Module V

Safety classification of structures, systems and components
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.
1 INTRODUCTION TO SAFETY CLASSIFICATION

Learning objectives
After completing this chapter, the trainee will be able to:
1. Define the purpose of safety classification.
2. List important general safety requirements for plant design.
3. Explain which items are important to safety.
4. Define items important to safety and the safety system.
5. List and explain the purpose of defence-in-depth (DiD) levels.

All presently operating NPPs have been designed and built with some sort of safety classification of their structures, systems and components (SSCs).

1 The functions to be categorized are those required to accomplish the main safety functions for the different plant states and primarily those included in the safety analysis.

This ensures that the appropriate engineering design rules are determined for each safety class, so that SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to standards appropriate to their safety significance.

This Module describes the present requirements agreed by consensus for the classification of SSCs which have a role in the nuclear safety of the plant. It describes a systematic approach to identifying and categorizing the functions\(^1\) to be considered in the classification process, to identifying the SSCs which have a role in performing those functions, and to classifying the SSCs in a manner commensurate with their importance for their function and category. Finally it describes how design requirements, such as design codes and standards, are set up for each safety class and gives some examples of the SSC classification in existing designs.

To ensure adequate safety, the following general safety requirements for the plant design are important:

- To control the reactivity of the reactor;
- To have the capability to safely shut down the reactor and to maintain it in the safe shutdown condition during and after normal and abnormal operation, design basis accident conditions and selected beyond design basis accidents (also named design
extension conditions);

- To remove heat from the core;
- To remove residual heat from the core after reactor shutdown following normal or abnormal operation, design basis accident conditions and selected beyond design basis accidents;
- To remove residual heat from the spent fuel storage;
- To confine radioactive material and control operational discharges and thereby reduce the potential for the uncontrolled release of radioactive materials;
- To assure that any releases are within prescribed limits during and after operational states and within acceptable limits during and after accident conditions.

These requirements include safety functions necessary to prevent accident conditions and safety functions necessary to mitigate the consequences of accidents, should they occur. Safety Requirements SSR 2/1 sets the safety classification of plant equipment (Fig. 1.1). In this context “items” are different structures, systems or components.

**Fig. 1.1:** Safety classification of the plant equipment.
A set of design extension conditions (DEC) [1] is derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant’s capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions are used to identify the additional accident scenarios to be addressed in the design, and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur.

All SSCs necessary for the accomplishment of the safety categorized functions, including SSCs belonging to their supporting systems, must be first identified and then classified on the basis of their function and significance with regard to safety. They must be designed, constructed and maintained such that their quality and reliability is commensurate with this classification.

The method for classifying the safety significance of an SSC must primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment, with account taken of factors such as:

- The safety function to be performed by the SSC;
- The consequences of failure to perform its function;
- The probability that the SSC will be called upon to perform a safety function;
- The time following a Postulated Initiating Event (PIE) at which, or the period throughout which it will be called upon to operate.

 Appropriately designed interfaces must be provided between SSCs of different classes to ensure that any failure in a system classified in a lower class will not propagate to a system classified in a higher class.

Safety classification of SSCs, and corresponding applicable codes and standards, are based on national approaches. Present national approaches are in general compliance with IAEA SSR 2/1 and SSG...
1.1 Identification of safety functional groups and allocation to defence-in-depth levels

Functions should be allocated to each of the five Defence-in-Depth (DiD) levels (the details are subject of Module 3), so that the relevant success criteria of the function can be achieved (Fig. 1.2).

---

**Fig. 1.2:** Safety functions in relation to the Defence in Depth levels.
1.2 Questions

1. What is the purpose of the safety classification?
2. Which general safety requirements for plant design are important to ensure adequate safety?
3. How is the plant equipment classified?
4. How do we define items that are important to safety?
5. What is the definition of a safety system?
6. What are design extension conditions (DEC)?
7. What is the basis for classifying the safety significance of an SSC?
8. What is the main purpose of each defence-in-depth (DiD) level?
2 SAFETY CLASSIFICATION

Learning objectives
After completing this chapter, the trainee will able to:
1. Explain when and how safety classification should be performed.
2. List the main steps in the classification process.
3. Define the terms functions and design provisions.
4. List examples of design provisions.
5. List and briefly explain the three levels of severity.
6. List the categorization of functions.
7. Describe the three safety categories.
8. Explain how the adequacy of the safety classification should be verified.

The categorization of functions recommended in the IAEA Specific Safety Guide SSG 30 [2] is based on three safety categories. On the basis of their classification, SSCs are designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained in accordance with established processes that ensure that the design specifications and the expected levels of safety performance are achieved.

Safety classification is an iterative process that should be carried out periodically throughout the design process and maintained throughout the lifetime of the plant.

Safety classification should be performed during the plant design, system design and equipment design phases.

It should be reviewed for any relevant changes during construction, commissioning, operation and subsequent stages of the plant’s lifetime.

The first step in the classification process is a basic understanding of the plant design, its safety analysis and how the main safety functions are achieved (Fig. 2.1). Using information from the safety assessment (the analysis of postulated initiating events), the functions are categorized on the basis of their safety significance. The SSCs belonging to the categorized functions are identified and classified on the basis of their role in achieving the function.

An SSC implemented as a design provision should be classified directly, because the significance of its postulated failure fully defines its safety class without any need for detailed analysis of the category of the associated safety function.

The process for classifying all SSCs according to their safety significance should take into account:
- The plant design and its inherent safety features;
- The list of all postulated initiating events.

**Fig. 2.1:** Flowchart of the classification process.

All functions and design provisions necessary to achieve the main safety functions for the different plant states, including all modes of normal operation, should be identified.

The functions should be classified into a limited number of categories on the basis of their safety significance, using an approach which takes into account three factors:

- **The consequences of failure** to perform the function;
- **The frequency of occurrence of the postulated initiating event** for which the function will be called upon;
- **The significance of the contribution of the function** in achieving either a controlled state or a safe state.
The next step in the process is to determine the safety classification of all SSCs important to safety. Deterministic methodologies should be applied, complemented where appropriate by probabilistic safety assessment and engineering judgment to achieve an appropriately low risk, i.e. a plant design for which events with high consequences have a very low predicted frequency of occurrence. The process of safety classification of SSCs important to safety are presented in Fig. 2.2.

From Fig. 2.2 we can see that design provisions are primarily implemented to decrease the probability of an accident occurring and functions to make the consequences acceptable with regard to its probability.

For most initiating events, a combination of both preventive and mitigation measures is implemented to decrease their frequency of occurrence and then to make their consequences acceptable and as low as reasonably practicable.

The implementation of functions to limit the consequences of an event
may not be necessary provided the consequences without any mitigation are acceptable, or the probability of their occurrence is so low that their mitigation is not required.

The efficiency of preventive and mitigation measures depends on the overall dependability of items of equipment, which is itself driven by the classification.

2.1 Identification of functions and design provisions

The term ‘function’ includes the primary function and any supporting functions that are expected to be performed to ensure the accomplishment of the primary function.

The functions to be categorized are those functions required to achieve the main safety functions for the different plant states, including all modes of normal operation.

These functions are primarily those that are included in the safety analysis and should include functions performed at all five levels of defence in depth:

- Prevention;
- Detection;
- Control and mitigation safety functions.

Although the main safety functions to be fulfilled are the same for every plant state, the functions to be categorized should be identified with respect to each plant state separately.

The lists of functions identified may be supplemented by other functions, such as those designed to reduce the actuation frequency of the reactor scram, and/or engineered safety features that correct deviations from normal operation, including those designed to maintain the main plant parameters within the normal range of operation of the plant. Such functions are generally not included in the safety analysis.

Owing to its importance to safety, monitoring to provide the plant staff and the off-site emergency response organization with a sufficient set of reliable information in the event of an accident should be considered for safety categorization. This should include monitoring and communication as part of the emergency response plan.

Functions included in the safety analysis either to prevent some sequences resulting from additional independent failures from escalating into a severe accident, or to mitigate the consequences of a severe accident, are counted as in functions associated with design
extension conditions.

The safety of the plant is also dependent on the reliability of various types of features, some of which are designed specifically for use in normal operation. In the Safety Guide, these SSCs are termed ‘design provisions’.

**Design provisions** need to be identified and may be considered to be subject to the safety classification process, and hence are designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained with sufficient quality to fulfil their intended role.

**Examples of design provisions**

- Design features that are designed to such a quality that their failure could be practically eliminated: e.g. the shells of reactor pressure vessels or steam generators.
- Features that are designed to reduce the frequency of accidents: e.g. piping of high quality whose failure would result in a design basis accident.
- Passive design features that are designed to protect workers and the public from harmful effects of radiation in normal operation: e.g. shielding, civil structures and piping.
- Passive design features that are designed to protect components important to safety from being damaged by internal or external hazards: e.g. concrete walls.

**2.2 Categorization of functions**

The functions required for fulfilling the main safety functions in all plant states, including modes of normal operation should be categorized on the basis of their safety significance.

Three levels of severity should be defined.

The severity should be considered **‘high’** if failure of the function could, at worst:
- Lead to a release of radioactive material that exceeds the limits for design basis accidents accepted by the regulatory body; or
- Cause the values of key physical parameters to exceed acceptance criteria for design basis accidents.

The severity should be considered **‘medium’** if failure of the function could, at worst:
- Lead to a release of radioactive material that exceeds the limits established for anticipated operational occurrences; or
- Causes the values of key physical parameters to exceed the design limits for anticipated operational occurrences.
The severity should be considered ‘low’ if failure of the function could, at worst:
- Lead to doses to workers above authorized limits.

Where more than one of these definitions is met, the highest of the three levels should be applied.

Assessment of the consequences is made by postulating that the function does not respond when challenged. For anticipated operational occurrences, in order to avoid ‘over-categorization’, assessment of the consequences should be made on the assumption that all other independent functions are preformed correctly and in due time.

The categorization of functions recommended in the Specific Safety Guide SSG 30 is based on three safety categories, as follows.

**Safety category 1:**
- Any function required to reach a controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of ‘high’ severity.

**Safety category 2:**
- Any function required to reach a controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of ‘medium’ severity; or
- Any function required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of ‘high’ severity; or
- Any function designed to provide a back-up of a function categorized in safety category 1 and required to control design extension conditions without core melt.

**Safety category 3:**
- Any function actuated in the event of an anticipated operational occurrence or design basis accident and whose failure when challenged would result in consequences of ‘low severity’; or
- Any function required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of ‘medium severity’; or
- Any function required to mitigate the consequences of design extension conditions, unless already required to be categorized in safety category 2, and whose failure, when challenged, would result in consequences of ‘high severity’; or
- Any function designed to reduce the actuation frequency of the reactor trip or engineered safety features in the event of a deviation from normal operation, including those designed to
maintain the main plant parameters within the normal range of operation of the plant; or

- Any function relating to the monitoring needed to provide plant staff and off-site emergency services with a sufficient set of reliable information in the event of an accident (design basis accident or design extension conditions), including monitoring and communication means as part of the emergency response plan (defence in depth level 5), unless already assigned to a higher category.

The categorization and relationship between Safety Function Type (functions credited in the analysis of postulated initiating events) and Safety Categories is shown in Table 2.1.

**Table 2.1:** Relationship between Safety Function Type and Safety Categories.

<table>
<thead>
<tr>
<th>Functions included in the safety assessment</th>
<th>Severity of the consequences if the function is not performed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Functions to reach a controlled state after anticipated operational occurrences</td>
<td>Safety Category 1</td>
</tr>
<tr>
<td>Functions to reach a controlled state after design basis accidents</td>
<td>Safety Category 1</td>
</tr>
<tr>
<td>Functions to reach and maintain a safe state</td>
<td>Safety Category 2</td>
</tr>
<tr>
<td>Functions for the mitigation of consequences of design extension conditions</td>
<td>Safety category 2 or 3</td>
</tr>
</tbody>
</table>

* A consequence of medium or low severity is not expected to occur in the event of non-response of a dedicated function for the mitigation of design extension conditions.
2.3 Classification of structures, systems and components

After the safety categorization of functions is completed, the SSCs performing these functions should be assigned to a safety class.

All the SSCs required to perform a function that is safety categorized should be identified and classified according to their safety significance.

Three safety classes are used consistent with the three categories recommended in Table 2.1.

The initial classification should take into account two factors:
- The consequences of failure to perform the safety function;
- The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

If an SSC contributes to the performance of several functions of different categories, it should be assigned to the class corresponding to the highest of these categories (i.e. the one requiring the most conservative engineering design rules). Applying these and other relevant considerations (e.g. engineering judgment), the final safety class of the SSC should then be selected.

Design provisions can be directly classified according to the severity of the consequences of their failure:
- **Safety class 1** - Any SSC whose failure would lead to consequences of ‘high’ severity;
- **Safety class 2** - Any SSC whose failure would lead to consequences of ‘medium’ severity;
- **Safety class 3** - Any SSC whose failure would lead to consequences of ‘low’ severity.

**Examples of SSC classification**

Any SSC (for example a fire or flood barrier) whose failure could challenge the assumptions made in the hazard analysis should be assigned in safety class 3 at least.

Any SSC that does not contribute to a particular function but whose failure could adversely affect that function (if this cannot be precluded by design) should be classified appropriately in order to avoid an unacceptable impact from the failure of the function.

Where the safety class of connecting or interacting SSCs is not the same (including cases where an SSC in a safety class is connected to an SSC that is not classified), interference between the SSCs should be prevented by means of a device (e.g. an optical isolator or automatic valve) classified in the higher safety class, to ensure that there will be no effects from failure of the SSC in the lower safety class.
By assigning each SSC to a safety class, a set of engineering, design and manufacturing rules can be identified and applied to the SSC to achieve the appropriate quality and reliability.

### 2.4 Verification of the safety classification

The adequacy of the safety classification should be verified using deterministic safety analysis, which should be complemented by insights from probabilistic safety assessment and/or supported by engineering judgement.

The contribution of the SSC to reduction in the overall plant risk is an important factor in the assignment of its safety class. Consistency between the deterministic and probabilistic approaches provides confidence that the safety classification is correct. Generally it is expected that probabilistic criteria for safety classification will match those derived deterministically. If there are differences, further assessment should be performed in order to understand the reasons for this and a final class should be assigned, supported by an appropriate justification.

The process of verification of the safety classification should be iterative, keeping in step with and informing the evolving design.

### 2.5 Selection of engineering design rules for SSCs

Engineering design rules are related to the following three characteristics:

- **Capability** is the ability of an SSC to perform its designated safety function as required, with account taken of uncertainties;
- **Dependability** is the ability of an SSC to perform the required plant specific safety function with a sufficiently low failure rate consistent with the safety analysis;
- **Robustness** is the ability of an SSC to ensure that no operational loads or loads caused by postulated initiating events adversely affect the ability of the safety functional group to perform a designated safety function.

The engineering design rules should ensure the SSCs in each safety functional group possess all the design features necessary to achieve the required levels of capability, dependability and robustness.

The engineering design rules should be determined by applying appropriate codes and standards, together with any relevant applicable regulatory limitations and criteria.
Quality assurance or management system requirements for the design, qualification, procurement, construction, inspection, installation, commissioning, operation, testing, surveillance and modification of SSCs should be assigned on the basis of their safety class.

The environmental qualification of SSCs should be determined in accordance with the conditions associated with normal operation and for postulated initiating events in which the SSCs may be called on to operate. Environmental qualification should include consideration of:

- Humidity;
- Temperature;
- Pressure;
- Vibration;
- Chemical effects;
- Radiation;
- Operating time;
- Ageing;
- Submergence;
- Electromagnetic interference;
- RF fields;
- Interference and voltage surges.

### 2.6 Questions

1. When in the life time of the power plant should the safety classification be performed?
2. What are the main steps in the classification process?
3. What is included in the term “function”?
4. What are the design provisions?
5. Give some examples of design provisions!
6. What are the three levels of severity?
7. How are functions categorized?
8. How should the adequacy of the safety classification be verified?
9. What are the three important characteristics in the selection of engineering design rules for SSCs?
3 IAEA SAFETY STANDARDS

Learning objectives
After completing this chapter, the trainee will be able to:
1. Recognize important safety standards for the safety classification of structures, systems and components.

For this chapter the following safety guides and safety requirements from the IAEA Safety Standards Series are relevant:
- Specific Safety requirements SSR-2/1; Safety of Nuclear Power Plants –Design,
- Specific Safety Guide SSG 30; Safety Classification of Structures, Systems and Components in Nuclear Power Plants,
- General Safety Requirements GSR Part 4; Safety for Facilities and Activities,

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.

Specific Safety requirements SSR-2/1 sets the requirements that must be met in design to achieve this fundamental safety objective. Further guidance is set forth in the Specific Safety Guide SSG 30 - Safety Classification of Structures, Systems and Components in Nuclear Power Plants.

To ensure attainment of the highest standards of safety that can reasonably be achieved, design measures must be taken to:
- Control the radiation exposure of people and the release of radioactive material into the environment;
- Restrict the likelihood of events that might lead to loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
- Mitigate the consequences of such events if they were to occur.

Safety Guide NS-G-1.2 from 2001 was superseded by General Safety Requirements GSR Part 4 and Specific Safety Guide SSG-2. They provide additional guidance for the safety classification of SSCs.

The safety classification system should be set up for each class of SSCs important to safety to identify the following:
- The appropriate codes and standards, and hence the appropriate provisions to be applied in design, manufacturing, construction and inspection of a component;
- System-related characteristics such as the degree of redundancy, need for emergency power supply and for environmental
qualification;
- The availability or unavailability status of systems for PIEs to be considered in deterministic safety analysis; and
- Quality assurance provisions.

The Safety classification of SSCs should be based on specified national approaches and should appropriately include deterministic and probabilistic considerations as well as engineering judgment.

In deterministic safety analysis, the safety functions that are used to determine compliance with acceptance criteria should be those performed using only safety classified SSCs.

Probabilistic safety analysis, which also considers the use of non-safety classified SSCs, may be used in the design phase to confirm the appropriate classification of SSCs. Some countries have adopted rules allowing risk-informed methods to be used for categorization of SSCs.

Failure of an SSC in one safety class should not cause failure of SSCs in a higher safety class. The adequacy of the isolation and separation of different and potentially interacting systems in different safety classes should be assessed.
4 EXAMPLE OF SAFETY AND QUALITY CLASSIFICATION OF A PWR - GERMANY

Learning objectives
After completing this chapter, the trainee will able to:
1. List important engineered safeguards in an NPP.
2. List the main safety objectives during operational and accidental conditions.
3. Explain the main purpose of establishing safety classes.
4. Explain the basic principles of quality classes for typical types of equipment.

Note:
Examples of safety and quality classification – examples from Germany and France were not established according to the Draft Safety Guide DS 367; the classification of the systems belonging to DiD level 4 and equipment necessary to the protection of the plant against the effects of natural hazards or to limit the propagation of the effects of the internal hazards might be upgraded.

This chapter presents an example of the practical application of safety classification, which is in principal agreement with the criteria and methodology of the IAEA Safety Guide 50-SG-D1 (this was withdrawn in the year 2000 because it did not comply with the new requirements on design), which was current at the time of the design, and is also in general agreement of intent with the present IAEA Safety Requirements SSR-2/1. Also included is the allocation of different kinds of systems and equipment to quality classes, which follows from the safety classification. Typically the most detailed quality classes exist for pressure-retaining system boundaries, due to their relation to both radiation barriers and safety functions.

The example is based on a three-loop pressurized water reactor (PWR) design concept of Siemens/KWU for an electrical output of 1000 MW.
**Fig. 4.1:** Engineered safeguards of a PWR plant.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reactor trip system</td>
</tr>
<tr>
<td>2</td>
<td>Accumulator</td>
</tr>
<tr>
<td>3</td>
<td>Borated water storage pool</td>
</tr>
<tr>
<td>4</td>
<td>Safety injection pump</td>
</tr>
<tr>
<td>5</td>
<td>Residual heat removal pump</td>
</tr>
<tr>
<td>6</td>
<td>Residual heat exchanger</td>
</tr>
<tr>
<td>7</td>
<td>Emergency power system</td>
</tr>
<tr>
<td>8</td>
<td>Vent system</td>
</tr>
<tr>
<td>9</td>
<td>Emergency feedwater system</td>
</tr>
<tr>
<td>10</td>
<td>Boric acid storage tank</td>
</tr>
<tr>
<td>11</td>
<td>Annulus air extraction system</td>
</tr>
</tbody>
</table>

### 4.1 Safety classification

Systems and components of the NPP are designated as important to safety if they perform safety actions required to avoid or mitigate the consequences of anticipated operational occurrences or accidents. The classification system applied reflects the gradation of requirements related to integrity or operability.

**Safety functions**

The NPP is designed in such a way that the necessary degree of occupational radiological protection is ensured at all times and no inadmissible quantities of radioactivity will be released to the environment during normal operation, under anticipated operational occurrences, or during and after postulated accidents.
The safety functions listed in Table 4.1 enable the design to meet these general requirements. These safety functions include those necessary to prevent accident conditions, as well as those necessary to mitigate the consequences of accidents. The safety functions can be accomplished, as appropriate, using SSCs provided for normal operation, or provided specifically to prevent anticipated operational occurrences from leading to accident conditions, or to mitigate the consequences of accident conditions.

**Safety classes**

For each safety function listed in Table 4.1 it is theoretically possible to establish a different design requirement. But it has been found practical to group these safety functions into safety classes. Each safety class contains safety functions with a similar degree of importance to safety. The safety classes themselves are then ranked according to their order of importance to safety, and requirements are assigned to each safety class.

The main purpose of establishing safety classes is to provide a basis for:
- A stepwise hierarchy of requirements for design;
- Materials selection;
- Manufacture or fabrication;
- Assembly;
- Developing an erection and construction programme.

It would be possible to establish such requirements corresponding to each individual safety function, but this would be not very practical in view of the large number of safety functions.

Four is a practical number of safety classes in the context of the different requirements. By using four safety classes, a useful grading in design requirements can be established on the basis of their relative importance to safety. Safety class 1 is most important to safety and safety classes 2, 3 and 4 are stepwise of decreasing importance to nuclear safety.

Table 4.2 gives a description of the four safety classes for the boundaries of fluid-retaining components. The correlation between these safety classes and the single safety functions is given in Table
4.1.
For NPP systems and components other than fluid-retaining boundaries, a lower number of safety classes is normally suitable. This is reflected in the corresponding quality classes, as described in the following chapter for several types of equipment.

**Table 4.1**: Correlation between safety functions and safety classes.

<table>
<thead>
<tr>
<th>Safety Function by Safety Requirements SSR 2/1</th>
<th>Safety Class (for Pressure Retaining Boundaries)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) Prevention of unacceptable reactivity transients</td>
<td>3</td>
</tr>
<tr>
<td>(b) Maintaining safe shutdown condition of the reactor</td>
<td>3</td>
</tr>
<tr>
<td>(c) Reactor shutdown for avoiding accidents and for mitigation of accident consequences</td>
<td>2</td>
</tr>
<tr>
<td>(d) Reactor shutdown after LOCA (Loss of Coolant Accident) where it is necessary to ensure acceptable reactor core cooling (not applicable to KWU-PWR, which has a “partial scram”, i.e. a step reduction in power level by partial injection of selected control rods)</td>
<td>1</td>
</tr>
<tr>
<td>(e₁) Maintaining a sufficient reactor coolant inventory during and after accidents</td>
<td>2</td>
</tr>
<tr>
<td>(e₂) Maintaining a sufficient reactor coolant inventory during and after all operational states</td>
<td>3</td>
</tr>
<tr>
<td>(f) Heat removal from the core after a failure in the RCPB (Reactor coolant pressure boundary)</td>
<td>2</td>
</tr>
<tr>
<td>(g) Residual heat removal from the core after operation and accidents with RCPB intact</td>
<td>2</td>
</tr>
<tr>
<td>(h) Heat transfer from other safety systems to the ultimate heat sink</td>
<td>3</td>
</tr>
<tr>
<td>(i) Assurance of necessary services (e.g. electrical power supply)</td>
<td>3</td>
</tr>
<tr>
<td>(j) Maintaining acceptable fuel cladding integrity</td>
<td>4</td>
</tr>
<tr>
<td>(k) Maintaining RCPB integrity</td>
<td>1</td>
</tr>
<tr>
<td>(l) Limitation of radioactivity release from the containment</td>
<td>2</td>
</tr>
<tr>
<td>(m) Keeping the radiation exposure within acceptable limits (from sources outside the containment)</td>
<td>3</td>
</tr>
<tr>
<td>(n₁) Limitation of radioactive material release below prescribed limits during all operational states of components (if they fail radiation exposure would result)</td>
<td>3</td>
</tr>
<tr>
<td>(n₂) As (n₁), but if components fail radiation exposure would not result</td>
<td>4</td>
</tr>
<tr>
<td>(o) Maintaining control of environmental conditions within the NPP</td>
<td>3</td>
</tr>
<tr>
<td>(p) Maintaining control of radioactive releases from irradiated fuel</td>
<td>3</td>
</tr>
<tr>
<td>(q) Decay heat removal from irradiated fuel</td>
<td>3</td>
</tr>
<tr>
<td>(r) Maintaining sufficient subcriticality of fuel stores outside RCPB</td>
<td>3</td>
</tr>
<tr>
<td>(s) Limiting the consequences of prevention of a component failure impairing a safety function</td>
<td>4</td>
</tr>
</tbody>
</table>
Some special components or equipment of high safety relevance are not covered by the safety classification in the Siemens/KWU classification system. This is especially valid for singular unique equipment types like fuel assemblies or the containment structure, for which different sets of graded requirements (for differently ranked pieces of similar equipment) are not needed. The requirements for these parts are described in separate specifications, based on separate rules and regulations.

**Table 4.2:** Transfer matrix for correlation of the safety classification to Siemens/KWU quality classes for pressure-retaining boundaries.

<table>
<thead>
<tr>
<th>Safety class (IAEA)</th>
<th>Quality class (Siemens/KWU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Prevention of release of core fission product inventory to the environment</td>
<td>K 1 RCPB and connecting pipes up to the first isolating valves</td>
</tr>
<tr>
<td>2 Mitigation of accident consequences, otherwise release of core fission products inventory to environment Prevention of anticipated operational occurrences leading to accidents (except those safety functions supporting another safety function) Functions which could result in a large fission product release if they fail, and a high probability that the safety function would be required (e.g. RHR)</td>
<td>K 2 Components with isolable connections to K 1 components and under reactor pressure Components for reactor shutdown and RHR which are not K 1 Components connected to secondary side of the steam generator (inside containment)</td>
</tr>
<tr>
<td>3 Supporting functions of class 1, 2 and 3 safety functions (no increase in radiation exposure) Prevention of radiation exposure from sources outside reactor coolant system Reactivity control on a slower time scale than in class 1 and 2 Maintaining subcriticality of fuel (outside reactor coolant system) Removal of decay heat from irradiated fuel (outside reactor coolant system)</td>
<td>K 2* Isolation valves between K 2 and K 3 or K 4 systems Main steam and feedwater piping inside containment</td>
</tr>
<tr>
<td>4 Safety functions not in class 1, 2 or 3</td>
<td>K 3 Components with isolable connections to K 2 components Components involved indirectly in RHR Components separated from K 1 components by barriers or normally closed valves Components for limitation of radioactive releases (whose failure would result in radiation exposure) Isolation valves between K 3 and K 4 or NC (Non-classified) systems</td>
</tr>
<tr>
<td></td>
<td>K 4 Components with isolable connections to K 3 components Components separated from K 2 components by barriers or normally closed valves Components for limitation of radioactive releases (whose failure would not result in radiation exposure) Isolation valves between K 4 and NC systems</td>
</tr>
</tbody>
</table>
4.2 Quality classes

The quality classes used by Siemens/KWU are defined for the different systems and components of the NPP in a different manner. In the following section examples are given for typical types of equipment:

- Fluid system pressure-retaining boundaries;
- Steel structures, supports;
- Heating, ventilation and air-conditioning systems;
- Hoists and cranes;
- Electrical equipment;
- Instrumentation and control equipment.

**Fluid system pressure-retaining boundaries**

The quality classes defined for the pressure retaining boundaries, named from K 1 to K 4, are based on the safety classes from 1 to 4 defined according to IAEA, 50-SG-D1 above, and Table 4.2. The only exception is the introduction of an additional quality sub-class K 2* for fulfilling the safety functions 6 and 7. The quality requirements for K 2* are between those of K 2 and K 1.

Moreover, items not related to nuclear safety are defined as non-classified (NC), which means that conventional codes and standards, as well as experience from industrial practice, are applied.

The correlation of the IAEA safety functions, the IAEA safety classes and the quality classes used by Siemens/KWU for pressure retaining boundaries is indicated in Tables 4.1 and 4.2.

The graded fundamental requirements for the different quality classes can be characterized as follows: For the class K 1 the highest design and quality requirements must apply, as defined in the nuclear rule KTA 3201, parts 1 to 4 (related respectively to materials, design and calculation, manufacture, inspections and surveillance). For the reactor pressure vessel additional requirements on supervision of material radiation embrittlement are defined in the rule KTA 3203.

For the class K 2 relatively high design and quality requirements are also valid, which are defined in the nuclear rule KTA 3211, parts 1 to 4 (subdivision as mentioned above for KTA 3201). The requirements of class K 3 are downgraded compared to the requirements of K 2, for example with respect to materials, but with respect to the fundamental design and quality requirements the rule KTA 3211 must be used.

In the case of class K 4 the norms and standards for conventional pressure-retaining components must apply, e.g. DIN or IEC norms, etc. For some aspects, for example inspections and surveillance, less
restrictive nuclear-specific requirements may apply. Components without relevance to nuclear safety are classified in the class NC (non-nuclear classified), and the norms and standards for conventional pressure-retaining components are applicable to them exclusively.

**Steel structures and supports**

Examples of the assignment of steel structures and supports to the three quality classes S 1, S 2 and NC are shown in the following table.

**Table 4.3:** Assignment of steel structures to quality classes.

<table>
<thead>
<tr>
<th>Type of structure</th>
<th>Quality class S 1</th>
<th>Quality class S 2</th>
<th>Quality class NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steel platforms</td>
<td>-</td>
<td>Seismic category I</td>
<td>Seismic category II</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Seismic category Ia</td>
<td></td>
</tr>
<tr>
<td>Piping supports</td>
<td>K 1 piping</td>
<td>K 2, K 3, K 4 piping</td>
<td>NC piping</td>
</tr>
<tr>
<td>Component supports</td>
<td>K components</td>
<td>K 2, K 3, K 4 components</td>
<td>-</td>
</tr>
<tr>
<td>Anchors</td>
<td>-</td>
<td>Seismic category I</td>
<td>Seismic category II</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Seismic category Ia</td>
<td></td>
</tr>
</tbody>
</table>

**Key to seismic categories:**
- I = relevant for nuclear safety,
- II = not relevant for nuclear safety,
- IIa = not relevant for nuclear safety, but may impair seismic category I equipment in case of its failure.

**Heating, ventilation and air-conditioning systems**

The systems and components for heating, ventilation and air-conditioning (HVAC) are assigned to two quality classes, L and NC. The nuclear safety relevant class L applies to:
- System sections which are necessary to prevent inadmissible radiation releases;
- System sections carrying out safety-related support functions in order to maintain the operability of safety systems;
- System sections serving for the habitability of main and emergency control rooms during and after accidents.

HVAC equipment of quality class L must be in accordance with the nuclear rule KTA 3601, whereas conventional norms and standards like DIN or IEC apply to class NC.
**Hoists and cranes**

The basic assignment of hoists and cranes is made into two quality classes H and NC. The class H includes lifting equipment with nuclear safety related effects, which means hoists and cranes whose failure may cause an unacceptable release of radioactivity to the environment or constitute a hazard to other safety related equipment.

For hoists and cranes of quality class H the nuclear rule KTA 3902 is applicable. This rule contains requirements for 3 types of lifting equipment, graded in accordance with their safety importance. The highest requirements apply to cranes with exclusion of load drop accidents, for example the main reactor building crane. Special requirements are also defined for refuelling machines in this KTA rule.

**Electrical equipment**

Electrical equipment is classified in the two safety related quality classes E 1 and E 2, and in the non-nuclear class NC. The class E 1 applies to the electrical equipment of safety systems, for example:

- Switchgear, transformers and distribution systems for the electricity supply of safety systems;
- Equipment for emergency electrical power production, conversion and storage;
- Electrical valve actuators of safety systems.

The class E 2 applies to safety related electrical equipment, for example emergency lighting or standard products used for complex applications (e.g. actuators of auxiliary equipment of pump units). Class NC applies to non-nuclear safety related electrical equipment.

For class E 1 several nuclear rules for design, fabrication and qualification exist, in particular KTA 3701 to KTA 3705 for emergency electrical distribution and production equipment, and KTA 3504 for electrical valve actuators.

Class E 2 equipment is basically fabricated in accordance with conventional industrial norms and standards (like NC equipment), but special qualification (for example for accidental environmental conditions or seismic events must be carried out in accordance with nuclear safety graded requirements (e.g. KTA 2201 for seismic qualification).

**Instrumentation and control equipment**

For instrumentation and control (I&C) equipment, the defined quality classes IC 1, IC 2 and NC are basically similar to those of electrical equipment. Class IC 1 mainly includes the reactor protection system, the actuation system of safety systems (ESFAS), accident instrumentation (overview and wide-range safety parameters), and high priority alarms. Class IC 2 is valid for safety related I&C systems, such as the reactor limitation systems, radiation control systems, safety system control systems, seismic instrumentation, fire
alarm system and safety related communication systems.

For class IC 1, several nuclear rules for its design, fabrication and qualification exist, in particular KTA 3501, 3503, 3505 to 3507 for reactor protection systems and ESFAS, KTA 3502 for accident instrumentation. For modern, computer-based systems rules for software qualification, such as IEC 880 and IEEE standards, must be taken into account in addition.

Class IC 2 equipment is basically fabricated in accordance with conventional industrial norms and standards (like NC equipment), but special qualification (for example for accidental environmental conditions or seismic events) must be carried out in accordance with nuclear safety graded requirements.

### 4.3 Questions

1. What are the important safety engineered safeguards in an NPP?
2. What safety objectives should be achieved during operational and accidental conditions?
3. Why is it important to establish safety classes?
Learning objectives

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

1. Define the terms equipment and component.
2. Explain the assignment of safety classes.
3. Describe design basis operating conditions.
4. Explain the safety classification of design basis operating conditions.
5. Explain the safety classification of complementary operating conditions.
6. List safety-related but non-safety grade equipment.
7. List items of equipment which are of seismic grade.

The classification of equipment ( mechanical equipment, electrical systems and civil engineering structures) determines the equipment quality requirements. The safety classification is finalized by drawing up a list of the equipment performing a safety function under the various conditions considered plausible.

In this section, the terms “equipment” and “component” have the following meanings:

<table>
<thead>
<tr>
<th>Equipment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A unit or assembly (pump, valve, pipe, motor, electrical cabinet, etc.) capable of performing a basic function.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part of the equipment participating in the accomplishment of this function.</td>
</tr>
</tbody>
</table>

5.1 Assignment of the safety class

The equipment is assigned a safety class reflecting its importance with respect to safety.

“Safety related” equipment is either designed as “safety grade” and assigned a safety class based on the operating conditions considered plausible, i.e. necessary to accomplish the following three objectives under the design basis operating conditions (categories 1, 2, 3 and 4 as defined below) and under the complementary operating conditions (defined below):

- Maintaining the integrity of the main primary system pressure boundary;
- Bringing the reactor to a safe shutdown state and maintaining it
there;

- Preventing and limiting the radiological consequences of accidents.

Or alternatively, it is designed as “non-safety grade”, when its failure is unlikely to interfere with the accomplishment of the three objectives indicated above or when correct operation is only necessary in the long term to accomplish these objectives.

Note that in American regulations a “Safety related” system or equipment is equivalent to a “Safety” systems or equipment in present IAEA standards, and to a “Safety grade” system or equipment in French terminology; in French N4 terminology, “Safety related” equipment is equivalent to items “important to safety” in present IAEA terminology; and in present IAEA terminology a “Safety related” item is similar to the French N4 “safety related but non-safety grade”.

**Design basis operating conditions**

The four categories of operating conditions comprise:

- **Category 1** – normal operating conditions,
- **Category 2** – minor but frequent incidents, of a frequency of $10^{-2}$ to 1 per unit per year,
- **Category 3** – unlikely incidents, of a frequency of $10^{-4}$ to $10^{-2}$ per unit per year and
- **Category 4** – limiting faults of a frequency of $10^{-6}$ to $10^{-4}$ per unit per year.

**5.2 Classification sequence**

The following sequential process is used for classification:

- Determination of the functions to be performed by each of the systems concerned (main system and support systems) under all operating conditions considered to be plausible (design basis operating conditions and complementary operating conditions). After this a list is drawn up of the equipment involved in accomplishing the functions and which must therefore be either safety grade or safety-related but non-safety grade.
- Determination of the class for each item of equipment on which certain of the following design requirements depend: redundancy and independence, electrical power back-up, qualification for accident conditions, subject to a design and construction code, seismic grade, quality assurance requirements and an operability requirement (periodic tests).

For particularly complex equipment, the classification is carried out at the level of its components (e.g. for diesel generators).
5.3 Safety classification for design basis operating conditions

Classification of mechanical equipment

Pressure retaining equipment ensuring a safety function under design basis conditions (conditions 1, 2, 3 and 4) are divided into three safety classes as indicated below.

**Safety class 1:**
Safety class 1 covers equipment constituting the pressure boundary of the reactor coolant system and whose failure, in normal operation, would result in loss of primary coolant at a rate exceeding the make-up capability.

This notably includes:
- The main primary system;
- The main primary system equipment (including its isolation devices) with equivalent inside diameters greater than the value which, in the event of rupture, could be compensated for by means of the normal make-up resources.

Class 1 is the highest safety class, since the failure of equipment belonging to this class would lead to the most serious consequences with respect to radioactive releases.

**Safety class 2:**
Safety class 2 covers the equipment of systems carrying primary coolant not included in safety grade 1, or that of systems directly necessary for containing radioactivity in the event of a LOCA.

This equipment notably includes:
- The pipes of the main primary system with equivalent inside diameters less than the value, in the event of a rupture, could be compensated for using the normal make-up resources;
- The main items of equipment of the containment atmosphere hydrogen control system;
- The safety injection system and the containment spray system;
- The residual heat removal system;
- The section of the component cooling water system inside the reactor building;
- The mechanical equipment constituting the third confinement barrier, including isolation devices (as well as the steam and water systems inside the reactor building);
- The sections of the secondary feedwater and steam systems outside the reactor building, up to and including the first isolation device.

**Safety class 3** notably includes the following systems (or sections
The auxiliary feedwater system;
The section of the component cooling water system outside the reactor building, and the essential service water system;
The reactor cavity and spent fuel pit cooling and treatment system; and
Certain effluent treatment systems.

The connection between two systems or portions of systems having different safety classes must employ an appropriate interface device, whose role is to ensure that failure of the equipment belonging to the lower safety class will not:
- Prevent the performance of the safety function of the higher class equipment or system; or
- Result in the uncontrolled release of radioactive gases normally stored to permit decay.

**Table 5.1:** The interface devices and safety classes.

<table>
<thead>
<tr>
<th>Higher safety class</th>
<th>Required interface</th>
<th>Lower safety class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>At least one safety valve or two active valves in series or two normally closed valves in series or a passive device (*)</td>
<td>Non-classified or 3 or 2</td>
</tr>
<tr>
<td>2</td>
<td>Two normally open remote controlled valves in series or one normally closed valve or one normally open remote controlled valve (<strong>) or one check valve or one safety valve or one heat exchanger surface, or an anchor (</strong><em>) or a passive equipment item (</em>**)</td>
<td>3 or non-classified</td>
</tr>
</tbody>
</table>

(*) The use of a flow-limiting orifice is only acceptable in small diameter pipes, i.e. pipes where the presence of the orifice ensures that, in the event of pipe rupture, leakage can be compensated for by normal make-up means.

(**) Provided that its failure, when combined with that of a lower safety class piece of equipment, will not prevent the higher safety class system from accomplishing its function nor result in the uncontrolled release of radioactive gases normally stored to permit decay.

(***) Provided that the failure of a lower safety class piece of equipment will not prevent the higher safety class system from accomplishing its function nor result in the uncontrolled release of radioactive gases normally stored to permit decay.
Module V: Safety classification of structures, systems and components

<table>
<thead>
<tr>
<th>Higher safety class</th>
<th>Required interface</th>
<th>Lower safety class</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Same as above (eight possibilities)</td>
<td>Non-classified</td>
</tr>
</tbody>
</table>

The interface devices (Table 5.1) must belong to the highest safety class.

*Design and construction rules:* The RCC-M code, which specifies the rules for design (including sizing and stress analysis) and construction (materials, manufacturing and test specifications) must be applicable, as a minimum, to pressure retaining equipment in the nuclear island. The safety class determines the RCC-M class.

**Table 5.2:** Relationship between safety class and RCC-M class from paragraph a 4231 of the RCC-M code.

<table>
<thead>
<tr>
<th>Safety class</th>
<th>RCC-M class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2 (*)</td>
</tr>
<tr>
<td>3</td>
<td>3 (**)</td>
</tr>
<tr>
<td>non-classified 1, 2 or 3</td>
<td>not applicable (**)</td>
</tr>
</tbody>
</table>

Instrumentation lines beyond the first isolation valve must be considered as small equipment as defined in the RCC-M, and the provisions in Subsection E of the RCC-M must be applied.

Where the scope of application of the RCC-M does not cover certain safety class equipment, any special requirements shall be provided in the equipment specification.

**Classification of non-pressure retaining equipment**

Class LS consists of mechanical equipment (other than pressure vessels) necessary for performing safety functions under design basis operating conditions. The main systems involved are those playing roles in the storage and handling of spent fuel or supporting safety grade pressure vessels, reactor internals and certain ventilation systems.

Basic Safety Rule IV.2.a lays down the requirements associated with safety-grade mechanical equipment, circulating or containing a fluid

(*) The pressure retaining envelope of the secondary side of the steam generators must be RCC-M class 1 although it is safety class 2.

(**) Under certain pressure, temperature and cyclic loading conditions, safety class 3 equipment may be RCC-M class 2 and equipment non-classified 1, 2 or 3 may be RCC-M 2 or 3, as explained in RCC-M Paragraph A 4232.
under pressure, of Levels 2 and 3. The RCC-M code is applicable to most of safety class 1, 2 and 3 equipment and some LS class mechanical equipment.

**Requirements related to the safety class of mechanical equipment**

As a minimum, the following requirements associated with safety class mechanical equipment (class 1, 2, 3 or LS) must apply (in addition to those specified for the resistance to seismic loading):

- Qualification, if applicable, under accident ambient conditions;
- Application of the administrative order dealing with quality assurance;
- Capacity for active equipment to undergo periodic tests;
- Design and construction of equipment according to rules specific to the equipment.

**Classification of electrical equipment and systems**

Electrical systems necessary to achieve the safety objectives under design basis conditions must be assigned a safety class. Two safety classes (1E and 2E) are defined for electrical systems as follows:

**Class 1E** covers systems and equipment performing safeguard functions and necessary for:

- Reactor trip;
- Reactor containment isolation;
- Emergency core cooling;
- Removal of residual heat from the reactor and the reactor building;
- Prevention of accidents or limitation of their radiological consequences.

These functions must be ensured even when postulating a single failure affecting a system participating in the accomplishment of these functions and when postulating the failure of the main grid. The following electrical systems are required to comply with the class 1E criteria:

- Reactor protection system;
- Reactor trip equipment;
- Cooling of reactor coolant by atmospheric steam dump;
- Safety injection;
- Containment spray;
- Auxiliary feedwater;
- Hydrogen concentration control;
- Containment annulus ventilation;
- Containment isolation;
- Certain ventilation systems, particularly the system for the control room (and the associated chilled water production), those ensuring an engineered safeguard function, those indispensable to the operation of the engineered safeguard
systems, those for electrical cabinets housing equipment ensuring an engineered safeguard function and those for cabinets housing electrical equipment for the diesel generators;

- Activity measurements which activate safeguards systems;
- Electrical systems corresponding to portions of the following functions supporting the above functions: emergency power supply (diesel generators, storage batteries and battery chargers, associated distribution networks), component cooling and essential service water.

Class 1E must apply to the instrumentation channel electrical equipment from the sensors and transmitters up to and including the actuators, as well as the associated power supplies. Under certain conditions, the I&C for these channels may be class 2E.

Class 1E must thus include: electrical power supplies, motors, valve operators, solenoid valves, on-site power distribution networks, instrumentation. Requirements relevant to class 1E systems are specified in RFS IV.2.b as follows:

- Redundancy (compliance with single failure criteria defined in RFS 1.3.a);
- Independence (geographical or physical and electrical separation);
- Back-up by on-site power supplies that comply with the principles of independence and redundancy;
- Qualification of equipment under ambient conditions;
- Capability of being periodically tested to verify the ability of the equipment to fulfil its function under all the standard plant unit conditions where its availability is required;
- Design and construction of equipment according to the specific rules specified in the RCC-E.

In addition, the administrative order dealing with quality assurance must apply.

**Class 2E:** Specifically for N4 power plants, Class 2E covers the electrical systems and equipment necessary for performing the following safety functions (on the basis of interpretation of Basic Safety Rule IV.1.a):

- Returning the reactor to the cold shutdown state and maintaining it there;
- Surveillance of the post-accident phase;
- Retention of gaseous effluents;
- Fuel handling where failure could result in radioactive releases;
- Cooling of spent fuel;
- Isolation of the primary system from the auxiliary systems;
- Isolation of systems or parts of systems of safety grade from systems or parts of systems that are non-safety grade.
The systems which accomplish a class 2E function are the following.

For the cold shutdown function:
- Reactor coolant system pressurizer on-off heaters;
- Chemical and volume control system for volume control, boration and auxiliary spray functions;
- Boron and water make-up system for the boric acid make-up function;
- Residual heat removal system;
- Component cooling system for the priority share parts;
- Control room auxiliary panel.

For the post-accident monitoring function:
- Post-accident monitoring system.

For the gaseous waste hold-up function:
- Gaseous waste treatment system;
- Ventilation system for safeguard rooms (exhaust and iodine retention).

For the fuel handling function:
- Spent fuel handling system in the reactor building (security systems);
- Fuel handling system in the reactor building (security systems);
- Fuel transfer system.

For the fuel cooling function:
- Reactor cavity and spent fuel pit cooling and treatment system (cooling portion) and connection with the residual heat removal system.

For the main primary system isolation function:
- Isolation valves on the lines connected to the main primary system.

For the safety class line isolation function:
- Isolation valves between safety class and non-safety class lines.

Class 2E concerns all the equipment referred to previously with respect to class 1E.

Safety class 2E requirements are specified on a case-by-case basis, depending on the role played by the systems being considered. They are specified in the sections dealing with the plant systems where class 2E functions are involved. As a minimum, the following requirements, in addition to those concerning the resistance to seismic loadings, must be applied:
- Emergency power supplies;
- Qualification under ambient conditions;
- Design and construction according to specific rules specified in
the RCC-E;
- Capability of being tested periodically while in service; and
- Administrative order dealing with quality assurance.

Justification must be provided, on a case-by-case basis, for non-compliance with the emergency power supply requirements and design and construction specifications in the case of certain equipment in safety class 2E systems and with the qualification rules specified in RCC-E section B for the equipment in safety class 1E systems.

**Classification of civil engineering structures**

Class LS covers civil engineering structures which, under design basis operating conditions:
- Perform a safety function confinements of radioactive materials (e.g. the reactor building), retention of radioactive fluids (e.g. certain concrete tanks), removal of residual heat or control of reactivity (e.g. the auxiliary feedwater supply tank); or
- Should they fail, would induce failure of an item of equipment with a safety function (i.e. certain supports); or
- Serve to protect safety-grade equipment from the consequences of the failure of other equipment or from the effects of the surrounding environment or external hazards.

These structures are designed and built in accordance with the rules of RCC-G.

### 5.4 Safety classification for complementary operating conditions

Permanently installed items of electrical and mechanical equipment necessary for performing safety functions and required under complementary operating conditions, which are not already classified as safety grade for design basis operating conditions, are classified as class SH (mobile equipment used in the longer term is classed as safety-related but non-safety grade). This class is introduced only on N4 power plants. These items are:
- The 380 V turbine generator;
- The electrical equipment of the test pump of the chemical and volume control system used for injection at the reactor coolant pump seals;
- The channel providing protection against failure of the automatic scram system in the event of a Category 2 operating condition (ATWS);
- The safety lighting of the control room;
- The instrumentation and control systems of the pressurizer relief valves required for operation with the primary system in the feed and bleed mode.

Safety class SH equipment for complementary operating conditions
must comply, as a minimum, with the following requirements:

- Design and construction rules (to be specified on a case-by-case basis);
- The capability of being tested periodically when in service;
- The administrative order dealing with quality assurance;
- Qualification adapted to the conditions under which the equipment will be required.

It should be verified that utilisation of the equipment required for complementary operating conditions will not compromise the design criteria applicable to systems containing safety class equipment for operation under design basis operating conditions.

### 5.5 Safety-related but non-safety grade equipment

The safety-related but non-safety grade equipment comprises:

- Equipment for which operating errors could result in inadvertent radioactive releases;
- Safety systems and equipment necessary particularly in the case of internal or external hazards (fire, flooding, explosion etc.) or during unit shutdown phases;
- Handling systems and equipment liable to harm spent fuel assemblies in the event of a load being dropped, as well as more generally equipment liable to damage seismic safety-grade equipment in the event of their collapse during an earthquake;
- Certain items of equipment that are useful but not indispensable in post-accident operation;
- Certain items of equipment necessary for re-supplying the auxiliary feedwater tank;
- Certain items of equipment which are only indispensable in the long term (particularly those used in procedures associated with complementary operating conditions) and those used for the raw water system make-up in operation in the closed circuit mode;
- Certain items of mobile equipment used under complementary operating conditions;
- Certain items of special equipment necessary for managing severe accidents.

The requirements for this equipment must be specified on a case-by-case basis in order to ensure a high degree of availability of the equipment. As a minimum, in-service periodic inspections must be possible (except in the event of damage following an earthquake) and the administrative order dealing with quality assurance must be applied.

### 5.6 Seismic category equipment

Items of equipment whose functions (integrity, functional capability
or operability) must be maintained when subject to the loading resulting from an earthquake corresponding to the design basis spectrum are classified as seismic grade. The requirement may apply during and/or after an earthquake, depending on the nature of the equipment and the functions it performs.

Electrical and mechanical equipment and civil engineering structures classified as safety grade for design basis operating conditions are classified as seismic grade, as is equipment classified as safety grade for the H3 additional operating condition. Non-safety grade equipment necessary for safety zoning is designed for earthquake conditions. The same applies (in the absence of measurement) to equipment which could compromise the functions of safety-grade equipment if it fell or failed.

Stresses resulting from operating conditions and stresses of seismic origin are taken into consideration in the design basis of the equipment in accordance with the rules of combination laid down in Basic Safety Rule IV.2.a:

- Stresses resulting from design basis operating conditions of Categories 1 and 2 are combined with those caused by an earthquake corresponding to the design basis spectrum. In these situations, the equipment remains capable of performing its functions for the remainder of the lifetime of the unit.
- Stresses resulting from design basis operating conditions are combined with those caused by an earthquake corresponding to the design basis spectrum. This conventional combination covers:
  - The integrity of all RCC-M Level 2 and Level 3 equipment,
  - The operability and functional capability of the safeguard systems and those necessary for reaching and maintaining a safe shutdown state and for cooling the spent fuel assemblies.

The main requirements applicable to safety-related structures are indicated in Table 5.3.
Table 5.3: Main requirements applicable to safety-related structures.

<table>
<thead>
<tr>
<th>Class</th>
<th>Redundancy</th>
<th>Power back-up</th>
<th>Qualification</th>
<th>Codes</th>
<th>Seismic grade</th>
<th>Quality Assurance</th>
<th>Periodic tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanical 1, 2, 3, LS</td>
<td>*</td>
<td>**</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Civil Engineering LS</td>
<td>/</td>
<td>/</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Electrical 1E</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Electrical 2E</td>
<td>case by case</td>
<td>case by case</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SH</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Safety related but non-safety grade equipment</td>
<td>no</td>
<td>case by case</td>
<td>case by case</td>
<td>yes</td>
<td>case by case</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

1. Within the scope of the directive of August 10, 1984.
2. Normal operations can be adequate proof of correct operation (testing unnecessary).
   - Redundancy of certain items of equipment (those covered by Basic Safety Rule I.3.a).
   - ** On a case-by-case basis for associated electrical equipment.

### 5.7 Questions

1. What is meant by the terms equipment and component?
2. What is the difference between safety grade and non-safety grade equipment?
3. Which operating conditions include design basis operating conditions?
6 REFERENCES


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