DS367 rev 6.7.
Date: January 2013

IAEA SAFETY STANDARDS

for protecting people and the environment

Status: for submission to CSS for endorsement

- **with resolution of Member States and NUSSC members' comments**
- **According to NUSSC decision 34.5, this new revision has been prepared by the core group and it reflects the consensus reached during the CS meeting hold in January 2013.**

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

DRAFT SAFETY GUIDE

DS367

New Safety Guide

IAEA : International Atomic Energy Agency

CONTENTS

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 methods for safety classification of structures, systems and components (SSCs) have evolved in the light of lessons learned during the design and operation of existing plants. Although the concept of a safety function as being what must be accomplished for safety has been understood for many years, the process by which SSCs important to safety can be derived from the fundamental safety objective has not been described in earlier IAEA Safety Guides dealing with SSC classification. Therefore, the classification schemes used in practice to identify those SSCs deemed to be of the highest importance to safety have, for the most part, been based on experience and analysis of specific designs.

1.2. This Safety Guide was prepared under the IAEA programme for safety standards for nuclear power plants. A 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Reactor (PWR), and Pressure Tube Reactor (PTR) Plants was issued in 1979 as IAEA Safety Series No. 50-SG-D1, but was withdrawn in 2000 because the recommendations contained therein were considered not to comply with the IAEA Safety Requirements publication NS-R-1, Safety of Nuclear Power Plants: Design, published in 2000.

1.3. In developing this Safety Guide, relevant IAEA publications have also been considered. This includes the Fundamental Safety Principles [1], and the Safety Requirements publications on Safety of Nuclear Power Plants: Design [2] and Safety Assessment for Facilities and Activities [3].

1.4. The goal of safety classification is to identify and classify those SSCs that are needed to protect people and the environment from harmful effects of ionizing radiation, based on their roles in preventing accidents, or limiting the radiological consequences of accidents should they occur. On the basis of their classification, SSCs are then designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained in accordance with established processes that ensure design specifications and the expected levels of safety performance are achieved. In accordance with Ref. [2], all items important to

safety are required to be identified and classified on the basis of their functions and their safety significance[1].

1.5. In preparing this Safety Guide, the existing safety classification methodologies applied in operating nuclear power plants and for new designs have been widely reviewed. This Safety Guide also describes the steps of safety classification, which are often not systematically expressed and documented in national classification schemes.

OBJECTIVE

1.6. This publication is primarily intended for use by organizations involved in the design of nuclear power plants, as well as by regulatory bodies and their technical support organizations. It might also be applicable to other nuclear facilities given appropriate adjustments relevant to the specific design of the type of facility being considered.

1.7. The objective of this Safety Guide is to provide recommendations and guidance on how to meet the requirements established in Refs [2] and [3] for the identification of SSCs important to safety and for their classification on the basis of their function and safety significance. This is to ensure a high level of safety by meeting the associated quality requirements and reliability targets. The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology (SSR 2/1 Requirement 18).

SCOPE

1.8. This Safety Guide applies to the design of all SSCs important to safety for all plant states, including all modes of normal operation, during the lifetime of a nuclear power plant.

1.9. This Safety Guide is written in technology-neutral terms. The approach proposed is intended to apply to new nuclear power plants and may not be applicable to existing plants built with earlier classification principles. How this Safety Guide is applied to such nuclear power plants is a decision for individual States.

[1] Factors relevant for determining the safety significance of items important to safety are set out in para 5.34 of Ref. [2].

STRUCTURE

1.10. Section 2 provides the basis and general principles for identifying the SSCs to be classified and for assessing their individual safety significance on which their ranking is established. Section 3 recommends a process for undertaking the safety classification of SSCs that applies these principles. Section 4 provides general recommendations on selecting the engineering design rules for SSCs on the basis of their safety classes.

2. GENERAL APPROACH

2.1. The general approach is to provide a structure and method for identifying and classifying SSCs important to safety on the basis of their functions and safety significance. Once SSCs are classified, appropriate engineering rules can be applied to ensure that they are designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained with sufficient quality to fulfil the functions that they are expected to perform and, ultimately the main safety functions[2], in accordance with the safety requirements of Ref. [2].

BASIS REQUIREMENTS

2.2. The basic requirements for classification are established in Ref. [2] and are reproduced here for convenience. Additional related requirements are established in Ref. [3].

Requirement 4 of SSR-2/1 (Ref. [2]): Fundamental safety functions

Fulfilment of the following fundamental safety functions (*) for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

A systematic approach shall be taken to identifying those items important to safety that are necessary to fulfil the fundamental safety functions **(*)** and to identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions **(*)** for all plant states.

Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled.

Requirement 18 of SSR-2/1 (Ref. [2]): Engineering design rules

The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology.

Requirement 22 of SSR-2/1 (Ref. [2]): Safety classification

All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

[2] According to the IAEA Safety Glossary [4], the formerly named ‘fundamental safety functions’ are now named ‘main safety functions’. In any quotation of IAEA safety standards, the term fundamental safety function is to be understood as main safety function” and is identified with (*) in the text.

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 and expert judgement, with due account taken of factors such as:

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

(b) The consequences of failure to perform the safety function;

(c) The frequency with which the item will be called upon to perform a safety function;

(d) 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.

The design shall be such as to ensure that any interference between items important to safety will be prevented, and in particular that any failure of items important to safety in a system in a lower safety class will not propagate to a system in a higher safety class.

Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment.

Requirement 27 of SSR-2/1 (Ref. [2]):: Support service systems

Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.

GENERAL RECOMMENDATIONS

2.3. Safety classification is an iterative process that should be carried out periodically throughout the design process and maintained during the plant life time. Any assignment of SSCs to particular safety classes should be justified using deterministic safety analysis complemented by insights from probabilistic safety assessment and supported by engineering judgment.

2.4. Safety classification should be performed during the plant design, system design and equipment design phases and should be reviewed for any relevant changes during construction, commissioning, operation and subsequent stages of the plant’s lifetime.

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

2.6. The safety classification process recommended in this Safety Guide is consistent with the concept of defence in depth set out in Ref. [2]. The functions[3] performed at all five levels of defence in depth should be considered and the associated SSCs then classified. Similarly, design provisions should also be classified (see 3.8 and 3.9).

2.7. The basis for the classification and the results of the classification should be documented in an auditable record. The final classification of SSCs should be complete and available for audit by the organization(s) responsible for quality assurance and by the regulatory body. As classifications may be affected by subsequent design changes to the plant (throughout its operating life), the classification records should be included in the management system as part of the plant configuration control.

OUTLINE OF THE SAFETY CLASSIFICATION PROCESS

2.8. This Safety Guide proposes a structured process for identifying and classifying the SSCs, which is illustrated in Figure 1.

2.9. Classification is a top down process that begins with a basic understanding of the plant design, its safety analysis and how the main safety functions will be achieved. Using this information, the functions and design provisions (see para 3.9) required to fulfil the main safety functions are systematically identified for all plant states, including all modes of normal operation. Using information from safety assessment, such as the analysis of postulated initiating events, the functions are then categorized on the basis of their safety significance. The SSCs belonging to the categorized functions are then identified and classified on the basis of their role in achieving the function. A SSC implemented as a design provision should however be directly classified because of the significance of its postulated failure fully defines its safety class without any need for detailed safety function category analysis.

[3] For the purpose of this safety guide, a function is defined as any action performed by a single SSC or a set of SSCs.

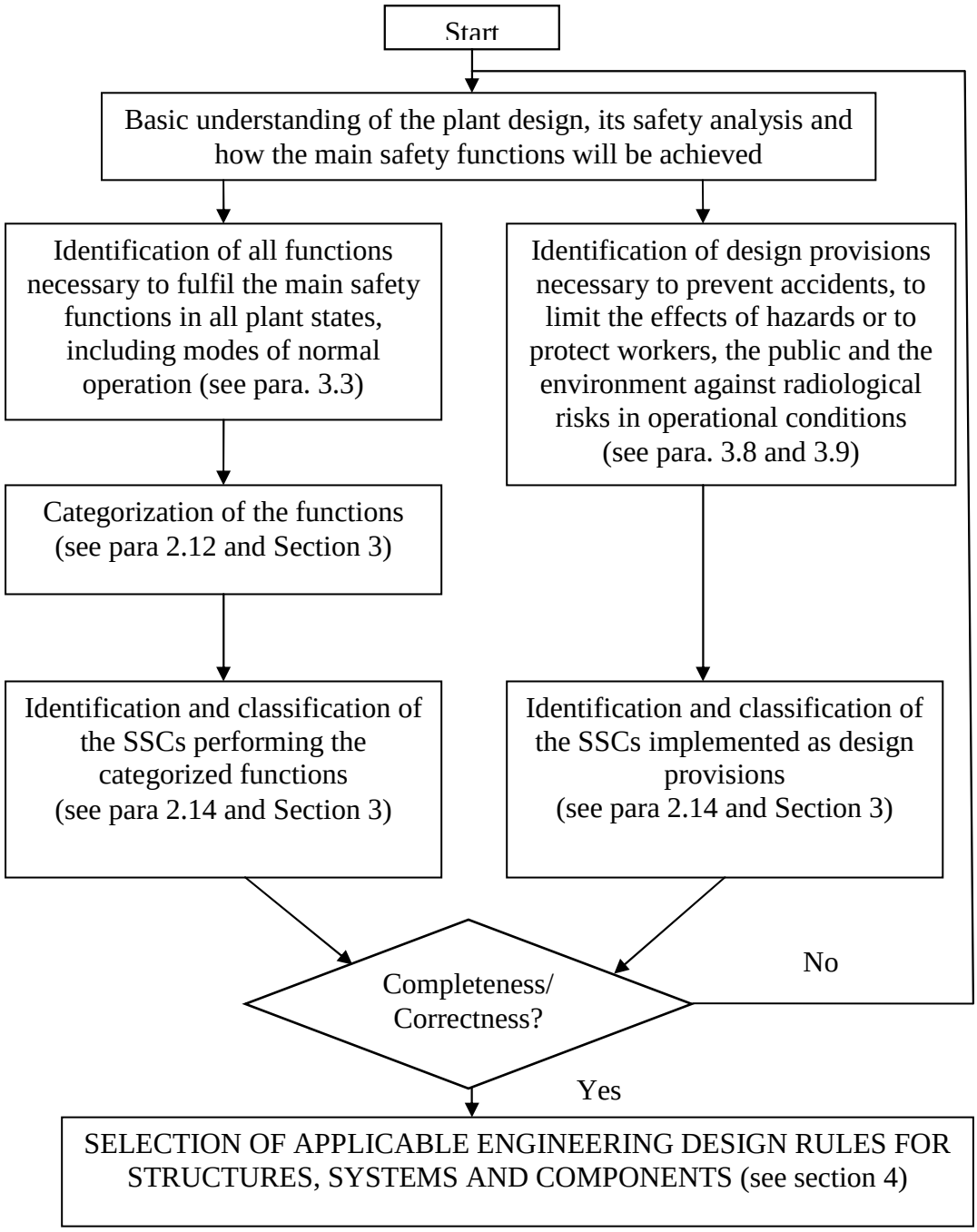

FIG. 1: Flowchart indicating the classification process

2.10. 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[4], as required in Ref. [2], Requirement 16.The frequency of occurrence of the postulated initiating events, as considered in the design of the nuclear power plant.

2.11. All functions and design provisions necessary to achieve the main safety functions (as defined in Ref. [2], Requirement 4) for the different plant states, including all modes of normal operation, should be identified.

2.12. The functions should then be categorized into a limited number of categories on the basis of their safety significance, using an approach which takes account of the following factors:

1) The consequences of failure to perform the function;
2) The frequency of occurrence of the postulated initiating event for which the function will be called upon;
3) The contribution of the function to reach either the controlled or the safe state as defined in Ref. [2].

2.13. Categorization of the functions provided by design provisions is not necessary because the safety significance of the SSC can be directly derived from the consequences of its failure. design provisions can therefore be directly assigned to a safety class without the need for a further analysis of safety function categories.

The next step in the process should be to determine the safety classification of all SSCs important to safety. The main approach followed should be to use deterministic methodologies, complemented where appropriate by probabilistic safety assessment and engineering judgment to achieve an appropriately shaped risk profile, i.e. a plant design where high consequence events have a very low predicted frequency of occurrence. The overall intent is illustrated schematically in Fig. 2.

[4] As stated in Ref. [2], para. 5.9, "The postulated initiating events used for developing the performance requirements for the items important to safety in the overall safety assessment and the detailed analysis of the plant shall be grouped into a specified number of representative event sequences that identify bounding cases and that provide the basis for the design and the operational limits for items important to safety."

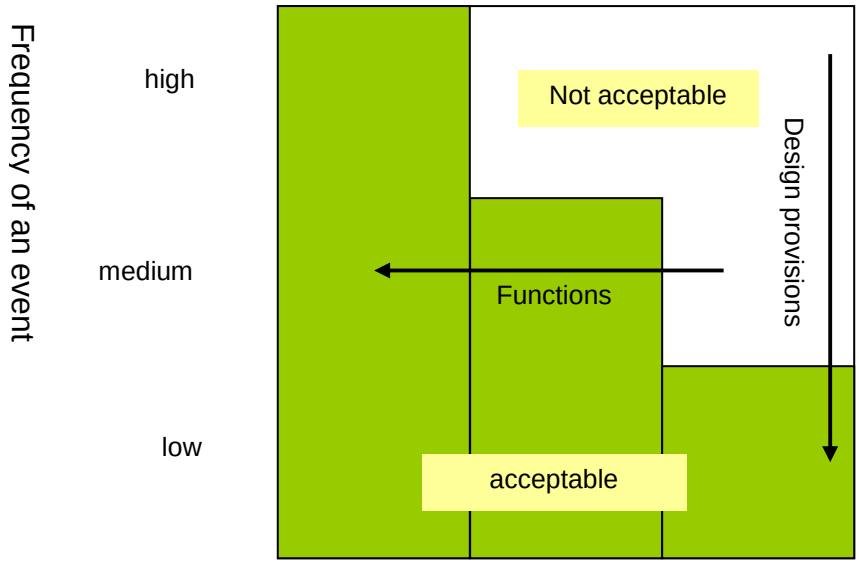

FIG. 2: Diagram indicating the basic principle of frequency vs. consequences

2.14. To achieve this aim, the SSCs needed to perform functions should be identified and classified into a limited number of classes based on their safety significance, using a process that takes into account the factors indicated in Requirement 22 of Ref [2]:

2.15. The SSCs implemented as design provisions should also be identified and classified using the same set of classes as those used for the classification of SSCs needed to perform safety functions.

2.16. Based on the experience of the Member States, in this Safety Guide three safety categories for functions and three safety classes of SSCs important to safety are recommended. Other approaches, utilising a larger or smaller number of categories and classes may be used provided these align with the guidance in paragraphs 2.12 and 2.14.

3. SAFETY CLASSIFICATION PROCESS

3.1. This section provides more detailed guidance on the identification of functions to be categorized and SSCs to be classified, to ensure that all items that are essential to protect people and environment from harmful effects of ionizing radiation will be captured.

IDENTIFICATION OF FUNCTIONS TO BE CATEGORIZED

3.2. For the purposes of simplification, 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.

3.3. 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 credited in the safety analysis and should include all levels of defence in depth, i.e. prevention, detection, control and mitigation safety functions.

3.4. 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.

3.5. 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 credited in the safety analysis.

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

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

IDENTIFICATION OF DESIGN PROVISIONS

3.8. The safety of the plant is also dependent on the reliability of different types of features some of which are designed specifically for use in normal operation. For the purpose of this guide, these SSCs are termed “design provisions”. These provisions need to be identified and

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

3.9. Design provisions that fall into this category are:

- Design features that are designed to such a quality that the failure could be practically eliminated [5]. For these design features, the plant design does not require an independent safety system to be available to mitigate the effects of their failure. Examples of these are the shells of reactor pressure vessels or steam generators. These design features can be readily identified by the high consequences that can be expected should they fail.
- Features that are designed to reduce the frequency of accident. Examples of these are 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 the harmful effects of radiation during normal operation. Examples of these are 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. Examples of these are concrete walls between components that are built specifically for this purpose.
- Features that are designed to prevent a postulated initiating event from developing into a more serious sequence without the occurrence of another independent failure. Examples of these are anti-whipping devices and fixed points.

SSCs which provide the design provisions should be directly classified as safety class 1, 2 or 3, depending on the outcome of the assessment of the consequences of their failures.

[5] The possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high level of confidence to be extremely unlikely to arise.

CATEGORIZATION OF FUNCTIONS

3.10. 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. The safety significance of each function is determined by taking account of the factors indicated in para. 2.12. In the approach recommended in this Safety Guide, the severity of consequences (factor 1) is divided into three levels (high, medium and low) on the basis of the worst consequences that could arise if the function was not performed, as defined in para 3.11.

3.11. The three levels of severity should be defined as follows:

- 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[6].
- The severity should be considered 'medium' if failure of the function could, at worst:
    - Lead to a release of radioactive material that exceeds limits established for anticipated operational occurrences; or
    - Cause 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.

The assessment of the consequences is made postulating that the function does not respond when challenged.

For AOOs, the assessment of the consequences should be made assuming the correct response in due time of all other any independent functions to avoid an excessive categorization.

[6] See Requirements 15 and 19 of Ref. [2].

3.12 Factor 2 (see para. 2.12) reflects the frequency that a function will be called upon. This frequency should be evaluated primarily in accordance with the frequency of occurrence of the respective postulated initiating event.

3.13. By including factors 1 and 2, the approach to classification recommended here is in line with the commonly agreed design principle that events with the most significant consequences ought to have the lowest frequency of occurrence. This means, for example that functions dedicated to the mitigation of the consequences of severe accidents may involve less stringent engineering design rules than those applied for functions for mitigation of the consequences of design basis accidents, because the frequency is lower. Figure 2 illustrates this approach.

3.14. Factor 3 (see para. 2.12) is about assessing the Categorisation of functions in relation to the intended state of the plant that the implementation of the function is intended to achieve. Generally two states are distinguished, first the controlled state then the safe state which can be found in the definitions section of Ref 2{SSR2/1}. The controlled state is for functions where the main focus is on acting automatically or in the short term to considerably reduce the potential for hazard. The safe state tends to focus on longer term functions once the controlled state has been achieved. For reactors, many accident transients will achieve the controlled state first before achieving the safe state. Typical functions for the controlled state are reactor trip, decay heat removal and safety injection whereas depressurising the reactor and connecting up residual heat removal system to ensure long term decay heat removal function is a good example of a function achieving the safe state.

3.15. The categorization recommended in this Safety Guide is based on the following three safety categories:

Safety category 1

> Any function required to reach the 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 the 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 backup 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.

3.16. The categorizations defined in para 3.15 are summarized in Table 1. Where a function could be considered to be in more than one category (e.g. because the function is needed for more than one postulated initiating event), it should be categorized in the highest category.

TABLE 1: RELATIONSHIP BETWEEN FUNCTIONS CREDITED IN THE ANALYSIS OF POSTULATED INITIATING EVENTS AND SAFETY CATEGORIES

Functions credited in the safety assessment	Severity of the consequences if the function is not performed		
	High	Medium	Low
Functions to reach the controlled state after anticipated operational occurrences	Safety category 1	Safety category 2	Safety category 3
Functions to reach the controlled state after design basis accidents	Safety category 1	Safety category 2	Safety category 3-
Functions to reach and maintain a safe state	Safety category 2	Safety category 3-	Safety category 3-
Functions for the mitigation of consequences of a design extension condition	Safety category 2 or 3 (see para. 3.15)	* Not- - categorized	* Not- - categorized

* A medium or low severity is not expected to occur in case of a non response of the dedicated DEC function.

CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS

3.17. Once the safety categorization of the functions is completed, the SSC performing these functions should be assigned to a safety class.

3.18. All the SSCs required to perform a function that is safety categorized to safety should be identified and classified according to their safety significance following a process that takes into account the factors indicated by Requirement 22 of Ref [2] and recalled in para 2.2.

3.19. Applying factors a) and c),SSCs (including supporting SSCs) that are designed to carry out identified functions should initially be assigned to the safety class corresponding to the safety category of the function to which they belong. In the approach recommended in this Safety Guide, three classes are proposed consistent with the three categories recommended in para 3.15.

The initial classification should then be amended as necessary to take factors b) and d).

For factor d), consideration of the time following a postulated initiating event before the function is called upon may permit the SSC to be moved into a lower class provided its

reliability can be demonstrated Demonstration may use for example time to repair or maintain (etc) the SSC, or the possibility of using alternative SSCs within the time window available to perform the required safety function.

3.20. If a 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).

3.21. Applying these and other relevant considerations (e.g. engineering judgement), the final safety class of the SSC should then be selected.

3.22. As explained in para.2.9, design provisions can be directly classified according to the severity of consequences of their failures:

- 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.

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.

3.23. 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 of the failure of the function .

3.24. 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 a SSC not classified), 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 from a failure of the SSC in the lower safety class.

3.25. 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. Recommendations on assigning engineering design rules are provided in Section 4.

VERIFICATION OF THE SAFETY CLASSIFICATION

3.27. 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[7].

The reliability contribution of the SSC to the overall plant risk.is an important factor in the assignment of its safety class .Consistency between the deterministic and probabilistic approaches will provide confidence that the safety classification is correct. Generally it is expected that probabilistic criteria for safety classification should match those derived deterministically. If there are differences however, 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 should be iterative, keeping in step with and informing the evolving design.

[7] Expert groups providing engineering judgement should include knowledgeable personnel from the operating organization of the plant, and personnel with skills and expertise in probabilistic safety assessment, safety analysis, plant operation, design engineering and systems engineering.

4. SELECTION OF APPLICABLE ENGINEERING DESIGN RULES FOR SSC

The engineering design rules are the relevant national or international codes ,standards and proven engineering practices that should be appropriately applied to the design of SSCs to meet the applicable design requirements.

4.1. Once the safety class of the SSCs is established, corresponding engineering design rules should be specified and applied. The engineering design rules should be chosen so that the plant design meets the objective that the most frequent postulated initiating events yield little or no adverse consequences, while more extreme events (those having the potential for the greatest consequences) have a very low probability of occurrence – see Figure 2.

4.2. Engineering design rules are related to the three characteristics of capability, reliability (dependability) and robustness:

a) Capability is the ability of an SSC to perform its designated function as required;

b) Reliability (dependability) is the ability of an SSC to perform its required function with a sufficiently low failure rate consistent with the safety analysis;

c) Robustness is the ability to ensure that no operational loads or loads caused by postulated initiating events will adversely affect the ability of the SSC to perform its function.

These characteristics should be defined taking into account uncertainties in performance and operating conditions.

4.3. A complete set of engineering design rules should be specified which ensure that SSCs will be designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained to appropriate quality standards. To achieve this, the design rules should identify appropriate levels of capability, reliability (dependability) and robustness. The design rules should also take due account of regulatory requirements relevant to safety classified SSCs.

4.4. It is reasonable to distinguish between design requirements that apply at the system level and design requirements that apply to individual structures and components:

- Design requirements applied at the system level may include specific requirements such as single failure criteria, independence of redundancies, diversity, testability, etc.

- Design requirements applied for individual structures and components may include specific requirements such as environment and seismic qualification, manufacturing quality assurance procedures, etc. They are typically expressed by specifying the codes or standards that applies.

4.5. The licensee or applicant should provide and justify the correspondence between the safety class and the associated engineering design and manufacturing rules, including the codes and/or standards that apply.to each SSC.

4.6 Once the engineering design requirements are identified for systems and their individual components it should be checked that the system can performed its function with the reliability assumed in the safety analysis.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012).

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

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

CONTRIBUTORS TO DRAFTING AND REVIEW

Barbaud, J.	Electricité de France, France
Bassing, G.	FORATOM-ENISS Reactor Safety Group,
Cook, S.	Canadian Nuclear Safety Commission, Canada
Erasmus, L.	Pebble Bed Modular Reactor, South Africa
Fil, N.	OKB Gidropress, Russian Federation
Fischer, K.C.	TÜV Nord Sys Tec GmbH & Co. KG, Germany
Froehmel, T.	World Nuclear Association, CORDEL Group
Hamon, D	General Electric Hitachi
Head, J.	General Electric Hitachi
Inabe, T.	Japan Atomic Energy Agency, Japan
Jarvinen, M.J.	Radiation and Nuclear Safety Authority, Finland
Jennings, R.	HSE- Office for Nuclear Regulations, United Kingdom
Jung, I.	Nuclear Regulatory Commission, United States of America
Klapp, U.	AREVA, Germany
Leong, J.	General Electric Hitachi
Matsumoto, T	Japan Nuclear Energy Safety, Japan
Nunighoff, K.	Gessellschaft fur Anlagen und Reaktorsichereit, Germany
Petzer, C.	Pebble Bed Modular Reactor, South Africa
Poulat, B.	International Atomic Energy Agency (Technical Secretary)
Rensburg, J.	Pebble Bed Modular Reactor, South Africa
Ringdahl, K.	Vattenfall Research and Development, Sweden
Shchekin, I.	OKB Gidropress, Russian Federation

Toth, C.	International Atomic Energy Agency
Tricot, N.	International Atomic Energy Agency
Upton, H.A.	General Electric Hitachi
Valtonen, K.	Radiation and Nuclear Safety Authority, Finland
Wattelle, E.	Institute for Radioprotection and Nuclear Safety, France
Waddington, J.	World Nuclear Association