BASIC PROFESSIONAL TRAINING COURSE

Module VI

Deterministic safety assessment

IAEA
International Atomic Energy Agency

International Atomic Energy Agency, May 2015

v1.0

Background

In 1991, the General Conference (GC) in its resolution RES/552 requested the Director General to prepare 'a comprehensive proposal for education and training in both radiation protection and in nuclear safety' for consideration by the following GC in 1992. In 1992, the proposal was made by the Secretariat and after considering this proposal the General Conference requested the Director General to prepare a report on a possible programme of activities on education and training in radiological protection and nuclear safety in its resolution RES1584.

In response to this request and as a first step, the Secretariat prepared a Standard Syllabus for the Post-graduate Educational Course in Radiation Protection. Subsequently, planning of specialised training courses and workshops in different areas of Standard Syllabus were also made. A similar approach was taken to develop basic professional training in nuclear safety. In January 1997, Programme Performance Assessment System (PPAS) recommended the preparation of a standard syllabus for nuclear safety based on Agency Safely Standard Series Documents and any other internationally accepted practices. A draft Standard Syllabus for Basic Professional Training Course in Nuclear Safety (BPTC) was prepared by a group of consultants in November 1997 and the syllabus was finalised in July 1998 in the second consultants meeting.

The Basic Professional Training Course on Nuclear Safety was offered for the first time at the end of 1999, in English, in Saclay, France, in cooperation with Institut National des Sciences et Techniques Nucleaires/Commissariat a l'Energie Atomique (INSTN/CEA). In 2000, the course was offered in Spanish, in Brazil to Latin American countries and, in English, as a national training course in Romania, with six and four weeks duration, respectively. In 2001, the course was offered at Argonne National Laboratory in the USA for participants from Asian countries. In 2001 and 2002, the course was offered in Saclay, France for participants from Europe. Since then the BPTC has been used all over the world and part of it has been translated into various languages. In particular, it is held on a regular basis in Korea for the Asian region and in Argentina for the Latin American region.

In 2015 the Basic Professional Training Course was updated to the current IAEA nuclear safety standards. The update includes a BPTC text book, BPTC e-book and 2 "train the trainers" packages, one package for a three month course and one package is for a one month course. The" train the trainers" packages include transparencies, questions and case studies to complement the BPTC.

This material was prepared by the IAEA and co-funded by the European Union.

Editorial Note

The update and the review of the BPTC was completed with the collaboration of the ICJT Nuclear Training Centre, Jožef Stefan Institute, Slovenia and IAEA technical experts.

CONTENTS

1 INTRODUCTION

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe the main purpose of performing safety analyses.*
2. *Identify whose responsibility is the performance of safety analyses.*
3. *Describe the main goals/outcomes of deterministic safety assessments.*

Safety analyses are analytical studies aimed at demonstrating that the safety requirements are met for all possible operating conditions of a nuclear facility, in our case of a nuclear power plant, for various postulated initiating events. They are an essential element of plant design as well as of the licensing process. In the design process, safety analyses are used to:

- confirm that the design meets all design and safety requirements,
- derive operational limits and conditions,
- establish and validate possible accident conditions and
- confirm that safety criteria which have been established to limit the risks posed by the nuclear power plant are met.

During the licensing process an independent verification of the above is necessary to assure the regulator and the public that the nuclear power plant is safe to operate.

Strictly speaking, this Module covers deterministic transient and accident analyses. The terms "safety analysis" and "safety assessment" are often used interchangeably and some languages even do not have a separate translation for each of those terms. The IAEA Safety Glossary [1] acknowledges the interchangeable use of both terms but specifies that "when the distinction is important, safety analysis should be used for the study of safety, and safety assessment for the evaluation of safety".

In this Module we do not make a distinction between these two terms and refer to these types of analyses as Deterministic Safety Analysis or Deterministic Safety Assessment (DSA) interchangeably.

The safety fundamentals publication, Fundamental Safety Principles [2], establishes the principles for ensuring the protection of workers, the public and the environment, now and in the future, from harmful effects of ionizing radiation. Safety analyses are undertaken as a means of evaluating compliance with safety principles and safety requirements for all nuclear facilities. They must be carried out and documented by the organization responsible for operating the facility, must be independently verified and must be submitted to the regulatory body as part of the licensing or authorization process. They are systematic processes that are carried out throughout the lifetime of

the facility to ensure that all the relevant safety requirements are met by the proposed or actual design.

The aim of safety analysis is to establish and confirm the design basis for the items important to safety by means of appropriate analytical tools as all design features cannot be verified experimentally. It should also ensure that the overall plant design is capable of meeting the prescribed and acceptable limits for radiation doses and releases for every plant condition.

The plant design models and data, which are the essential foundation for the safety analysis, should be kept up to date during the design phase and throughout the lifetime of the plant, including decommissioning. This is the responsibility of the designer during the design stage and of the operating organization over the life of the plant.

The safety analysis assesses the performance of the plant against a broad range of operating conditions, many of which may never be experienced in actual plant operation, in order to obtain a complete understanding of how the plant is expected to perform in these situations.

Deterministic safety assessment postulates a number of initiating events (postulated initiating events - PIEs) and simulates the response of the facility to these initiators.

Deterministic safety assessments are performed under specific predetermined assumptions concerning the initial operational state and the initiating event, with specific sets of rules and acceptance criteria. A DSA can be conservative or a best estimate.

Deterministic safety analysis mainly provides [3]:

- Establishment and confirmation of the design basis for all items important to safety;
- Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;
- Analysis and evaluation of event sequences that result from postulated initiating events;
- Comparison of the results of the analysis with dose limits and acceptance limits, and with design limits;
- Demonstration that the management of anticipated operational occurrences and design basis accident conditions is possible by automatic actuation of safety systems;
- Demonstration that the management of design extension conditions is possible by actuation of plant systems in combination with prescribed operator actions.

It is an international requirement [3], adopted in almost all national legislations that both deterministic and probabilistic safety analysis

must be used in a safety analysis of the design of nuclear power plants to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. Such analyses are an integral part of any licensing process and part of the Final Safety Analysis Report (FSAR) for every nuclear power plant.

Both types of safety analysis support safe operation of the plant by serving as an important tool in developing and confirming plant protection and control system set points and control parameters. They are also used to establish and validate the plant's operating specifications and limits (technical specifications), normal operating procedures, maintenance and inspection requirements, emergency operating procedures (EOPs), and severe accident management guidelines (SAMGs).

The safety analysis process must be highly credible, with sufficient scope, quality, completeness and accuracy to fulfil the confidence of the designer, the regulator, the operating organization and the public in the safety of the plant. The results of the safety analysis ensure with a high level of confidence that the plant will perform as designed and that it will meet all the design acceptance criteria at commissioning and throughout the life of the plant [4].

2 PLANT STATES

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe different NPP plant states.*
2. *Distinguish between normal operational states and accident conditions.*
3. *Distinguish between design basis accidents and design extension conditions.*

Plant states for nuclear power plants are specified in IAEA SSR 2/1 [3], as shown in Table 2.1. They are divided into operational states and accident conditions. Operational states include normal operation as well as anticipated operational occurrences. Accident conditions include conditions within design basis accidents and design extension conditions. In the past, design extension conditions were termed beyond design basis accident conditions. Design extension conditions include severe accident conditions, which are characterized as states with significant core degradation in which, for example, core components start to melt (as was the case for the beyond design basis accident conditions).

Table 2.1: Plant states.

Operational states		Accident conditions	
Normal operation	Anticipated operational occurrences	Design basis accidents	Design extension conditions

Normal Operation

For the plant states in Table 2.1, normal operation is defined as operation within specified operational limits and conditions. Deterministic analysis is applied to normal operation, with the aim of showing that normal operation can be carried out safely, that is with acceptable doses to workers and the public, and with acceptable planned releases. The analysis should also demonstrate that, during normal operation, plant parameters remain within acceptable limits and provide the information that is needed to establish the necessary settings for the safety and control systems, writing the operating procedures for the staff and defining the constraints that must not be exceeded when the plant is operating. The analysis must consider all aspects of normal operation such as power operation, shutdown and refuelling.

Anticipated operational occurrences

An anticipated operational occurrence (AOO) 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. Such events have the potential to challenge the safety of the plant but, because of appropriate design provisions, they do not lead to any significant fuel damage, and, therefore, no offsite consequences. Deterministic analysis is carried out to assess the response of the control and safety systems and to show the robust nature of the design. Generally, the analysis should consider uncertainties in modelling and data to demonstrate that there are adequate safety margins, even with conservative assumptions.

Anticipated operational occurrences typically include turbine trip, failure of control equipment and loss of power to the main coolant pump.

Design basis accidents

Design basis accidents (DBAs) are accident conditions against which a facility is designed according to established design criteria, and for which damage to fuel and release of radioactive material are kept within authorized limits [5].

DBAs are not expected to occur in the lifetime of the plant, but are of sufficiently high probability that they are reasonably considered as tests of the safety design of the plant. The chance of their appearance is judged to be greater than 1 % over the lifetime of the plant, even though modern designs have reduced their frequency below this value.

Examples of DBA are large coolant pipe or steam line breaks.

Design extension conditions

Deterministic analysis should also be carried out for design extension conditions (DECs) and severe accidents (SAs). DECs are defined as accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology. Such accidents are of extremely low frequency, so they have not historically been considered to be within the design basis. Some recent designs have included features to mitigate the consequences of severe accidents. The intention is to minimise or practically eliminate the need to apply counter measures to protect members of the public outside the site. The analysis of DECs is conducted using best estimate codes and data with an analysis of the uncertainties, which can be considerable. In contrast to analyses of normal operation, AOOs and DBAs, where well-defined acceptance criteria are available, no such generally accepted deterministic criteria are available for severe accidents. The principal role of deterministic analysis of DECs and SAs is to define those scenarios that will progress to SAs, and to support probabilistic analyses of the risk associated with SAs.

3 INITIATING EVENTS

Learning objectives

After completing this chapter, the trainee will be able to:

1. *List internal and external postulated initiating events (PIE) and their possible grouping.*
2. *Describe the basis for grouping of initiating events.*
3. *Distinguish among expected, possible, unlikely and remote initiating events.*

Both deterministic and probabilistic analyses start by identifying a set of Postulated Initiating Events (PIEs). A PIE is some event that disturbs the normal operation of the plant, and leads to an Anticipated Operational Occurrence (AOO) or an accident condition. PIEs may include internal events, such as equipment failures or human errors, and external events, such as earthquakes or floods.

3.1 Types of postulated initiating events

For all plant states, a comprehensive listing of postulated initiating events (PIEs) should be prepared to ensure that the analysis of the behaviour of the plant is complete. A **PIE** is defined as an **event identified in the design as leading to anticipated operational occurrences or accident conditions**. Following an initiating event, such as failure of a pump seal, a transient will occur. Depending on the transient, the safety systems and/or actions by the operator will return the plant to normal operating conditions or a safe shut down state. The sequence of events that follows the seal failure is known as an accident sequence and it is this sequence of events that is analysed in a safety analysis.

PIEs are identified using analytical methods, such as Failure Modes and Effects Analysis, analyses of operating experience with existing plants and engineering judgement.

It is useful to classify PIEs according to whether they:

- are internal to the plant, or external in origin,
- are considered to lead to an anticipated operational occurrence event, a design basis accident, or to a design extension condition, or
- occur during power operation, shutdown, refuelling, or other plant operating condition.

Internal PIEs are those that originate from within the plant, and challenge the control and safety systems provided in the design. Some events, which physically originate from off the site, such as loss-of-offsite power, are usually considered to be internal events if they

provide a challenge to internal safety systems. They usually fit into one of the following categories [6]:

- Increase or decrease in heat removal from the reactor coolant system,
- Increase or decrease in the reactor coolant flow,
- Increase or decrease in reactor coolant system pressure,
- Increase or decrease in reactor coolant inventory, including failures in the primary coolant pressure boundary,
- Reactivity and power distribution anomalies causing changes in core power operation.

In addition, events which cause the release of radionuclide from a system or component, which do not necessarily fit into one of the above categories, should be considered.

External events are usually considered to arise from outside the plant and to include both natural and man-made events. External events can lead to an internal initiating event, and in addition may disable safety equipment. Typical external events include:

- Earthquakes,
- Tornadoes, hurricanes, cyclones, fires, high or low temperatures, extreme snowfall and other severe weather conditions,
- Flooding,
- Aircraft crashes, external fires, explosions or the release of hazardous materials.

3.2 Bounding accident sequences and grouping of initiating events

After the initiating event, it is necessary to consider any plant failures that may occur as a result. This leads to the identification of a large number of possible accident sequences and it is not practicable to analyse them all. It is therefore necessary to identify a limited number of sequences for analysis that include all the others of the same type. These bounding sequences should be chosen so that, of all the sequences in their group, they provide the greatest challenge to the relevant acceptance criteria, which are discussed in Section 3.

Most safety analyses use two alternative ways of grouping postulated initiating events and their associated transients. Currently, the most common approach is to group them according to the expected frequency of the initiating events as indicated in Table 3.1. The second approach is to group them according to the frequency of the accident scenarios. The frequency of each accident scenario is usually determined by performing a probabilistic safety analysis (event trees). The frequency of each scenario is calculated by multiplying the frequency of the PIE by the availability of the safety systems appearing in the event tree. This will be further discussed in the second part of this Chapter, devoted to PSA.

Table 3.1: Possible grouping of postulated initiating events.

Occurrence (per reactor year)	Charac-teristics	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
$< 10^{-4}$ (Very unlikely to occur)	Remote	Beyond Design Basis Accident	Faulted conditions	Emergency response needed

A different grouping of initiating events and transients is more useful when calculating potential releases of radioactive material to the environment. In particular, these accidents in which major barriers such as the containment may be ineffective should be identified and it should be ensured that analyses are performed for these transients. Examples of such cases include steam generator tube ruptures as postulated initiating events or consequential events, loss of coolant accidents in the auxiliary building and faults that occur when the containment is open during shutdown.

Design extension conditions, including severe accidents, are typically treated separately in deterministic safety analyses, although some initiating events may be the same as for design basis accidents. The results help to determine the measures necessary to prevent severe accidents and to mitigate their radiological consequences if they do occur.

4 ACCEPTANCE CRITERIA

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe acceptance criteria for deterministic safety analysis.*
2. *Distinguish between basic acceptance criteria and derived acceptance criteria.*
3. *State the most widely used derived acceptance criteria for the Emergency Core Cooling Systems of LWRs.*

Basic acceptance criteria are usually defined as the limits and conditions that must be met in order to ensure an adequate level of safety. They are commonly set by the regulatory body. 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:

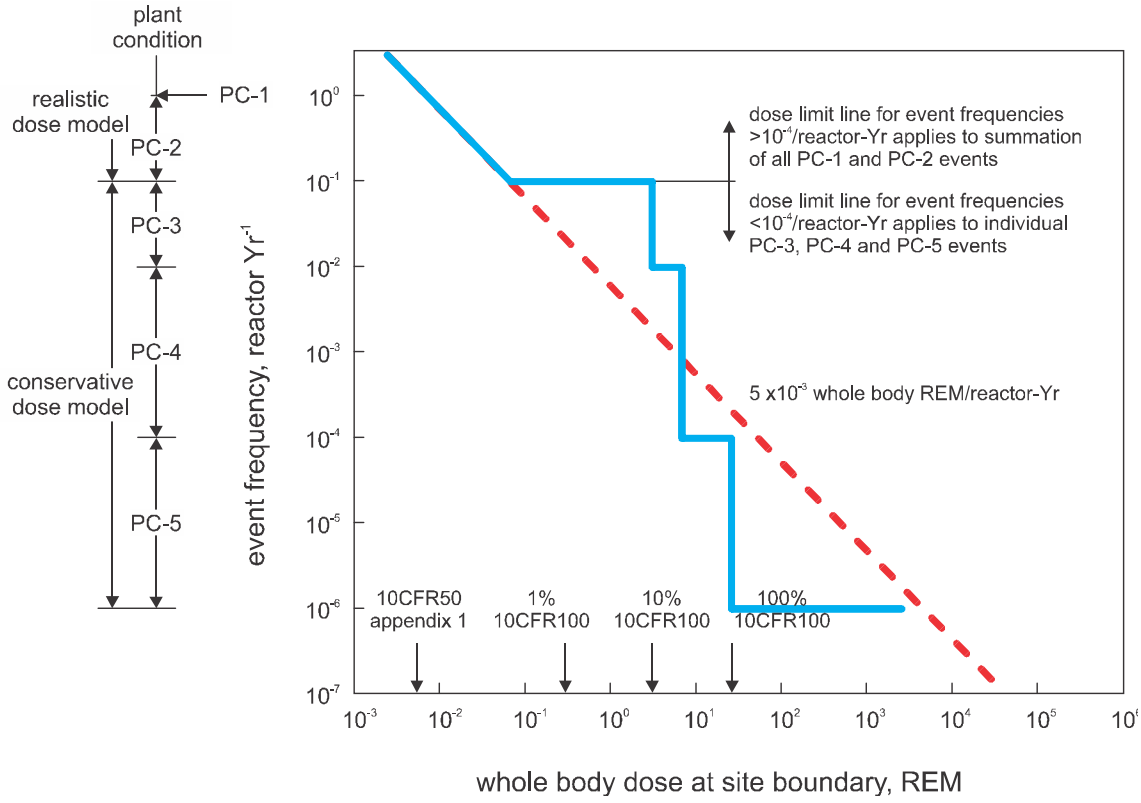
- the individual doses and collective doses to workers and the public are required to be within prescribed limits and as low as reasonably achievable (ALARA principle) in all operational states by ensuring mitigation of the radiological consequences of any accident;
- the integrity of barriers to the 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, according to the categories of the plant states for those accidents in which their integrity is required;
- the capabilities of systems that, and of operators who, are intended to perform a safety function, directly or indirectly, should be ensured for those accidents in which performance of the safety function is required;
- in some designs, early large releases of radioactive material must be practically excluded.

Basic acceptance criteria, such as radiation dose criteria, should be related to the frequency of the initiating event or initiating sequence, depending on the approach adopted. Acceptance criteria should be established for the entire range of operational states and accident conditions. Acceptance criteria should also be related to the frequency of the event. Events that occur frequently, such as anticipated operational occurrences, should have more restrictive acceptance criteria than less frequent events such as design basis accidents.

An illustration of acceptance criteria that are related to the frequency of the sequence following each Postulated Initiating Event is given in

Figure 4.1 (from ANSI/ANS 51.1).

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, which, if not exceeded, will ensure the integrity of the barrier. Examples of surrogate variables are peak cladding temperature (PCT), departure from nucleate boiling ratio (DNBR) 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.



Best estimate frequency of occurrence (F) per reactor year	Plant conditions (PC)	Offsite radiological dose criterion
Normal operation	PC-1	10 CFR 50, App.1
$F \geq 10^{-1}$	PC-2	10 CFR 50, App.1
$10^{-1} \geq F \geq 10^{-2}$	PC-3	10 % of 10 CFR 100
$10^{-2} \geq F \geq 10^{-4}$	PC-4	25 % of 10 CFR 100
$10^{-4} \geq F \geq 10^{-6}$	PC-4	100 % of 10 CFR 100

Figure 4.1: Whole body dose limits at site boundary.

Each safety related structure, system or component should be assessed

to demonstrate that it will perform according to its design function during the course of a design basis accident. In addition to demonstrating that the acceptance criteria for the surrogate variables are met, it should be shown that the acceptance criteria for each safety related component are also met. For example, for a small break loss of coolant accident, it should be demonstrated that the design criteria for the diesels are not exceeded. Compliance with the single failure criterion should be evaluated for each safety system in the plant where practicable.

Typical acceptance criteria **(derived acceptance criteria)** are:

- Numerical limits to the values of calculated variables (e.g. peak cladding temperature, fuel cladding oxidation);
- Conditions for plant states during and after an accident (e.g. limitations on power depending on the coolant flow through the core, achievement of a long term safe state);
- Performance requirements on structures, systems and components (e.g. injection flow rates);
- Requirements for operator actions, with account taken of the specific accident environment (e.g. the reliability of the alarm system and habitability in the control areas).

An example of such acceptance criteria can be found in the US NRC 10 CFR 50.46 regulation for the Emergency Core Cooling Systems (ECCSs) for Light water reactors (LWRs), addressing safety limits that must be assured under Loss of Coolant Accident (LOCA) conditions [7]:

- Maximum zircalloy cladding temperature (1204 C);
- Maximum oxidation of cladding (17 %);
- Maximum amount of hydrogen generated by chemical reaction of the zircalloy cladding with water and/or steam (1 %);
- Coolable core geometry;
- Long term cooling.

Compliance with acceptance criteria should always be demonstrated in licensing applications.

Acceptance criteria for design basis accidents may be supplemented by criteria that relate to severe accidents and other design extension conditions. These are typically core damage frequency, prevention of consequential damage to the containment, large early release frequency, probability of scenarios requiring emergency measures off the site, limiting the release of specific radionuclides such as ^{137}Cs, dose limits or risks to the most exposed individual.

5 TYPES OF DETERMINISTIC SAFETY ANALYSES

Learning objectives

After completing this chapter, the trainee will be able to:

1. *List four options available for deterministic calculations.*
2. *Distinguish between conservative and best estimate calculations.*
3. *Describe the difference between determination of the availability of safety systems in conservative and PSA based options.*

Deterministic safety analyses are calculations that are performed to describe the behaviour of a plant under a given set of conditions. These conditions include the physical description of the plant or relevant parts of it, equations that describe the relevant phenomena, information about the properties of the materials and a set of initial conditions, including the PIE in question, For a nuclear power plant, the analysis may include neutronics, reactor dynamics, radiation shielding, steady state and transient thermal-hydraulics, heat transfer in the core and in various components, fuel behaviour, and structural statics and dynamics. A number of computer codes are used to perform the calculations as described in Section 7. These codes, the analytical models used, and the plant descriptive models must be verified and validated, before being accepted for their particular application as discussed in Section 7.

The IAEA Specific Safety Guide No. 2 [5] describes the types of deterministic safety analysis. There are three alternative ways of analysing anticipated operational occurrences and design basis accidents to demonstrate that the safety requirements are met:

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 calculated 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). A conservative value of the relevant parameter, which reflects the quantified level of uncertainty, is used in the safety evaluation.

These are the first three options shown in Table 5.1.

Table 5.1: 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[1]
4. Risk informed	Best estimate	Derived from probabilistic safety analysis	Realistic input data with uncertainties[1]

Initially, AOOs and DBAs were analysed using conservative input data and codes that contained conservative models. This was mainly because of the difficulty in modelling complicated physical phenomena with a limited computer capacity and the lack of adequate data. As more experimental data become available and the capability of computer codes advanced, practice in many member states has moved towards a more realistic approach together with an evaluation of uncertainties. This is termed a best estimate approach. It has been particularly applied to the analysis of loss of coolant accidents (LOCAs).

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

- The use of conservative assumptions may sometimes lead to the prediction of an incorrect progression of events or unrealistic timescales, or it may not include 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;
- The use of a conservative approach often does not show the margins to the acceptance criteria that apply in reality and which could be taken into account to improve operational flexibility;
- 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 a more realistic comparison with acceptance criteria;
- For anticipated operational occurrences, the use of a best estimate approach together with an evaluation of the

[1]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.

uncertainties may avoid selecting unnecessarily restrictive limits and set points. In turn, this may provide additional operational flexibility and reduce unnecessary reactor scrams or actuations of protection systems.

A conservative approach has not been used to analyse design extension conditions but best estimate calculations are performed to analyse them in many states. Because of a lack of data for these infrequent events, a thorough uncertainty analysis is not always possible for these sequences, but the range of uncertainties associated with the relevant phenomena should be taken into account when determining what actions should be taken and what design features should be incorporated to prevent the core melting, failure of the reactor pressure vessel, or failure of the containment.

In principle, Options 2 and 3 in Table 5.1 are distinctly different types of analysis. However, in practice, a mixture of Options 2 and 3 is employed. This is because whenever extensive data is available the tendency is to use realistic input data, and whenever data are scarce the tendency is to use conservative input data.

Option 4 is not yet widely used. It is an attempt to combine insights from probabilistic safety analyses with a deterministic approach, which results in a risk informed safety analysis. In Options 1 – 3, the availability of safety systems is based on conservative assumptions, whereas in Option 4 the availability of safety systems is derived by probabilistic means.

6 CONSERVATIVE DETERMINISTIC SAFETY ANALYSIS

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe the purpose of conservative deterministic safety analysis.*
2. *Describe the initial and boundary conditions used in deterministic safety analyses.*
3. *Explain the importance of the single failure criterion.*
4. *Describe the technique of NPP nodalization used in deterministic calculations.*

In a conservative approach, any parameter that has to be specified for the analysis is allocated a value that will have an unfavourable effect in relation to the relevant specific acceptance criteria. In a traditional conservative analysis, both the assumed plant conditions and the physical models used are set conservatively. The intention is that such an approach will provide results that are also conservative; they bound the effect of the uncertainties. This is Option 1 in Table 5.1. Option 2 is also considered to be a conservative approach even though the models used in the computer codes are meant to be realistic.

6.1 Initial and boundary conditions

The initial conditions are the assumed values of plant parameters at the start of the transient to be analysed.

Examples of these parameters are reactor power level, power distribution, pressure, temperature and flow in the primary circuit.

The boundary conditions are the assumed values of parameters throughout the transient.

Examples of boundary conditions are the actuation of safety systems such as pumps and power supplies, leading to changes in flow rates, and external sources and sinks for mass and energy.

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.

6.2 The single failure criterion

In conservative analyses, the single failure criterion should be applied when determining the availability of systems and components. In view of their importance, safety systems that are required during AOOs or accidents must have a very high level of reliability. For the design of safety systems the **single failure criterion** means that **safety related systems must be able to fulfil their function in an adequate manner even in the event of failure of any one of their components**. A failure should be assumed in the system or component that would have the largest negative effect on the calculated safety parameter.

When applying the criterion to electrical systems, it is postulated that at the moment a system is actuated a single component is faulty. The component selected is that with the most serious consequences. For mechanical systems, active components for which correct operation requires external actuation (pumps, valves, power-assisted check valves) are differentiated from passive components (pipes, heat exchangers, simple check valves, etc.). An active failure might consist of **a failure to operate or inadvertent operation of a component**. A passive failure could be a worsening leak or the blocking of flow through a system.

6.3 Common cause and consequential failures, loss of off-site power, operator actions

All the common cause and consequential failures associated with the postulated initiating event should also be included in the analysis in addition to the single failure. Furthermore, unavailability due to on-line maintenance should be considered if this is permitted in the plant operating procedures.

In addition to the postulated initiating event itself, a loss of off-site power should be considered when analysing design basis accidents and anticipated operational occurrences. For such cases, the assumption that gives the most negative effect on the limits of the acceptance criterion should be chosen. Likewise, equipment that is not qualified for specific accident conditions should be assumed to fail unless its continued operation results in more unfavourable conditions. The malfunction of control systems and delays in the actuation of protection systems and safety systems should be taken into account in the analysis. For such systems, the issue of whether their continued functioning leads to more unfavourable conditions than their non-availability should be addressed.

For design purposes, credit should not be taken for operator action to limit the evolution of a design basis accident or anticipated operational occurrence within a specified time. Exceptionally, the design may take credit for earlier operator action but, in these cases, the actuation times should be conservative and should be fully justified. Conservative assumptions should be made with respect to the timing of operator actions. It should be assumed that in most cases post-accident recovery actions would be taken by the operator.

6.4 Nodalization, plant modelling and large break LOCA analysis

In a thermal-hydraulic code, the reactor plant is described in terms of discrete volumes or nodes. Normally, but not always, the more nodes that are used, the more accurate is the representation of the plant. However with an increasing number of nodes, the time to perform the calculation also increases. In some cases, the results produced by a conservative analysis are sensitive to decisions made by the user about the number and structure of nodes that are used. User effects such as this could be particularly large for a conservative analysis for which the 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.

Over the years, the DBA that has drawn the most attention is the **large-break loss-of-coolant accident (LBLOCA)** and its historical analysis typifies the conservative approach. This accident is the limiting design basis accident for the emergency core cooling systems (ECCS) and the containment buildings for most current light-water reactors. In the USA, the RELAP5 and TRAC codes were both developed under the auspices of the USNRC to analyse this DBA, and the RETRAN code was developed by EPRI for utility use. In addition, reactor designers have their own proprietary codes. Development of the codes was supported by numerous experiments, among them being the loss-of-fluid tests (LOFT) and semi-scale experiments conducted in the 1970s and 1980s. The analysis includes consideration of blowdown of the primary system following the postulated pipe break, followed by reflood of the core by the ECCS, and finally long-term cooling by recirculation of water within the containment. The deterministic analysis is aimed at showing compliance with limits of a maximum cladding temperature of 1204°C and a maximum oxidation of less than 17% of the cladding thickness. The LBLOCA analysis is a classical illustration of deterministic safety analysis.

7 BEST ESTIMATE PLUS UNCERTAINTY (BEPU) ANALYSIS

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe the use of the best estimate approach.*
2. *Describe the concept of safety margins.*
3. *List several widely used computer codes for deterministic calculations.*

7.1 Best estimate approach

The disadvantages of using a conservative approach have been described in the previous Section. In addition, it is not always easy to determine what assumptions will lead to a conservative result, and thus some calculations that were thought to be conservative might not be. For example, the assumption of a high core power level may lead to high levels of the steam–water mixture in the core in the case of a postulated small break loss of coolant accident (SBLOCA). Consequently, the calculated peak cladding temperature may not be conservative. As another example, the assumption that reduced interfacial shear between water and steam may lead to higher cladding temperatures in the upper core region is conservative. However, this conservative assumption will lead to an optimistic estimate for the refilling/reflooding time, as it will appear that more water remains in the primary cooling system than is actually the case.

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 the acceptance criteria. This type of analysis is referred to as a **best estimate plus uncertainty (BEPU) approach** and is Option 3 in Table 5.1. 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 margins existing between the results of calculations and the acceptance criteria; this information can be used to obtain more power from the reactor.

For a best estimate analysis, a best estimate code should be used that realistically describes the behaviour of physical processes in a component or system. This requires sufficient data to be able to ensure that all the important phenomena have been taken into account in the modelling, or that their effects are bounded as discussed below. Establishing that all the important phenomena have been taken into account in the modelling or that their effects are bounded should be part of the validation programme. Uncertainties in the results due to unavoidable approximations in the modelling should be quantified (or

bounded) using experimental results.

In order to establish the effect of uncertainties, it is necessary to perform a number of computer runs for different values of the critical parameters. The overall uncertainty is based on statistically combining the uncertainties due to different plant conditions and code models in order to establish, with a specified high probability, that the calculated results do not exceed the acceptance criteria. It is common practice to provide assurance that the applicable acceptance criteria for a plant will not be exceeded with a probability of 95% or more. A probability of 100 % (i.e. certainty) cannot be achieved because only a limited number of calculations can be performed. The basis for selecting the 95% probability level is primarily to be consistent with standard engineering practice in regulatory matters. However, national regulations may require a different level of probability that the applicable acceptance criteria will not be exceeded.

Some parameters, such as departure from the nucleate boiling ratio in pressurized water reactors, or the critical power ratio in boiling water reactors, have been found to be acceptable at the 95% probability level. Techniques may be applied that use additional confidence levels, e.g. 95% confidence levels, with account taken of the possible sampling error due to the fact that a limited number of calculations have been performed. This leads to so-called (95/95) results, meaning a 95% probability and a 95 % confidence level.

The uncertainty in parameters associated with the results of a computer code may be determined with the assistance of a phenomena identification and ranking table (PIRT) for each event that is analysed. This is a process in which several experts perform evaluations to rank the importance of different phenomena for the scenarios that are being considered. The ranking should identify the most important phenomena for which the suitability of the code has to be assured and should be based on the 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.

A specific phenomena identification and ranking table should be developed for each event for which a computer code or methodology is used. Accidents of different types, such as large break loss of coolant accidents, small break loss of coolant accidents and transients, develop as a result of different phenomena and therefore require specific phenomena identification and ranking tables.

An alternative to relying completely on expert judgement in an analysis made on the basis of a PIRT is to use a statistical method. Statistical methods are increasingly being used to provide information on the ranking of parameters.

The conservative Options 1 and 2 have been used since the early days of civil nuclear power and are still widely used today. However, the desire to utilise current understanding of important phenomena and to maximise the economic potential of nuclear plants without compromising their safety has led many countries to use Option 3, i.e. to use best estimate codes and data together with an evaluation of the uncertainties.

Using the Best Estimate plus Uncertainty (BEPU) approach leads to the distribution of code predictions/results for the most limiting value of the safety variable (for example the peak clad temperature during a transient). This distribution is a consequence of uncertainties in the initial and boundary conditions as well as in the computer model.

On the other hand, the distribution of failures is a consequence of the fact that failures are random and our knowledge of the precise phenomena that can cause a failure is limited.

Assuming that both distributions (of code predictions and of actual failures) follow a Gaussian distribution leads us to the concept of the licensing margin, as illustrated in Fig. 7.1.

In this figure the total margin (sometimes also defined as the safety margin) is the range between the two dotted lines; the left one representing the 95/95 value of the calculated results, and the right one the start of the non-negligible failure probability.

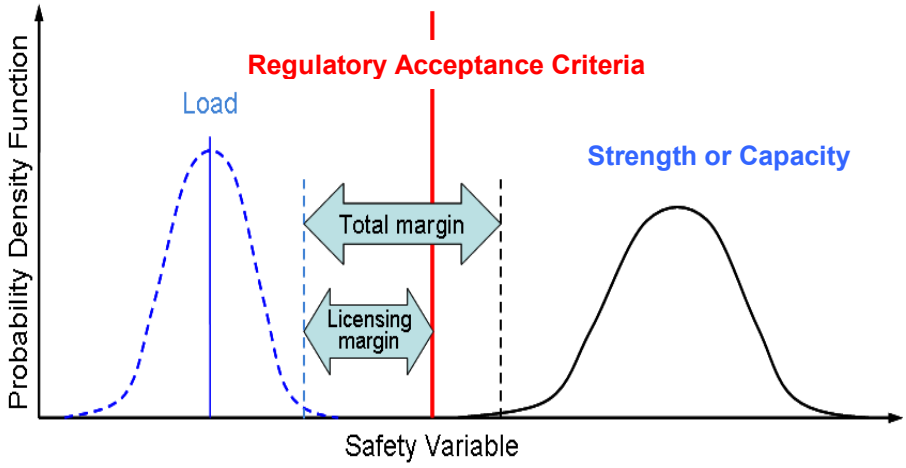


Figure 7.1: Probability densities for load and strength /capacity.

In order to illustrate the way in which the available licensing margin is expected to increase as one goes from Option 1 to Option 3, we compare the results of a single calculation for Option 3 with the results of calculations using Options 1 and 2. This is illustrated in Figure 7.2.

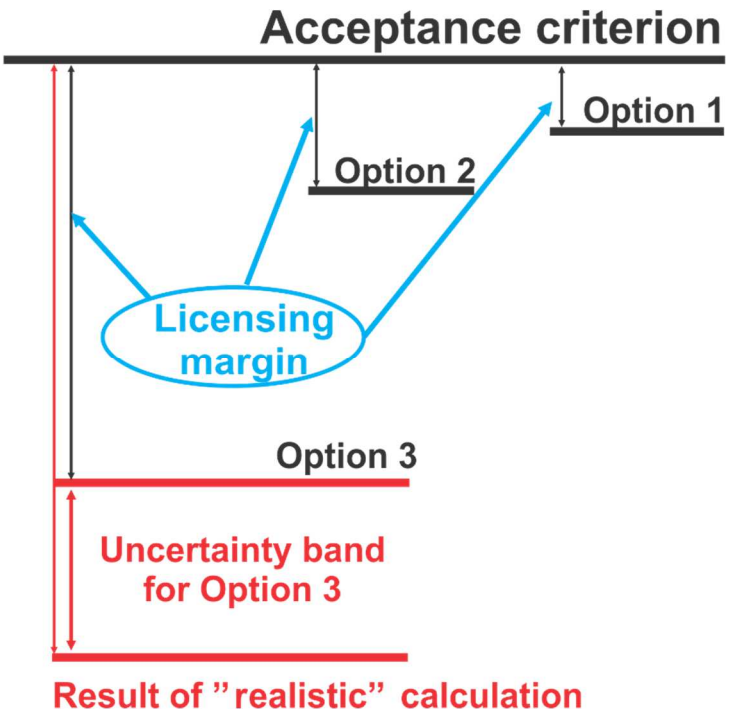


Figure 7.2: Illustrative licensing margins for different options.

However Option 3 includes a detailed evaluation of the uncertainties, and therefore several calculations are performed to obtain the uncertainty distribution. The Safety Guide SSG 2 [5] recommends that the value that should be compared with the acceptance criterion is the value that encompasses 95% of the range of uncertainty with a 95% confidence level (The 95/95 value). This is illustrated in Figure 7.3.

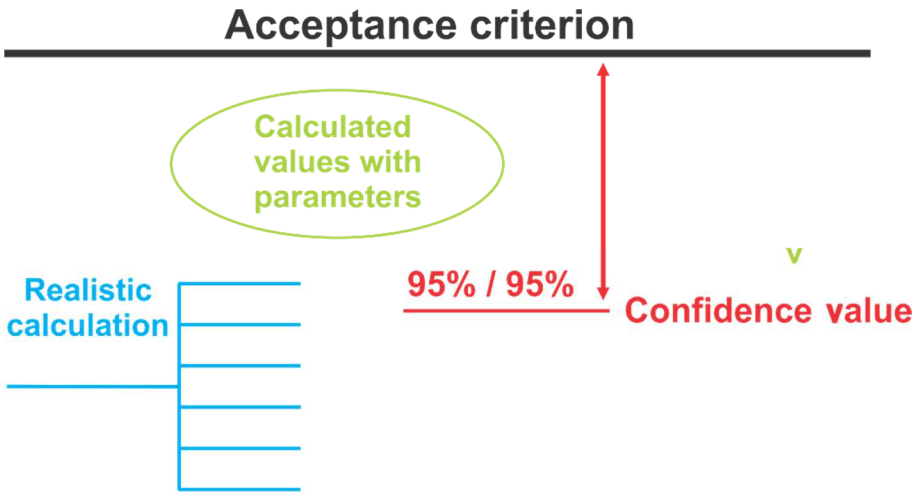


Figure 7.3: Illustrative design margin for Option 3.

7.2 Best estimate computer codes

A best estimate calculation uses modelling in an attempt to realistically describe the physical processes that occur in a nuclear power plant. The key issue in using a best estimate approach, therefore, is the availability of computer codes that can be used to realistically model the important phenomena and to simulate the behaviour of the plant systems. The codes that are capable of meeting these requirements are termed best estimate computer codes.

Best estimate computer codes have various levels of qualification, for reasons such as the different levels of availability of experimental data or operational data, and the extent of independent assessment of such data. An extensive database is therefore needed for comparison with the results obtained by the code that is used for design and licensing in order to establish confidence in the use of that code.

For best estimate analyses, the following classes of codes are available:

- System thermo-hydraulic codes,
- Core physics codes,
- Structural analysis codes,
- Component-specific or phenomenon-specific codes,
- Computational fluid dynamics codes,
- Coupled codes.

System thermo-hydraulic codes

The class of **system thermo-hydraulic codes** includes those computer codes (computational tools) that are capable of modelling the primary system, the interface with the secondary system, the containment or the confinement system, and other plant systems that are important to safety.

Development of these codes began in the 1970s and has continued ever since. Originally they contained conservative modelling of the phenomena that occur during operational states and accidents, but in recent years code developers in France, Germany and the USA have developed and validated best estimate codes. As well as using many large and small experimental facilities for their validation, confidence in these codes has been established by comparing the results that they produce for the same transient [8]. The validation of codes is discussed further in Section 9.

Among the commonly used codes are ATHLET (Germany) [9], CATHARE (France) [10], RELAP5 (USA) [11, 12] and TRACE (USA) [13].

Other codes

The class of **'core physics codes'** includes computational tools that

are specialized for performing detailed core physics calculations, including calculations of the neutron flux, of the detailed power distribution (two dimensional or three dimensional), criticality, long term burn-up, fuel management and refuelling calculations.

Structural analysis methods and codes must address a wide variety of problems, both static and dynamic. Some of these problems include:

- Static calculations of stresses in piping and pressure containing components under various normal, anticipated operating occurrence (AOO), design basis accident and design extension conditions.
- Dynamic calculations of stresses and displacements due to phenomena such as flow induced vibration, pipe whip in pipe break accidents, and water hammer events.
- Calculations of piping motion and stresses, and calculation of equipment response in earthquakes, including the effects of seismic restraints.

Structural analysis methods and data are more extensively codified than is the case for most other areas. The ASME Boiler and Pressure Vessel Code provides rules and guidance for many calculations used in nuclear design and operation, including quality assurance and in-service inspection requirements. The American National Standards Institute (ANSI) B31.1 Code for power piping provides design rules and guidance for the various piping systems used in power plants. Many well-known commercially available finite difference and finite element computer codes are available to perform the required static calculations. Similarly, numerous structural dynamic finite element computer codes have been developed, but are somewhat more specialized in nature and less generally available.

The class of **'component-specific or phenomenon-specific codes'** includes computational tools that are specialized in the evaluation of the steady state or transient performance of components of the nuclear steam supply system, such as fuel rods, reactor core, pumps, valves or heat exchangers, or of individual phenomena such as critical heat flux, fuel heat-up following reactivity excursions, dynamic loads on components associated with the occurrence of breaks and pressure wave propagation.

Computational fluid dynamics codes are used to solve equations for the conservation of mass, momentum and energy for different media with a high level of detail. The codes are typically used to model multi-component distribution and mixing phenomena. Although these codes were originally developed to model one-phase flow in non-nuclear applications, there are many examples of their use in safety analyses. Development to extend computational fluid dynamics codes to two-phase flow regimes is ongoing.

Coupled codes include those computational tools that are formed by the combination of codes belonging to two or more classes. Examples of coupled codes are codes that combine three-dimensional neutron kinetics and system thermo-hydraulics, or pressurized thermal shock codes, which combine thermo-hydraulics, stress analysis and fracture mechanics.

The quality of best estimate codes should be ensured when they are used for designing and licensing. Validation and verification are essential steps in qualifying any computational method as discussed in this Section.

8 SENSITIVITY AND UNCERTAINTY ANALYSIS

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Distinguish between sensitivity and uncertainty analyses.*
2. *Explain the importance of performing uncertainty and sensitivity analyses.*
3. *Distinguish between epistemic and aleatory uncertainties.*
4. *Describe the concept of the use of single failure criteria with coincident loss of off-site power in determination of the availability of safety systems.*

A sensitivity analysis includes a systematic variation of the individual code input variables and the individual parameters that are used in models, to determine their influence on the results of the calculations.

An uncertainty analysis addresses the uncertainties in the code models, in the plant model and in the 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.

Two different kinds of uncertainties, **epistemic** uncertainties and **aleatory** uncertainties should be distinguished and they should be treated separately.

Epistemic uncertainty occurs because of imperfect knowledge or incomplete information. The parameters that are uncertain have a definite but not precisely known value. Epistemic uncertainty is directly addressed by uncertainty analysis and sensitivity analysis of the results obtained by deterministic as well as probabilistic computational models. Such analyses quantify the uncertainty associated with the result of a computation and identify the principal sources of this uncertainty.

Aleatory uncertainty represents the unpredictable random performance of the system and its components and values of plant parameters (e.g. the primary circuit pressure and temperature). The random failure of equipment is an example. Variables that are subject to aleatory uncertainty are random in nature.

Methods for performing uncertainty analysis have been published, such as [14]. These include:

- a combination of expert judgement, statistical techniques and sensitivity calculations;
- use of scaled experimental data;
- use of bounding scenario calculations.

The large number of parameters that are normally used in performing safety analyses contribute to the uncertainties in the results of these calculations. Most methods for quantifying the uncertainty of results rely on identifying the input parameters that are considered to be uncertain. The input uncertainties are quantified by determining the range and distribution of possible values of the model parameters. If this is not feasible, conservative values should be used. This should be performed for each phenomenon that is important to the analysis.

The evaluation of uncertainties is an essential element of using best estimate calculations to analyse operational states and accident scenarios. The need for quantifying the uncertainties in predictions made using computer codes comes from the unavoidable approximations that are made in the modelling, including an inadequate knowledge of the magnitude of a number of input parameters. The uncertainties in the results should therefore always be provided when a best estimate approach is used for a deterministic analysis. This evaluation of the uncertainties should include the uncertainties due both to the models and to the numerical methods used. The combined effect of both uncertainties can be evaluated using experimental data or by comparison with validated codes.

8.1 Initial and boundary conditions

A plant input model should be used to define the status of the initial conditions and boundary conditions of the plant, and the availability and performance of equipment. These conditions include the initial power, the pump performance, the valve actuation times and the functioning of the control systems. Uncertainties associated with the initial conditions and boundary conditions, and the characterization and performance of equipment should be taken into account in the analysis. It is acceptable to limit the variability to be considered by setting the values of the initial conditions and boundary conditions to conservative bounds. Setting the variability to conservative bounds is one way of not combining two different kinds of uncertainties, namely epistemic uncertainties and aleatory uncertainties.

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 initial conditions for the safety analysis of a loss of coolant accident are presented below. The following unfavourable deterministic requirements may also be valid in a ‘best estimate’ approach:

- Most unfavourable single failure;
- If unavailability of a system/equipment due to preventive maintenance during operation is allowed, this should be included in the analysis;
- Most unfavourable break location;

- 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;
- Loss of off-site power;
- Initial core power should be specified for the most unfavourable conditions and values that may occur in normal operation, with account taken of the set-points for integral power and power density control;
- Conservative values for the reactivity feedback coefficients;
- Time within the fuel cycle, i.e. beginning of cycle, end of cycle, burn-up;
- The values of thermo-hydraulic parameters such as pressure, temperature, flow rates and water levels in the primary circuit and secondary circuit that result in the shortest time to uncover the core;
- Temperature conditions for the ultimate heat sink;
- The rod which has the greatest effect on reactivity is assumed to be stuck (in certain reactor designs).

Initial conditions that cannot occur in combination should not be considered when performing a realistic analysis. For example, the limiting decay heat and the limiting peaking factors cannot physically occur at the same time, but they are assumed to do so in a conservative analysis.

Availability of systems, single failure criterion and loss of off-site power

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.

9 VERIFICATION AND VALIDATION OF COMPUTER CODES

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe the process of computer code verification and validation.*
2. *Distinguish between the concepts of validation and verification.*

All the computer codes that are used to perform deterministic safety analyses for nuclear power plants should be verified and validated. **Verification means** that the **numerical calculations performed by the code are carried out as intended**. **Validation means** that the **results of calculations performed by the code are sufficiently accurate** when compared with the results of experiments representing the conditions that the code is analysing. An important aspect of validation is determining the accuracy of the results produced by the code. Thus, computer codes should be validated for all the applications in which they will be used to support the design and licensing of nuclear power plants.

The management process ensuring that computer codes have the required quality is carried out by procedures that address the entire lifetime of the code including its production, verification, validation and the continuous process of maintaining it and correcting errors.

It is impracticable to perform full size experiments for all the accident conditions that are analysed in the safety analysis. Thus, different types of experiment are performed. These include:

- **Separate effect experiments:** These experiments involve a phenomenon that may occur at a nuclear power plant, but not others that may occur at the same time. Thus, they can only be used to validate the ability of the code to represent one phenomenon and other experiments have to be performed to address the others.
- **Integral experiments:** These experiments are directly related to a nuclear power plant and all the important phenomena are represented. These are the most powerful way of validating the codes that are used to analyse accidents. A well-known example is the LOFT facility that was used to validate codes that analyse a large break loss of coolant accident (LOCA).
- **Tests on nuclear power plants and operational transients:** These situations only address relatively small variations from normal operation in contrast to accidents, but they provide valuable data to test that the way the plant is modelled in the computer code is adequate. This includes issues such as the number of nodes that are used.

As a typical example, the validation of the thermal hydraulic code CATHARE involved comparing its calculations with 135 separate

effect experiments, which were carried out at 14 different facilities, and comparison with the results of integral experiments in the LOFT, PKI, BETHSY and LOBI facilities.

Codes have been validated by comparing their results with those of other codes that have been validated. This process is known as benchmarking.

10 APPLICATION OF DETERMINISTIC SAFETY ANALYSIS

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe the use of deterministic safety analysis in the design of NPPs.*
2. *Describe the use of deterministic safety analysis in the licensing of NPPs.*
3. *Describe the use of deterministic safety analysis in the assessment of safety analysis reports for NPPs.*
4. *Describe the use of deterministic safety analysis in the analysis of operational events at NPPs.*
5. *Describe the use of deterministic safety analysis in the development of EOPs and SAMGs for NPPs.*
6. *Describe the use of deterministic safety analysis in the context of a periodic safety review.*

10.1 Areas of application

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

- Design of nuclear power plants. Such analyses require either a conservative approach or a best estimate analysis together with an evaluation of uncertainties.
- 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. For such applications, in many countries, but not all, conservative approaches and best estimate plus uncertainty methods may be used.
- The assessment by the regulatory body of safety analysis reports. For such applications, in many countries, but not all, conservative approaches and best estimate plus uncertainty methods may be used.
- The analysis of incidents that have occurred or of combinations of such incidents with other hypothetical faults. Such analyses would normally require best estimate methods, in particular for complex occurrences that require a realistic simulation.
- The development and maintenance of emergency operating procedures and accident management procedures. Best estimate codes together with realistic assumptions should be used in these cases.
- The 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. As with the original analyses, both conservative approaches and best estimate plus

uncertainty methods may be used.
- By the Regulatory Body to provide independent oversight of licensee activities.

Application to the design of nuclear power plants

The design basis for items that are important to safety must be established and confirmed by means of a comprehensive safety assessment [3]. The design basis comprises the design requirements for structures, systems and components that must be met for the safe operation of a nuclear power plant, and for preventing or mitigating the consequences of events that could jeopardise safety. For example, deterministic analyses are carried out to determine what pressure and temperature the components of the primary coolant system must be able to withstand.

Application to the licensing of nuclear power plants

The use of deterministic safety analyses to develop the design, and to license a nuclear power plant, are closely related. The plant must be designed so that it complies with all the applicable regulations and standards and this must be demonstrated in safety analysis reports in order to obtain licenses to construct and operate the plant. The analyses that are presented in the safety analyses reports should represent the current state of the design and should be presented in a way that demonstrates to the regulatory body that its requirements have been met.

Application to the assessment of safety analysis reports

The operating organisation must ensure that an independent verification of the safety assessment is performed by individuals or groups separate from those carrying out the design, before the design is submitted to the regulatory body [3]. Additional independent analyses of selected aspects may also be carried out by or on behalf of the regulatory body.

Application in plant modifications

The modification of existing nuclear power plants is normally undertaken to counteract the ageing of the plant, to justify its continued operation, to take advantage of developments in technology, or to comply with changes to the applicable rules and regulations. To comply with the regulatory requirements, 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 are made in operating procedures owing to operational experience.

Other important applications of deterministic safety analysis are aimed at the more economical utilization of the reactor and the nuclear fuel. Such applications encompass up-rating 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.

Application to the analysis of operational events

The analysis of actual events that have occurred in operating nuclear power plants is a very important way of establishing the extent to which the deterministic analysis that has been performed accurately represents the behaviour of the plant. Such analyses should form an integral part of the feedback from operational experience. Operational events may be analysed with the following objectives:

- To check the adequacy of the selection of postulated initiating events;
- To determine whether the transients that have been analysed in the safety analysis report adequately describe 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.

The analysis of operational events requires the use of a best estimate approach. Actual plant data should be used. If there is a lack of detailed information on the plant status, sensitivity studies, with the variation of certain parameters, should be performed.

Application to the development and validation of emergency operating procedures (EOPs)

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.

After the emergency operating procedures have been developed, a validation analysis should be performed. This analysis is usually performed using a qualified simulator.

Application to the development of severe accident management guidelines (SAMGs)

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 carried out by using one or more of the specialized computer codes that are available to model relevant physical phenomena. For light water reactors, these include thermo-hydraulic effects, heating and melting of the reactor core, the retention of the molten core in the lower plenum, molten-core–concrete interactions, steam explosions, hydrogen generation and combustion, and fission product behaviour.

Periodic safety reviews

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 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.

11 QUESTIONS

1. What is the main purpose of performing deterministic safety assessments?
2. Who is responsible for the performance of deterministic safety assessments?
3. What is the main goal of deterministic calculations?
4. Name different NPP plant states.
5. What is the difference between design basis accidents and design extension conditions?
6. Name two broad categories of postulated initiating events (PIEs)!
7. Describe one possible grouping of PIEs!
8. What is the difference between basic and derived acceptance criteria for deterministic safety analyses?
9. Give an example of derived acceptance criteria for ECCS for LWR as defined in US NRC 10 CFR 50.46 regulation.
10. Describe briefly the different types of deterministic safety analysis.
11. What is the safety (or licensing) margin?
12. What is the difference between sensitivity and uncertainty analysis?
13. What are epistemic and aleatory uncertainties?
14. Describe the concept of the use of single failure criteria with coincident loss of off-site power for determination of the availability of safety systems.
15. Name a few applications of deterministic safety analysis.

12 REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Terminology Used in Nuclear Safety and Radiological Protection 2007, IAEA Safety Glossary, IAEA Vienna (2007).

[2] 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).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plant, Specific Safety Requirements SSR-2/1, IAEA, Vienna (2012)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Guide NS-G-1.2, IAEA, Vienna (2001).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Specific Safety Guide No 2, IAEA Vienna (2009).

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

[7] US NUCLEAR REGULATORY COMMISSION, Domestic Licensing of Production and Utilization Facilities, 10 CFR 50.46, Washington, DC (1974).

[8] STEINHOFF, H.G., TESCHENDORFF, F., Comparison of Thermal-Hydraulics Safety Codes for PWR Systems, Publication No. EUR 11522, Graham & Trotman, London (1988).

[9] LERCHL, G., AUSTREGESILO, H., ATHLET Mod 1.2 Cycle A, User's Manual, GRS-P-1/Vol. 1, (1998).

[10] CATHARE References: User's manual of CATHARE, Dictionnary of operators and directives, General description, Equipe CATHARE, Centre d'études nucléaires de Grenoble, STR/LML (2006).

[11] RANSOM, V.H., et al., RELAP 5/MOD 2 Code Manual, Volume 1: Code Structure, System, Models, and Solution Methods, NUREG/CR 4312, EGG-2396, Washington, DC (1985).

[12] RANSOM, V.H., et al., RELAP 5/MOD 2 Code Manual, Volume 2: Users Guide and Input Requirements, NUREG/CR 4312, EGG-2396, Washington, DC (1985).

[13] LILES; D.R., et al, TRAC-PFl/MOD 1: An advanced best-estimate computer program for pressurized water reactor

thermal -hydraulic analysis, LA-10157-MS, NUREG/CR, Los Alamos National Laboratory (1986).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, Safety Report Series No. 52, Vienna (2008).

The views expressed in this document do not necessarily reflect the views of the European Commission.