to doses. The evaluation of the full power activity of the reactor coolant should be made on the basis of the best operational data that are available for the particular type of nuclear power plant, the materials of the primary circuit and the chemical regime under which the plant is operated. The data should be relevant to the fuel cycles for which the activity of the primary coolant is expected to be greatest, which is normally after five years, when the activity of ^{60}Co has reached equilibrium. Thus, the source term should be calculated on the basis of a reasonably conservative value of the primary coolant activity, which may be the operational limit for the activity of the primary coolant.

The consequences associated with all identified fault conditions or accident conditions that may have an impact on physical barriers for containing radioactive material or that may otherwise give rise to radiological risks should be addressed in the safety analysis of a nuclear power plant [5]. For many types of postulated accident, the important release of radionuclides would be from the reactor core into the primary circuit and, for power reactors, from the core into the containment or the confinement system. Evaluation of the source term should thus involve determining the behaviour of the radioactive species along this route; their retention in the containment or the confinement system; their release to the secondary containment, if one is provided; and their subsequent release to the atmosphere. Separate analyses of the source term should be carried out for each type of fault for which the phenomena that would affect the source term would be different.

The evaluation of source terms should also include a comprehensive analysis of postulated accidents in which the release of radioactive material would occur outside the containment. For example, a loss of reactor coolant might involve a break in a system such as the secondary circuit that is outside the containment, and there would be a potential for the containment to be bypassed if there were a leakage path between the primary and secondary circuits. Accidents in which the release of radioactive material could bypass the containment form a very important category, because a bypass accident with a relatively small release of radioactive material from the fuel may have the same radiological consequences as an accident with a large release into the intact containment. Moreover, such bypass accidents (e.g. leaks or pipe breaks in the secondary circuit accompanied by rupture of a steam generator tube) do not allow much time for taking action to protect the public in the vicinity of the plant.

Handling accidents with irradiated fuel and spent fuel should also be evaluated. Such accidents can occur both inside and outside the containment. A fuel handling accident outside the containment may provide the bounding scenario, because if a loss of power resulted in a loss of ventilation in the fuel building, the radioactive material that would be released from the damaged fuel would leak directly to the atmosphere.

All postulated initiating events that could originate outside the plant should also be identified in the safety analysis. Examples are earthquakes, fires, floods, extreme weather conditions, volcanic eruptions, aircraft crashes, nearby industrial activities and sabotage [6]. In general, these would result in accidents similar in nature to those arising from internal events that might lead to a release of radioactive material, but the magnitude of the release may be different. For example, a release following a fire due to an aircraft crash might be much greater than releases resulting from internal fires. The main design requirements associated with protecting against external events involve designing structures, systems and components to perform their safety functions if such events were to occur.

8. CONCLUSIONS

The Safety Guide SSG-2 discusses methods for analyzing anticipated operational occurrences, design basis accidents and severe accidents to demonstrate that the safety requirements are met. Currently, the most adopted approaches to support applications for licensing are:

1. Use of conservative computer codes with conservative initial and boundary conditions (conservative analysis);
2. Use of best estimate computer codes combined with conservative initial and boundary conditions (combined analysis);
3. Use of best estimate computer codes with conservative and/or realistic input data but coupled with an evaluation of the uncertainties in the calculation results, with account taken of both the uncertainties in the input data and the uncertainties associated with the models in the best estimate computer code (best estimate analysis). The result, which reflects conservative choice but has a quantified level of uncertainty, is used in the safety evaluation.

Moreover, the Safety Guide SSG-2 focuses on thermal-hydraulic and source term evaluation for operational states and accident conditions for nuclear reactors. The quality of the analysis of computer codes and their verification and validation are also described together with the relationship of deterministic safety analysis to engineering aspects of safety and to probabilistic safety analysis.

The Safety Guide SSG-2 also addresses applications of deterministic safety analysis for the development and validation of emergency operating procedures and the determination of safety margins for modifications to nuclear power plants.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

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

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants, Safety Reports Series No. 23, IAEA, Vienna (2002).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Models for Use in Assessing the Impact of Discharges of Radioactive Substances to the Environment, Safety Reports Series No. 19, IAEA, Vienna (2001).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Control of Radioactive Discharges to the Environment, IAEA Safety Standards Series No. WS-G-2.3, IAEA, Vienna (2000).

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