DS367 Draft 6.1
Date: 20 November 2010

Formatted: Space Before: 0 pt, After: 0 pt, Line spacing: single

Deleted: 5.10

Deleted: 1912 October

Deleted: 18

IAEA SAFETY STANDARDS

for protecting people and the environment

Formatted: Indent: Before: 0.25 cm, Hanging: 1.5 cm, Space Before: 0 pt, After: 0 pt, Line spacing: single

Deleted: ¶

Status: for submission to NUSSC

with resolution of Member States and NUSSC members' comments

Reviewed in NS-SSCS (Asfaw)

Deleted: ¶

Safety Classification of Structures, Systems and Components in Nuclear Power Plants

DRAFT SAFETY GUIDE

DS367

Deleted: ¶

New Safety Guide

IAEA

International Atomic Energy Agency

CONTENTS

Deleted: 1. INTRODUCTION . 3¶
BACKGROUND . 3¶
OBJECTIVE . 4¶
SCOPE . 4¶
STRUCTURE . 5¶
¶
2. BASIS FOR AND GENERAL APPROACH TO SAFETY CLASSIFICATION . 6¶
REQUIREMENTS FOR A SAFETY CLASSIFICATION PROCESS . 6¶
GENERAL APPROACH TO THE SAFETY CLASSIFICATION PROCESS . 7¶
¶
3. SAFETY CLASSIFICATION PROCESS . 10¶
ESTABLISHING THE INPUT TO THE CLASSIFICATION PROCESS: REVIEW OF POSTULATED INITIATING EVENTS . 10¶
IDENTIFICATION OF PLANT SPECIFIC SAFETY FUNCTIONS . 10¶
CATEGORIZATION OF SAFETY FUNCTIONS . 13¶
GROUPING OF STRUCTURES, SYSTEMS AND COMPONENTS . 17¶
CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS . 17¶
VERIFICATION OF THE SAFETY CLASSIFICATION . 19¶
¶
4. SELECTION OF APPLICABLE DESIGN RULES FOR STRUCTURES, SYSTEMS AND COMPONENTS . 21¶
¶
APPENDIX I SAFETY FUNCTIONS IN RELATION TO THE CONCEPT OF DEFENCE IN DEPTH . 23¶
APPENDIX II RELATIONSHIP BETWEEN DESIGN AND SAFETY ANALYSIS PROCESSES AND THE SAFETY CLASSIFICATION PROCESS . 24¶
¶
REFERENCES . 25¶
¶
ANNEX I REACTOR TYPE SAFETY FUNCTIONS FOR LIGHT WATER REACTORS . 27¶
ANNEX II: EXAMPLES OF DESIGN RULES FOR SSCS . 31¶
¶
CONTRIBUTORS TO DRAFTING AND REVIEW . 36¶

1. INTRODUCTION

BACKGROUND

1.1. The need to classify equipment in a nuclear power plant according to its importance to safety has been recognized since the early days of reactor design and operation. The existing methods for safety classification of structures, systems and components (SSCs) have evolved in this light of lessons learnt during the design and operation of existing plants, mainly with light water reactors. Although the concept of a safety function as being what must be accomplished for safety has been understood for many years, and examples based on experience have been provided, the process by which safety functions can be derived from the general safety objectives has not been described in earlier IAEA publications. Therefore, it was mainly from experience and analysis of specific designs that classification systems identified those SSCs that were deemed to be of the highest importance in maintaining safe operation, such as the continuing integrity of the primary pressure boundary, and classified them at the highest level.

1.2. This Safety Guide was prepared under the IAEA programme for safety standards for nuclear power plants. An IAEA Safety Guide on Safety Functions and Component Classification for Boiling Water Reactor (BWR), Pressurized Water Reactor (PWR), and Pressure Tube Reactor (PTR) Plants was issued in 1979 as Safety Series No. 50-SG-D1 and was withdrawn in the year 2000 because the recommendations contained therein were considered not to comply with the IAEA Safety Requirements publication, Safety of Nuclear Power Plants: Design, published in 2000. This Safety Guide represents an update of that earlier Safety Series publication.

1.3. In developing this Safety Guide, relevant IAEA publications have been considered. This included the Safety Requirements publications, Safety of Nuclear Power Plants: Design [1] and Safety Assessment for Facilities and Activities [2], the Fundamental Safety Principles [3], and current versions and ongoing revisions of Safety Guides and INSAG reports, including Safety Assessment and Verification for Nuclear Power Plants [4] and Defence in Depth in Nuclear Safety [5]. These publications have addressed the issues of safety functions and the safety classification of SSCs for nuclear power plants. Information from a significant number of other international and national publications such as Refs [6], [7] and [8] has been considered in developing this Safety Guide.

Deleted: s

1.4. The purpose of safety classification in a nuclear power plant is to identify and categorize the safety functions and to identify and classify the related SSC items on the basis of their safety significance. This will ensure that 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. Reference [1] requires designers to undertake a number of steps to perform safety classification and to justify the assignment of SSCs to safety classes.

1.5. The IAEA reviewed widely the existing safety classification methodologies applied in operating nuclear power plants and for new designs. This Safety Guide is based on this review. The principles and method of classification provided in this Safety Guide aim at harmonizing national practices. Furthermore, this Safety Guide explicitly describes the steps of safety classification, which are often not systematically expressed and documented in national classification methods. The principles and method classification provided in this Safety Guide do not invalidate classifications of SSCs achieved using other methods or the national requirements of the individual Member States provided these follow similar underlying principles.

Deleted: the

Deleted: To adopt the best practices in Member States, t

Deleted: classification

Formatted: Font: (Default) Times New Roman, 12 pt, Complex Script Font: Times New Roman, 12 pt

Formatted: Font: 12 pt, Complex Script Font: 12 pt

Formatted: Font: 12 pt, Complex Script Font: 12 pt

OBJECTIVE

1.6. The objective of this Safety Guide is to provide recommendations and guidance on how to meet the requirements established in Refs [1] and [2] for identification and categorization of safety functions and for classification of related SSCs to ensure safety by meeting associated quality and reliability targets accordingly. This Safety Guide presents a technology neutral approach and, therefore, issues relating to particular types of reactor are discussed in general terms.

Formatted: Font: 12 pt, Complex Script Font: 12 pt

1.7. This publication is intended for use by organizations designing, manufacturing, constructing and operating nuclear power plants, as well as by regulatory bodies and their technical support organizations for the conduct of regulatory reviews and assessments.

SCOPE

1.8. This Safety Guide covers all safety aspects of a nuclear power plant that are included in the plant's safety analysis report, including the storage and handling of new and spent fuel at the site of the plant. The recommendations on safety classification as presented in this Safety

Guide are intended to be applicable to any plant type. The approach is intended to be suitable for new designs of nuclear power plants; however, it should not be fully applied to existing plants or designs that have already been licenced. For the purpose of this Safety Guide, existing nuclear power plants are those nuclear power plants that are: (a) at the operational stage (including long term operation and extended temporary shutdown periods); (b) at a pre-operational stage for which the construction of structures, the manufacturing, installation and/or assembly of components and systems, and commissioning activities are significantly advanced or fully completed; or (c) at a temporary or permanent shutdown stage while nuclear fuel is still within the facility (in the core or the pool). For upgrading of existing plants, the use of this Safety Guide will help to classify new SSCs, and reclassify existing SSCs interfacing with new SSCs if necessary.

Deleted: may also

1.9. This Safety Guide is written in technology neutral terms. This assumes that there are features of all nuclear power plants that are common to all reactor types. For example, it is assumed that all plants have a series of physical barriers or other barriers for the retention of the inventory of radioactive material and that all such barriers have to meet a set of requirements that govern the safe operation of the plant. Furthermore, all plants are assumed to require certain physical processes to operate, including cooling of the fuel, limitation of chemical attack and mechanical processes to prevent degradation of the barriers retaining radioactive material, although in different designs, each of these aspects may be of different relative importance. This Safety Guide is applicable for all SSCs at nuclear power plants, but the recommendations it provides could be extended to cover any type of nuclear facility, if the appropriate amendments are made.

STRUCTURE

1.10. Section 2 provides the basis and general approach recommended for meeting the safety requirements on safety classification. Section 3 describes the steps in the safety classification process. Section 4 provides recommendations on determining the engineering design rules for plant specific safety functions and SSCs on the basis of their safety categories and safety classes respectively. Appendix I provides a chart indicating how safety functions relate to the various levels of defence in depth in this approach. Appendix II provides a table indicating the different steps typically performed in classification of SSCs in line with other design processes. Annex I lists reactor type safety functions for light water reactors. Annex II gives examples of engineering design rules for SSCs.

Deleted: to be adopted in

Deleted: to be

2. BASIS FOR AND GENERAL APPROACH TO SAFETY CLASSIFICATION

REQUIREMENTS FOR A SAFETY CLASSIFICATION PROCESS

2.1. The basic requirements for a safety classification system are established in Ref. [1] and are repeated in the following paragraphs. Additional related requirements are established in Ref. [2]. The recommendations on how to meet these requirements are developed in this Safety Guide.

2.2. Paragraph 4.1 of Ref. [1] states that "A systematic approach shall be taken to identify the items important to safety that are necessary to fulfil the fundamental safety functions, and to identify the inherent features that are contributing to or affecting the fundamental safety functions, for the first four levels of defence in depth."

Deleted: r

Deleted: followed

Deleted: all

2.3. Requirement 23 of Ref. [1] states that "All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance."

Deleted: the items identified

2.4. Paragraph 5.35 of Ref. [1] states that "The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methodologies complemented where appropriate by probabilistic methods, with account taken of factors such as:

Deleted: primarily

(1) the safety function(s) to be performed by the item;

(2) the consequences of failure to perform the safety function;

(3) the frequency at which the item will be called upon to perform a safety function;

(4) the time following a postulated initiating event at which, or the period for which, it will be called upon to operate."

2.5. Paragraph 5.36 of Ref. [1] states that "The design shall be such as to ensure that any interference between items important to safety shall be prevented. In particular any failure of items important to safety in a system classified in a lower class will not propagate to a system classified in a higher safety class."

2.5b. Paragraph 5.37 of Ref. [1] states that "Equipment that performs multiple functions shall be classified consistent with the most important function performed."

2.6. Requirement 4 of Ref. [1] states that "Fulfilment of the following fundamental safety functions shall be ensured for all plant states:

(1) control of reactivity;

(2) removal of heat from the core and from spent fuel;

(3) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases."

Deleted: Requirement 22 of Ref. [1] states that "Interference between safety systems and systems of lower classification or between redundant elements of systems of the same class shall be prevented by means such as physical separation of safety systems, electrical isolation, functional independence and independence of communication (data transfer), as appropriate." ¶

Deleted: provision of

Deleted: operational discharges

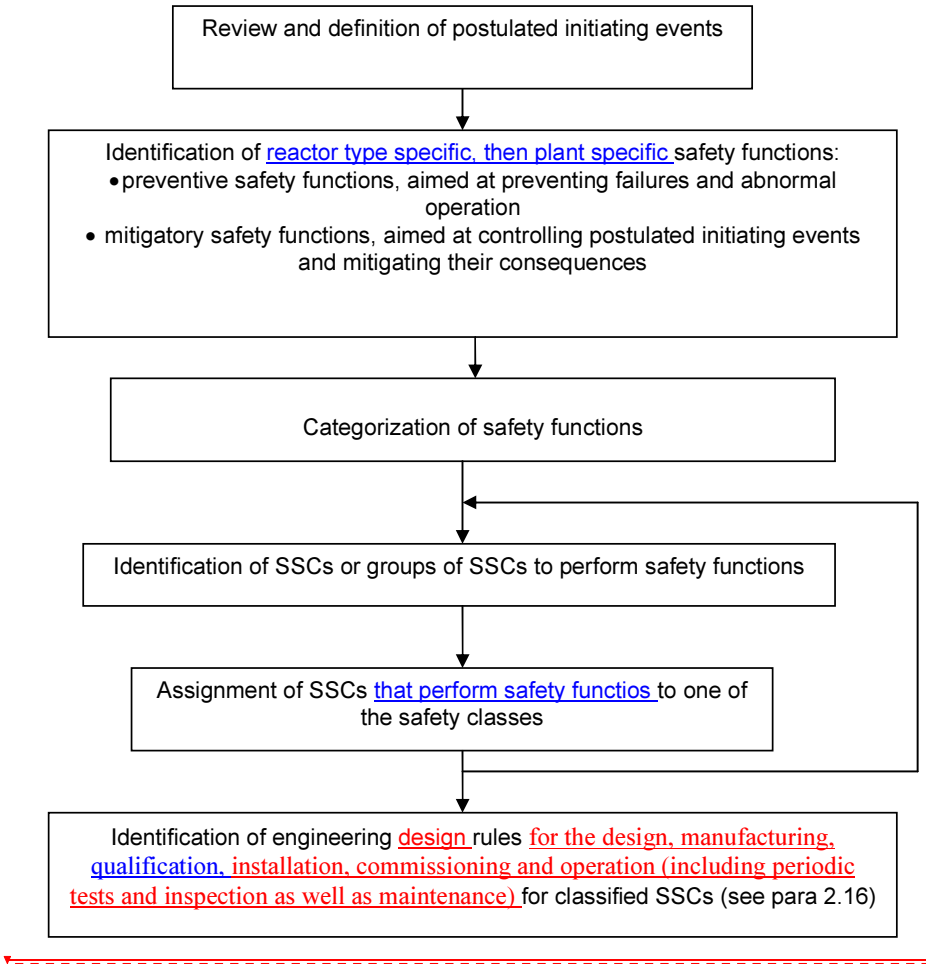
GENERAL APPROACH TO THE SAFETY CLASSIFICATION PROCESS

Deleted: <sp>¶

Deleted: s

Deleted: teps in classifying SSCs.

FIG 1. Main steps in classifying SSCs.



2.7. The approach to safety classification recommended in this Safety Guide involves, broadly, categorization of safety functions, followed by classification of the SSCs. The main steps involved are shown in Fig. 1. The details of the safety classification process, together with explanations of key concepts and terms, are set out in Section 3 and the last step shown in Fig. 1 is set out in Section 4.

2.8. For a specific plant, prerequisites for classifying all SSCs according to their safety significance should be based upon:

- A list of all postulated initiating events[1] considered in the plant design basis;
- The identification of the safety functions needed to achieve the fundamental safety functions (see para 2.6) for the different plant states.

2.9. For new NPPs initially during the design, the postulated initiating events should be arranged in groups in which attributes (or features) of the initiating events are the same (or very similar) (see Ref. [1], para 5.9 and Ref. [10], para. 5.34). Where this simplifies the analysis, one or more PIEs should be selected from the group that bound all aspects of the event that are important to safety.

2.10. The safety functions that prevent and mitigate these postulated initiating events should be derived at an adequate level of detail in order later to identify the SSCs that perform these safety functions. These safety functions will be specific to each plant.

2.11. These plant specific safety functions (see Section 3) should then be categorized into a limited number of categories, on the basis of their safety significance should take into account aspects such as:

- the consequences of the failure of the safety function,
- the frequency of occurrence of the postulated initiating events they prevent or mitigate, and
- the time during which or after which they are required to perform (the time for achieving a controlled state or safe shutdown state, as described in paragraph 3.12.).

Deleted: are the following

Deleted: S

Deleted: implemented

Deleted: Initially

Deleted: properties

Formatted: Font: 12 pt, Complex Script Font: 12 pt

Deleted: At least one significant bounding postulated initiating event should be identified in each group

Deleted: (i.e.

Formatted: Bullets and Numbering

Deleted: the consequences of the failure of the safety function,

[1] As indicated in the IAEA Safety Glossary [9], the primary causes of postulated initiating events may be credible equipment failures and operator errors or human induced or natural events.

2.12. The SSCs or groups of SSCs that work together to perform the plant specific safety functions should then be identified.

2.13. The SSCs are subsequently classified, mainly on the basis of the category of the safety functions they perform. Preliminary safety classifications of SSCs should then be verified applying an appropriate assurance process. In this Safety Guide three classes of SSCs are recommended, based on experience in Member States. However, a larger or smaller number of class may be used if warranted.

Deleted: are
Deleted: subject to
Deleted: cation
Formatted: Font: 12 pt, Complex Script Font: 12 pt

2.14. The safety classification process described in this Safety Guide highlights the significant linkage that exists between design, analysis of postulated initiating events and the consequences of failure of safety functions, and classification of SSCs. In the design process the aims of safety classification are to determine the appropriate engineering design rules for all SSCs and to ensure that SSCs are then designed, manufactured, qualified, constructed, installed, commissioned, quality assured, maintained, tested and inspected to standards appropriate to their safety significance (see Section 4).

Deleted: T
Deleted: is
Deleted: ,

2.15. The basis for the classification and the results of the classification should be documented in an auditable record.

2.16. Safety classification is an iterative process that should be carried out throughout the design process. Any preliminary assignments of SSCs to particular safety classes should be justified using deterministic safety analysis and, where appropriate, probabilistic safety analysis. Engineering judgment could also be used at this stage.

Deleted: possible
Formatted: Font: 12 pt, Complex Script Font: 12 pt

2.17. The safety classification should be performed during plant design, system design and equipment design phases and should be reviewed for any relevant changes during construction, commissioning and commercial operation and subsequent stages in the plant's lifetime.

Deleted: reconsidered

2.18. The safety classification process recommended in this Safety Guide is consistent with the concept of defence in depth that is required in the design process [1]. The preventive safety functions (for use in normal operation) may be associated with defence in depth level 1 and the mitigatory safety functions (for mitigation of the consequences of anticipated operational occurrences and design basis accidents and consequences in excess of acceptance criteria for design extension conditions with defence in depth levels 2 to 4, as described in Refs [1] and [5]. See the chart in Appendix I for further detail.

Deleted: basis accidents)

2.19. Although the precise nature of the steps taken at each stage could vary according to regulatory requirements and the plant design, the safety classification process should include the steps outlined in Section 3. Different methods for the safety classification of SSCs have been used for different types of reactors and in different States for operating nuclear power plants and for new designs. The differences between the various methods are, for instance, the number of classes and the grouping of safety functions.

3. SAFETY CLASSIFICATION PROCESS

3.1. This section describes in detail the step-by-step approach to safety classification of SSCs, as shown in Fig. 1.

ESTABLISHING THE INPUT TO THE CLASSIFICATION PROCESS: REVIEW OF POSTULATED INITIATING EVENTS

3.2 In order to establish the inputs required to start the classification process, the safety objective for the design should be analysed and the specific safety challenges associated with the specific reactor type (or technology) and with a specific plant should be identified, as well as the philosophy for prevention of these challenges and mitigation of their effects. The list of postulated initiating events (or bounding postulated initiating events; see Ref. [2] and para 7.3 of Ref. [11][2]) applicable to the reactor type (or technology) should be reviewed and adapted to the particular plant taking into consideration the relevant internal and external hazards[3] in accordance with the requirement established in Ref. [1], para. 5.8. Grouping or bounding of postulated initiating events should be performed and assessed during the design prior to the safety classification process using deterministic safety analysis and where appropriate, probabilistic safety assessments. The methods are described in Refs [10, 11, 12].

Deleted: safety

3.3. For plant modifications, the newly identified or modified postulated initiating events should be assessed, with account taken of interfaces with existing safety functions and safety classes of SSCs that may be affected.

IDENTIFICATION OF PLANT SPECIFIC SAFETY FUNCTIONS

3.4. At the early stage of design, 'reactor type safety functions', which are necessary to fulfil the fundamental safety functions (see para 2.6) in all plant states, should be identified in accordance with the safety objectives for the design. These comprise preventive safety functions and mitigatory safety functions. Examples of reactor type safety functions for existing designs of light water reactors are provided in Annex I.

Deleted: safety

Deleted: is

[2] A list of bounding postulated initiating events for each reactor type is available in accident studies and is typically provided by the designer.

[3] Postulated initiating events that originate in internal and external hazards (e.g. fire in one electricity supply bus)

3.5. Safety functions that are required for performing the fundamental safety functions should be defined to an adequate level of detail in order to allow the identification of the SSCs that are required for performing these safety functions. Therefore the reactor type safety functions should be broken down to 'plant specific safety functions', which are related to plant specific postulated initiating events (to prevent or mitigate the bounding postulated initiating events).

3.6. The plant specific safety functions are specific to the plant design, and each should be linked to particular bounding postulated initiating events. The plant specific safety functions should be refined in the design process to establish a complete set of safety functions to fulfil the fundamental safety functions. Some plant specific safety functions can be defined to cover more than one postulated initiating event.

3.7. For existing nuclear power plant designs, lists of plant specific safety functions are usually available. In some safety classification schemes, reactor type safety functions are detailed enough such that they can be used as plant specific safety functions and immediately allocated to bounding postulated initiating events.

3.8. The preventive plant specific functions important to safety should be identified at an adequate level of detail in order later to identify the SSCs to keep the plant parameters within their expected normal range (limits for this usually documented in the technical specifications), maintain the integrity of the main confinement barriers[4] (see para. 2.12 of Ref. [1]) and prevent system failures that may cause initiating events. Failures of SSCs can originate from malfunctions, the effect of external and internal hazards or human induced events. Specific events can be ruled out of the plant design basis (for example: rupture of reactor pressure vessel for pressurized water reactors)[5] provided sufficient design provisions or requirements have been implemented or respectively met.

3.9. These preventive plant specific safety functions should ensure that the fundamental safety functions are fulfilled in normal operation. Some plant specific safety functions perform the three fundamental safety functions only indirectly (e.g. safety function (19) in

[4] The confinement barriers are different for different plant designs and include the fuel with its cladding (for example ceramic material of the ceramic fuel itself performes an important barrier function, e.g. in the pebble bed modular reactor), the reactor coolant system boundary and the containment.

[5] Failure of the reactor pressure vessel is nowhere considered as a bounding postulated initiating event, but has to be prevented, because it can not be mitigated in the plant design basis (the vessel is designed and manufactured, tested, maintained according to requirements imposed by the highest safety category/class) and the likelihood of such an event is much lower then the occurrence.

Deleted: to be

Deleted: safety

Deleted: .

Deleted: P

Deleted: ing

Deleted: e

Deleted: support

Deleted: whereby the

Deleted: has an

Deleted: including for

Formatted: Font: 10 pt, Complex Script Font: 10 pt

Deleted: .

Formatted: Font: 10 pt, Complex Script Font: 10 pt

Formatted: Font: 10 pt, Complex Script Font: 10 pt

Formatted: Font: 10 pt, Complex Script Font: 10 pt

Annex I). Preventive plant specific safety functions identified during the early stage of the design should be reviewed.

3.10. Mitigatory plant specific safety functions should be identified at an adequate level of detail in order later to identify the SSCs that control and mitigate the consequences of initiating events such that the relevant safety acceptance criteria are met for all anticipated operational occurrences and design basis accidents and the consequences of designed extension conditions are appropriately reduced.

Deleted: other accidents

Deleted: should

3.11. Safety functions for the mitigation of anticipated operational occurrences detect and intercept deviations from normal operation in order to prevent anticipated operational occurrences from escalating to an accident condition.

Deleted: should

3.12. Safety functions for the mitigation of design basis accidents control accidents within the safety acceptance criteria of the plant's design basis. Mitigatory safety functions for design basis accidents can be subdivided into two levels (A and B – see following paragraphs), depending on the potential consequences of the accident and the time needed to achieve a controlled or safe shutdown state. The two levels are based on the definition of plant states in Ref. [1].

Deleted: ing

Deleted: of

Deleted: ing

Deleted: state

Formatted: Highlight

Deleted: , as described in following paragraphs

Deleted: This subdivision is

3.13. Level A mitigatory safety functions for design basis accidents should establish a controlled state following a design basis accident. A controlled state should be reached as soon as possible. A controlled state can be ensured by means of operator actions or by the active or passive safety systems that control reactivity, heat removal and releases to the environment within prescribed limits.

Deleted: should

Deleted: However automatic means should be preferred to reach the controlled state

3.14. Level B mitigatory safety functions for design basis accidents should:

a) After a controlled state is reached, achieve and maintain a safe shutdown state following a design basis accident;

Formatted: Highlight

b) Minimize the challenge to the remaining barriers (see para. 2.12 of Ref. [1]) from the design basis accident.

These safety functions can be achieved by means of operator actions or by the active or passive safety systems and features that control reactivity, heat removal and radioactive releases to the environment. In a safe shutdown state, plant parameters are well below the design limits for components and structures, the reactor remains sub-critical, decay heat is

Deleted: A safe shutdown state should be ensured

Deleted: within prescribed limits

Formatted: Highlight

removed for as long as necessary and radiological release don't exceed those of normal operation.

3.15. Safety functions for the mitigation of design extension conditions are intended to limit accident progression (e.g. in-vessel mitigation before significant core degradation occurs) and are intended to mitigate the consequences of a severe accident[6] (e.g. ex-vessel mitigation to control the remains of a significantly degraded core).

CATEGORIZATION OF SAFETY FUNCTIONS

3.16. The plant specific safety functions, preventive or mitigatory, which are required to be performed in operational states and in the event of a fault or accident, should be categorized on the basis of their safety significance. The safety significance of each safety function is determined by taking account of the factors (2), (3) and (4) indicated in para. 2.4.

3.17. Factor (2) of para. 2.4 reflects the potential severity of the consequences of failure of a plant specific safety function. The severity is usually divided into three levels, high, medium and low, as assessed assuming that subsequent plant specific safety functions respond as designed (if there are any of them). Notwithstanding, particular attention should be paid to ensure that the probability claimed for its failure is achieved with the selected safety category.

- The severity should be considered 'high' if:
  - The failure of the safety function could lead directly to a release of radioactive material that exceeds the limits for design basis accidents set by the regulatory body; or
  - The values of key physical parameters could challenge or exceed design limits[7] for design basis accidents[8].
- The severity should be considered 'medium' if:

[6] Mitigation of the consequences of severe accidents includes limitation of radiological consequences, control of reactivity excursions, removal of decay heat for as long as necessary, confinement of radioactive material by means of the remaining barriers, and monitoring of the state of the plant and radiation levels.

[7] Also called safety acceptance criteria.

[8] See Requirements 15, 19, 20 and 21 of Ref. [1].

Formatted: Font: 12 pt, Complex Script Font: 12 pt

Deleted: should

Formatted: Font: 12 pt, Complex Script Font: 12 pt

Deleted: consequences in excess of acceptance criteria for design basis accidents

Deleted: should

Deleted: should

Deleted: be

Deleted:

Deleted: follows:

Deleted: specified

Deleted: specified

- The failure of the safety function could at worst lead to a release of radioactive material below the limits for design basis accidents set by the regulatory body; or
- The values of key physical parameters could exceed the design limits for anticipated operational occurrences, but remain within the specified design limits for design basis accidents[8].

- The severity should be considered 'low' if:
  - The failure of the safety function could at worst lead to a release of radioactive material below the limits for the plant conditions for anticipated operational occurrences; or
  - The values of key physical parameters could exceed the specified design limits for normal operation[9], but would remain within the specified design limits for anticipated operational occurrences[8].

3.18. Factor (3) of para. 2.4 reflects the probability that a plant specific safety function will be called upon. This should be taken into account in the categorization of mitigatory safety functions. It should be expressed primarily through the probability of occurrence of postulated initiating events leading to anticipated operational occurrences, design basis accidents and design extension conditions. For preventive safety functions, no differentiation is necessary regarding probability.

3.19. Factor (4) of para. 2.4 reflects the time at which or the period for which a plant specific safety function will be called upon. The time factor should be considered for the control/mitigation of design basis accidents and for design extension conditions. For example, a controlled state should be reached as soon as possible. After a controlled state is reached, a safe shutdown state should be achieved and maintained as long as is necessary. The safety functions that needed to reach and maintain the safe shutdown state may be categorized lower than the safety functions needed to reach the controlled state as there is more time available at which this safety function to be called upon. [10] [11].

[9] The limits specified in the technical specifications.

[10] For example, safety functions F1A, F1B and F2 of the European Utility Requirements for LWR Nuclear Power Plants [8] need to be performed to reach a controlled state or for a safe shutdown state.

Deleted: specified

Deleted: specified

Deleted: 9

Deleted: 9

Deleted: , preferably using automatic means

Deleted: to be performed

Deleted: 7

3.20. Because of the importance of the objective to limit radiological consequences for workers, the public and the environment, and for the purposes of safety classification, particular emphasis should be placed on the barriers aimed at limiting releases of radioactive material (see para. 2.12 of Ref. [1]). Depending on the reactor type (or technology), the emphasis placed on the different barriers (e.g. fuel cladding, pressure boundary and confinement system) might be different. For many reactor types, the integrity function of the reactor coolant boundary plays a very important role[12], not only for retaining radionuclides, but also to ensure sufficient core cooling.[13]

3.21. The safety significance of all plant specific safety functions should be established and each plant specific safety function should be categorized according to the risk[14]. Usually three but for certain new designs four categories may be used[15].

Deleted: in one of the following safety categories

Safety category 1:

- Any preventive plant specific safety function whose failure would result in consequences with a 'high' severity should be assigned to safety category 1.

- Any mitigatory plant specific safety function required to reach a controlled state following a design basis accident or anticipated operational occurrence and whose failure would result in consequences with a 'high' severity or any other design basis accident mitigatory plant specific safety function (requested during the time period of reaching a controlled state) and any other anticipated operational occurrence mitigatory plant specific safety function whose failure would result in consequences with a 'high' severity should be assigned to safety category 1.

Formatted: Font: 12 pt, Complex Script Font: 12 pt

[11] Certain safety functions must be complete by within a defined time, e.g., temperature or pressure sensors that must trigger safety systems before they can be damaged by a PIE-induced hostile environment. See rules in Section4.

Formatted: Font: 10 pt, Complex Script Font: 10 pt

[12] Reference [6] identifies pressure integrity criteria for five different categories of safety functions.

Deleted: 5

[13] Consequently, maintaining the integrity of the reactor coolant boundary is considered in Table 1 a preventive safety function and is assigned to the highest category. The highest category should apply to those components of the reactor coolant boundary where loss of integrity is not covered by mitigatory safety functions, e.g. failure of the reactor pressure vessel. At the other extreme, for those components of the reactor coolant boundary where loss of integrity is already mitigated by operational systems (e.g. failure of a transducer line), safety category 3 would be appropriate.

[14] Risk is understood as a combination of the probability of occurrence of an event and the severity of its consequences [9].

[15] The number of categories is limited to avoid having too many collections of engineering rules. Usually 3 categories used. A special category may be introduced (category 4) for plant specific safety functions mitigating design extension conditions.

Formatted: Font: 10 pt, Complex Script Font: 10 pt

Safety category 2:

- Any preventive plant specific safety function whose failure would result in consequences with a 'medium' severity should be assigned to safety category 2.
- Any mitigatory plant specific safety function required to reach a safe shutdown state following a design basis accident or any other mitigatory plant specific safety function whose failure would result in consequences with a 'medium' severity should be assigned to safety category 2.

Safety category 3:

- Any preventive plant specific safety function designed to keep the main reactor process variables (i.e. the main plant parameters) within their specified ranges for normal operation or any other preventive plant specific safety function whose failure would result in consequences with a 'low' severity (e.g. an anticipated operational occurrence) should be assigned to safety category 3.
- Any mitigatory plant specific safety function designed for early interception of departure from normal operation before a reactor trip is initiated or the safety systems are challenged or any other mitigatory plant specific safety function whose failure would result in consequences with a 'low' severity should be assigned to safety category 3.
- Any mitigatory plant specific safety function designed to limit the consequences of hazards should be assigned at least to safety category 3.
- Even if they are not directly needed to ensure the performance of the fundamental safety functions, any preventive plant specific safety function required to prevent significant staff exposure to direct radiation, or monitoring of radiation level and monitoring of releases of radioactive material at the site should be assigned at least to safety category 3.

Safety category 4:

- Any mitigatory plant specific safety function required to control design extension condition, in order to prevent core melt or to mitigate other high or medium consequences in a design extension condition, should be assigned to safety category 4.

Deleted: consequences in excess of acceptance criteria for design basis accidents

3.22. The plant specific safety functions categorized according to the concepts set out in para. 3.21 are summarized in Table 1. Plant specific safety functions whose failure would lead to

the most severe consequences should be assigned to safety category 1, as described in para. 3.21. Where a safety function could be considered to be in more than one category, depending on events considered, it should be categorized in the highest category.

3.23. By categorizing the plant specific safety functions in accordance with Table 1, engineering design rules (functional requirements such as single failure criterion, diversity, etc.), linked to the applicable safety categories, can be assigned to the plant specific safety functions or to groups of SSCs performing plant specific safety functions. This is further considered in Section 4.

TABLE 1. RELATIONSHIP BETWEEN TYPE OF SAFETY FUNCTION AND SAFETY CATEGORIES FOR PLANT SPECIFIC SAFETY FUNCTIONS

Type of safety function [16]	Severity of the consequences of the failure of plant specific safety functions		
	High	Medium	Low
Preventive functions important to safety	Safety category 1	Safety category 2	Safety category 3
Safety functions for mitigation of anticipated operational occurrences	Safety category 1	Safety category 2	Safety category 3
Safety functions for control/ mitigation of design basis accidents (Time period of level A)	Safety category 1	Safety category 2	Safety category 3
Safety functions for control/ mitigation of design basis accidents (Time period of level B)	Safety category 2	Safety category 3	Safety category 3
Safety functions for mitigation of consequences in design extension conditions	Safety category 4	Safety category 4	No safety category

Deleted: safety

Deleted: No safety category

Deleted: N/A[18]

Deleted: [17]

Deleted: N/A

Deleted: Other safety fun... [1]

[16] Factor (3) and Factor (4) are taken into account indirectly through the type of plant specific safety function

Formatted: Font: 10 pt, Complex Script Font: 10 pt

[19] All SSCs working together to perform one plant specific safety function are in one safety functional group. All safety functional groups (all SSCs) that work together to mitigate the consequences of anticipated operational occurrences and design basis accidents form a 'safety group' (see the IAEA Safety Glossary [9]).

GROUPING OF STRUCTURES, SYSTEMS AND COMPONENTS

3.24. All the SSCs required to perform each plant specific safety function should be identified and grouped into 'safety functional groups'[19]. Depending on the design, a particular SSC can be allocated to more than one plant specific safety function, and thus could be assigned to several safety functional groups.

CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS

3.25. Initially, SSCs (including supporting SSCs) should be assigned to the safety class corresponding to the safety category of the plant specific safety function that they fulfil (see Fig. 2). However, because not all SSCs within a safety functional group may have an equal contribution towards achieving the desired safety function, some SSCs may then be assigned to a different safety class, as described in paras 3.26 and 3.27.

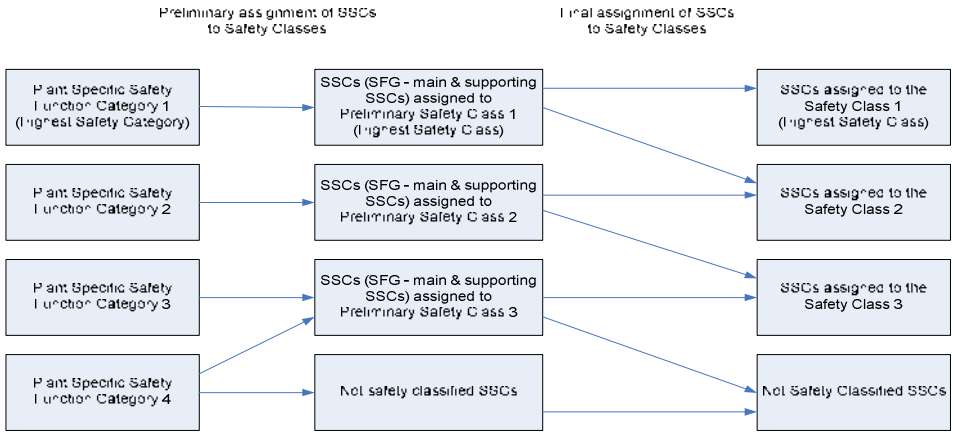


FIG. 2. Assignment of SSCs to safety classes

3.26. If justified by an appropriate safety analysis, a safety class lower than the safety class initially assigned can be proposed for a SSC. For example, an SSC can be assigned to a lower safety class, generally of one level lower, in the following cases:

- The SSC does not directly support the accomplishment of the plant specific safety function in the corresponding safety category;
- The SSC would already be in operation at the moment the postulated initiating event occurs, and would not be affected by it;
- The corresponding plant specific safety function is fulfilled by more than one SSC, providing the following conditions apply:
    - The SSC to be assigned to a lower safety class is less likely to be used;
    - It will be possible to deploy it in time for it to be effective.

3.27. If there are main SSCs (also known as lead SSCs or frontline SSCs[20]) within certain safety functional groups whose failure cannot be accepted because the conditional probability for unacceptable consequences is 1 or close to 1 (e.g. the reactor pressure vessel for light water reactors), then these SSCs should be allocated to the highest safety class, and additional requirements should be specified on a case by case basis.

3.28. Supporting SSCs should be assigned to the same class as that of the frontline SSCs to be supported. The class of a supporting SSC can then be lowered according to the rules set out in para. 3.26.

3.29. If an SSC contributes to the performance of several plant specific safety functions of different categories, it should be assigned to the class corresponding to the highest safety category requiring the most conservative engineering design rules.

3.30. In the classification of SSCs, no account should be taken of whether the operation of the SSC is active or passive, or a mixture.

3.31. Any SSC that is not part of a safety functional group but whose failure could adversely affect this safety functional group in accomplishing its plant specific safety function (if this cannot be precluded by design) should be classified in accordance with the safety category of that safety functional group. The SSC may be later be assigned to a lower safety class depending on the conditional probability of the consequential failure of the safety functional group.

[20] Main SSCs are those SSCs in a safety functional group that, with the support of supporting SSCs, perform the preventive and mitigatory plant specific safety functions.

3.32. 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 not important to safety), interference between the SSCs should be prohibited 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 of a failure of the SSC in the lower safety class. An exception may be made where there is no mechanism to propagate a failure from the lower safety class SSC to the higher safety class SSC (e.g. because of physical separation). See Requirement 60 of Ref. [1].

3.33. By assigning each SSC to a safety class, a set of common engineering design rules can be identified that will ensure that the appropriate quality and reliability is achieved. Recommendations on assigning engineering design rules are provided in Section 4.

VERIFICATION OF THE SAFETY CLASSIFICATION

3.34. The adequacy of the safety classification should be verified using deterministic safety analysis, which should cover all postulated initiating events and all aspects of the prevention of events that are credited in the concept for the design safety of the plant. This should be complemented, as appropriate, by insights from probabilistic safety assessment and should be supported by engineering judgement[21]. Consistency between safety classifications verified using deterministic analyses and probabilistic analyses will provide confidence that the classification is correct. If there are deviations between the safety classifications resulting from probabilistic safety assessment and those from the deterministic calculations, then the more conservative safety classification (i.e. the higher safety class) should be used; however, the methods used will depend on the design information available and national regulations.

Deleted: of

3.35. The safety classification process should be verified in order to confirm that:

a) A complete set of bounding postulated initiating events has been defined;

b) A sufficient set of preventive plant specific safety functions has been provided to prevent system failures which could cause initiating events;

[21] Experts providing engineering judgement, including knowledgeable personnel of the operating organization of the plant, should have expertise in probabilistic safety assessment, safety analysis, plant operation, design engineering and systems engineering.

c) An adequate set of mitigatory plant specific safety functions, including consideration of common cause interactions, is available to maintain the consequences of an event within acceptable limits.

3.36. Safety analysis should confirm that:

a) all the plant specific safety functions are performed by SSCs within safety functional groups;

b) the SSCs in each safety functional group are assigned to the correct safety class and the appropriate engineering design rules are applied;

c) the operational limits or other safety acceptance criteria for each postulated initiating event will be met.

4. SELECTION OF APPLICABLE ENGINEERING DESIGN RULES FOR STRUCTURES, SYSTEMS AND COMPONENTS

4.1. A complete set of engineering design rules should be specified for performing each plant specific safety function. The SSCs in each safety functional group should possess all the design features necessary to achieve the appropriate capability, dependability and robustness.

4.2. The engineering design rules selected should reflect the required quality and should be assigned in accordance with the category of the safety function and the safety class of the SSC. The appropriate codes and standards, with any applicable regulatory limitation including nationally adopted international codes and standards, should be used for determining the engineering design rules for all types of SSCs.

4.3. Engineering design rules are related to the three characteristics of capability, dependability and robustness:

a) Capability is the ability of an SSC to perform its designated safety function as required, with account taken of uncertainties;

b) Dependability is the ability of an SSC within a safety functional group to perform the required plant specific safety function with a sufficiently low failure rate;

c) Robustness is the ability to ensure that no operational loads or loads caused by any associated postulated initiating events on an SSC in a safety functional group will adversely affect the ability of the safety functional group to perform its designated safety function.

SSCs should be designed, manufactured, procured, installed, commissioned, constructed, qualified (included within the scope of the quality assurance program), operated, tested and maintained to ensure the proper capability, dependability and robustness.

4.4. The engineering design rules relating to dependability and robustness of an SSC may be adjusted in accordance with the probability of failure of the SSC and the associated consequences.

4.5. Annex II provides examples of engineering design rules for SSCs of different safety classes, depending on their preventive or mitigatory safety functions.

4.6. Design rules relating to fire protection and fire suppression should be applied as outlined in Ref. [13] for the design of SSCs and as appropriate, for the performance of safety functions.

4.7. The design rules for instrumentation and control and information technology equipment and software should be applied in accordance with the recommendations provided in Refs [14] and [15].

4.8. Quality assurance or management system requirements for the design, qualification, procurement, construction, inspection, installation, testing, surveillance and modification of SSCs should be assigned on the basis of their safety class, in accordance with the requirements established in Ref. [16].

4.9. The seismic categorization of safety related SSCs and SSCs not important to safety should be determined in accordance with the recommendations provided in Ref. [17].

4.10. The environmental qualification of SSCs should be determined in accordance with the conditions associated with normal operation and for postulated initiating events where the SSCs may be called on to operate. At a minimum, environmental qualification should include consideration of humidity, temperature, pressure, vibration, chemical effects, radiation, operating time, ageing, submergence, electromagnetic interference, radio frequency interference and voltage surges, as applicable.

APPENDIX I

SAFETY FUNCTIONS IN RELATION TO THE CONCEPT OF DEFENCE IN DEPTH

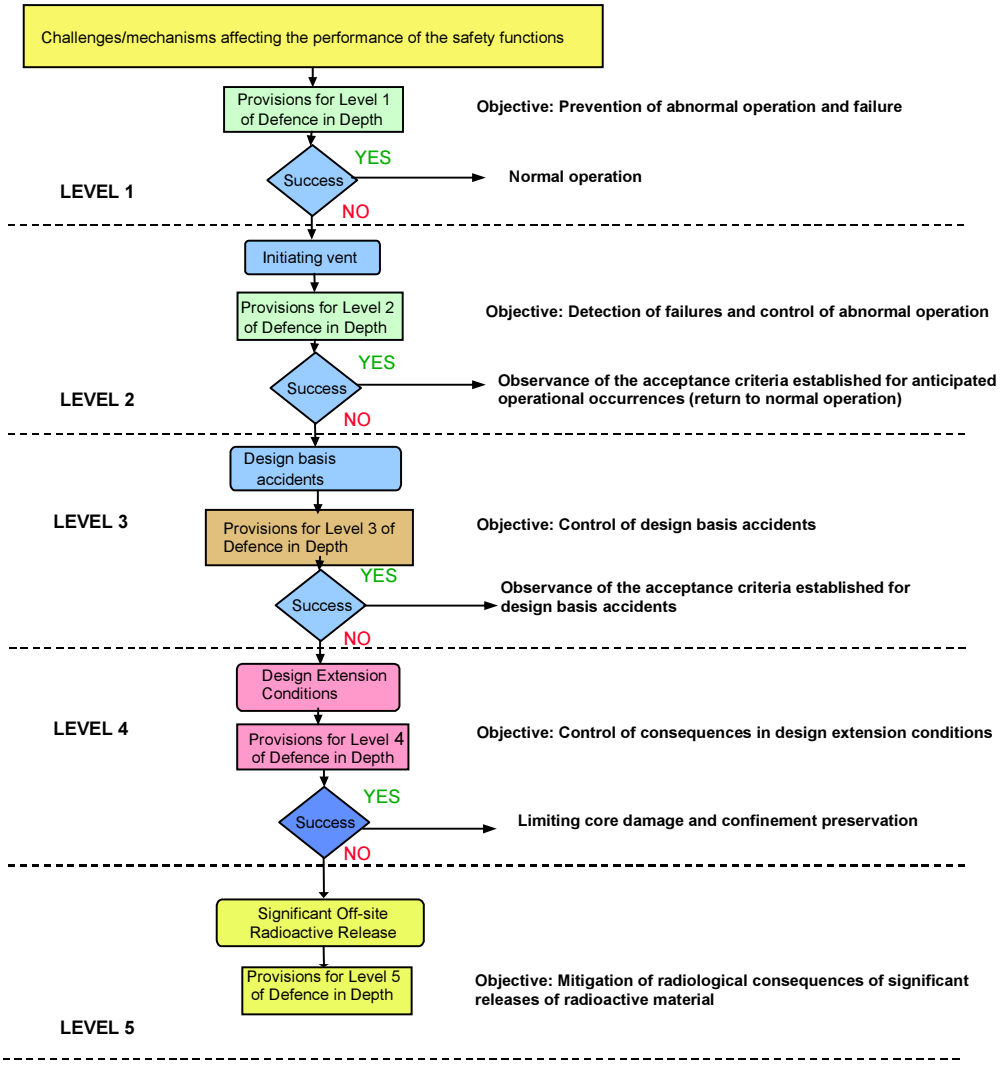


Fig. 3 Logic flow diagram for the allocation of safety functions to levels of defence in depth, showing safety functions and success criteria.

APPENDIX II

RELATIONSHIP BETWEEN DESIGN AND SAFETY ANALYSIS PROCESSES AND THE SAFETY CLASSIFICATION PROCESS

Design and safety analysis processes	**Safety classification process**
Development of the basic objective for the design safety of the nuclear power plant	Review of the applicable postulated initiating events and identification of bounding postulated initiating events
Specification of parameters for normal operating conditions Review of failures of SSCs which could be caused by malfunctions, the effect of external and internal hazards or human induced events Grouping of postulated initiating events,	
Development/review of reactor type safety functions based on the fundamental safety functions for preventing or mitigating bounding postulated initiating events	Assignment of safety functions to bounding postulated initiating events • Review of reactor type safety functions (for preventing initiating events or mitigating each bounding postulated initiating event) • Decomposition of reactor type safety functions into plant specific safety functions (for preventing initiating events or mitigating each bounding postulated initiating event)
Decomposition of reactor type safety functions into plant specific safety functions (for preventing or mitigating each bounding postulated initiating event) at an adequate level of detail in order to allow the identification of the SSCs that are required for performing these safety functions	
Specification of acceptance criteria for plant specific safety functions Conduct of preliminary safety analysis	Categorization of the plant specific safety functions(with consideration given to frequency, consequences of failure and time before the safety function is called upon, for the bounding postulated initiating events)
Definition of safety functional groups (and the list of main and supporting SSCs) to fulfil plant specific safety functions	Review of the safety functional groups (and the list of main and supporting SSCs)
	Assignment of main and supporting SSCs to safety classes (on the basis of the category of their associated plant specific safety function(s))
	• Assignment of functional requirements to the plant specific safety functions • Assignment of engineering design rules to SSCs within each safety functional group
Conduct of final safety analysis	Verification of safety classification

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (20xx).(in preparation).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, IAEA, Vienna (2008).

[3] 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, Main Safety Principles, Safety Fundamentals No. SF-1, Vienna (2006).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

[5] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[6] AMERICAN NUCLEAR SOCIETY, Safety and Pressure Integrity Classification Criteria for Light Water Reactors, ANSI/ANS-58.14, ANS, La Grange Park, Il (1993).

[7] UNITED STATES REGULATORY COMMISSION, NRC Regulatory Guide 1.201, Guidelines for Categorizing Structures, Systems, and components in Nuclear Power plants According to their Safety Significance, USNRC, Washington DC (2006).

[8] BRITISH ENERGY PLC, ELECTRICITÉ DE FRANCE, FORTUM, IBERDROLA, NRG, ROSENERGOATOM, SOGIN, SWISSNUCLEAR, TRACTEBEL, TVO, VATTENFALL, VGB POWERTECH, European Utility Requirements for LWR Nuclear Power Plants, Volumes 2.1 and 2.8, http://www.europeanutilityrequirements.org/

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

Formatted: Font: (Default) Times New Roman, 12 pt, Complex Script Font: Times New Roman, 12 pt

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2010).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-4, IAEA, Vienna (2010).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Software For Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.3, IAEA Vienna (2003).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).

ANNEX I
REACTOR TYPE SAFETY FUNCTIONS FOR LIGHT WATER REACTORS

TABLE I-1. EXAMPLE OF REACTOR TYPE SAFETY FUNCTIONS[22] FOR BOILING WATER REACTORS AND PRESSURIZED WATER REACTORS

Safety functions[23]	Preventive	Mitigatory
(1) to prevent unacceptable reactivity transients;	F1	
(2) to maintain the reactor in a safe shutdown condition after all shutdown actions;	F1	F1
(3) to shut down the reactor as necessary to prevent anticipated operational occurrences from leading to design basis accidents and to shut down the reactor to mitigate the consequences of design basis accidents;	F1	F1
(4) to maintain sufficient reactor coolant inventory for core cooling in and after accident conditions not involving the failure of the reactor coolant pressure boundary;		F2
(5) to maintain sufficient reactor coolant inventory for core cooling in and after all postulated initiating events considered in the design basis;		F2
(6) to remove heat from the core after a failure of the reactor coolant pressure boundary in order to limit fuel damage;		F2
(7) to remove residual heat in appropriate operational states and accident conditions with the reactor coolant pressure boundary intact;	F2	F2
(8) to transfer heat from other safety systems to the ultimate heat sink;		F2
(9) to ensure necessary services (such as electrical, pneumatic, hydraulic power supplies, lubrication) as a support function for a safety system;	F1, F2, F3 supporting	F1, F2, F3 supporting
(10) to maintain acceptable integrity of the cladding of the fuel in the reactor core;	F3	F3
(11) to maintain the integrity of the reactor coolant pressure boundary;	F 2, F3	F2, F3
(12) to limit the release of radioactive material from the reactor containment in accident conditions and conditions following an accident;		F3
(13) to limit the radiation exposure of the public and site personnel in and following design basis accidents and selected severe accidents that release radioactive material from sources outside the reactor containment;		F3
(14) to limit the discharge or release of radioactive waste and airborne radioactive material to below prescribed limits in all operational states;	F3	
(15) to maintain control of environmental conditions within the plant for the operation of safety systems and for habitability for personnel necessary to allow performance of operations important to safety;		F1, F2, F3 supporting

[22] This list of safety functions is taken from the annex of the IAEA Safety Requirements publication, Safety of Nuclear Power Plants: Design, published in 2000. The numbering (in brackets) of the safety functions listed in that annex has been retained for ease of identification.

[23] The three fundamental safety functions are as follows: F1: control of reactivity; F2: removal of heat from the core; F3: confinement of radioactive material.

(16) to maintain control of radioactive releases from irradiated fuel transported or stored outside the reactor coolant system, but within the site, in all operational states;	F3	
(17) to remove decay heat from irradiated fuel stored outside the reactor coolant system, but within the site;	F2	
(18) to maintain sufficient subcriticality of fuel stored outside the reactor coolant system but within the site;	F1	
(19) to prevent the failure or limit the consequences of failure of a structure, system or component whose failure would cause the impairment of a safety function.	F1, F2, F3 supporting	F1, F2, F3 supporting

ANNEX II: EXAMPLES OF ENGINEERING DESIGN RULES FOR SSCS

TABLE II-1 EXAMPLE OF ENGINEERING DESIGN RULES FOR CATEGORIES OF SAFETY FUNCTIONS

SAFETY **CATEGORY**		**CAPABILITY**	**DEPENDABILITY**	**ROBUSTNESS**
Safety Category-1	Preventive	Prevent deviation from design basis accident regulatory limits	Meet regulatory requirements for design basis accidents	Withstand normal operation, anticipated operational occurrence and design basis accident conditions
	Mitigatory	Achieve anticipated operational occurrence and design basis accident regulatory limits as appropriate	Meet regulatory requirements for anticipated operational occurrences and design basis accidents[24] as required	Withstand conditions due to normal operation and postulated initiating events to be mitigated
Safety Category-2	Preventive	Prevent deviation from normal operation regulatory limits.	Meet regulatory requirements for anticipated operational occurrences	Withstand normal operation, and anticipated operational occurrence conditions
	Mitigatory	Achieve anticipated operational occurrence and design basis accident limits as appropriate	Meet regulatory requirements for anticipated operational occurrences and design basis accidents[1] as required	Withstand conditions due to normal operation and postulated initiating events to be mitigated
Safety Category-3	Preventive	Prevent deviation from normal operating limits	Meet requirements for normal operation	Withstand normal operation conditions
	Mitigatory	Achieve anticipated operational occurrence and design basis accident limits as appropriate	Achieve regulatory requirements for normal operation, anticipated operational occurrences and design basis accidents [1] as required	Withstand conditions due to normal operation and postulated initiating events to be mitigated
Safety	Mitigatory	Achieve requirements for design extension	Achieve appropriate regulatory	Withstandconditions due to normal

[24] Regulatory requirements may be deterministically developed or probabilistically developed, and may include requirements such as a target dependability for a mitigation system determined by the national regulatory cut-off probability for a specific event category divided by the probability of occurrence of that specific initiating event.

Category-4		conditions	requirements	operation and postulated initiating events to be mitigated

TABLE II-II EXAMPLES OF ENGINEERING DESIGN RULES FOR SSCS

	CHALLENGES (examples)	DESIGN SOLUTIONS (examples)
CAPABILITY	Failure to perform safety function adequately	• Appropriate code selection • Conservative margins • Material selection • Design qualification
DEPENDABILITY	Effect of : • Single failure • Common cause failure • Errors in design, construction, maintenance and operation • Failure of supporting systems	• Appropriate code selection • Fail-safe design • Reliability/availability • Diversity • Redundancy • Independence • Maintainability • Testability • Material selection • Design qualification • Surveillance methodology
ROBUSTNESS	Effect of : • Internal hazards • External hazards • Harsh and moderate environmental conditions • Induced loads	• Appropriate code selection • Fail-safe design • Material selection • Seismic and environmental qualification • Diversity • Separation

Formatted: Font: (Default) Times New Roman, 12 pt, Complex Script Font: Times New Roman, 12 pt

Formatted: Bullets and Numbering

		• Independence • Maintainability • Testability

TABLE II-III. EXAMPLES OF EGINEERING AND DESIGN RULES AND CODES FOR SSCS BASED ON SAFETY CLASSES

	Preventive safety functions			**Mitigatory safety functions**		
Engineering design rules and codes	**Safety class 1**	**Safety class 2**	**Safety class 3**	**Safety class 1**	**Safety class 2**	**Safety Class 3**
Quality assurance	Nuclear grade	Nuclear grade	Commercial grade[25] or specific requirements	Nuclear grade	Nuclear grade	Commercial grade or specific requirements
Environmental qualification	Harsh or mild[26]	Harsh or mild	Harsh or mild	Harsh or mild	Harsh or mild	Harsh or mild
Pressure retaining components (example codes)[27]	High pressure : C1 Low pressure : C2	High pressure : C2 Low pressure : C3	High pressure : C3 Low pressure : C4	High pressure: C2 Low pressure : C3	C3	C4
Electrical components (IEEE)	1E [II-3]	1E	Non 1E	1E	1E	Non 1E
Instrumentation and control (IEC 61226 category [III-4])[28]	B or C	B or C	B or C	A	B	C

Deleted: D

[25] Commercial Grade practices need to demonstrate that the SSC is capable of performing its safety function consistent with its categorization.

Formatted: Font: (Default) Times New Roman, 10 pt, Complex Script Font: Times New Roman, 10 pt

[26] Harsh or mild environmental conditions; SSCs need to be qualified for normal operation and for postulated initiating events, depending on the environmental conditions at their location in the plant.

[27] C1 indicates quality level 1, for example level 1 of ASME III [II-1] or RCC-M [II-2] (e.g. reactor pressure boundary); C2 indicates quality level 2. for example level 2 of ASME III [II-1] or RCC-M [II-2] (e.g. emergency core cooling system); C3 indicates quality level 3, for example level 3 of ASME III [II-1] or RCC-M [II-2] (e.g. component cooling water system, essential service water system); C4 is a quality class comprising non nuclear grade pressure retaining components with special requirements (for example seismic design, quality requirements): components in class C4 can be designed in accordance with any pressure retaining component design code, with account taken of special requirements (e.g. for the fire system).

[28] Category A denotes functions that play a principal role in the achievement or maintenance of plant safety to prevent design basis accidents from leading to unacceptable consequences. Category B denotes functions that play a complementary role to the category A functions in the achievement or maintenance of plant safety, particularly functions

Seismic qualification	Seismic category 1	Seismic category 1	Specific requirements	Seismic category 1	Seismic category 1	Specific requirements

required to operate after the controlled state has been achieved, to prevent design basis accidents from leading to unacceptable consequences, or to mitigate the consequences of a design basis accident. Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of plant safety.

REFERENCES TO ANNEX II

[II-1] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Boiler and Pressure Vessel Code, Section III: Rules of the Construction of Nuclear Facility Components, ASME, Fairfield NJ (2010).

[II-2] FRENCH SOCIETY FOR DESIGN AND CONSTRUCTION RULES FOR NUCLEAR ISLAND COMPONENTS, Design and Conception Rules for Mechanical Components of PWR Nuclear Islands, RCC-M, AFCEN, Paris (2008).

[II-3] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations, IEEE (2004).

[II-4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions, IEC 61226, IEC, Geneva (2009).

CONTRIBUTORS TO DRAFTING AND REVIEW

ASFAW, K.	International Atomic Energy Agency
BARRETT, A.	Nuclear Regulatory Commission, United States of America
BERBEY, P.	EDF SEPTEN, France
BOUSCASSE, M.	Institute for Radiation Protection and Nuclear Safety, France
COE, I.	AMEC, United Kingdom
COOK, B.	Westinghouse Electric Company, United States of America
EL-SHANAWANY, M.	International Atomic Energy Agency
ERASMUS, L.	Pebble Bed Modular Reactor (Pty) Ltd, South Africa
FIL, N.	OKB Gidropress, Russian Federation
FISCHER, K.C.	TÜV, Germany
GASPARINI, M.	International Atomic Energy Agency
HAKATA, T.	Nuclear Safety Commission, Japan
HIDAKA, A.	Japan Atomic Energy Agency, Japan
HILL, R.	ERIN Engineering, United States of America
IMBRO, G.	Nuclear Regulatory Commission, United States of America
INABE, T.	Japan Atomic Energy Agency, Japan
JOHNSON, G.	International Atomic Energy Agency
KADAMBI, P.	American Nuclear Society Standards Board, United States of America
LINN, M.	Oak Ridge National Laboratory, United States of America
MATHET, E.	AREVA, France
MIRANDA, S.	US Nuclear Regulatory Commission, United States of America
PETZER, C.	Pebble Bed Modular Reactor (Pty) Ltd, South Africa
POULAT, B.	AREVA, France
RENSBURG, J.	Pebble Bed Modular Reactor (Pty) Ltd, South Africa
SHCHEKIN, I.	OKB Gidropress, Russia
TOTH, C.	International Atomic Energy Agency
TRICOT, N.	International Atomic Energy Agency

VALTONEN, K.	Radiation and Nuclear Safety Authority, Finland
VAYSSIER, G.	Nuclear Service Corporation, Netherlands
WAAS, U.	AREVA NP GmbH, Germany
ZAISS, W.	FORATOM, Germany

Other safety functions	No safety category