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

February 2011 version submitted to NUSCC Members

Since November 2011, simplified version prepared by Core Team and Reviewed in NS-SSCS (Asfaw)

For submission to NUSSC Members for submission to CSS

Including NUSSC Members comments (November 2012)

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, and the existing 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 the classification. Therefore, it was mainly on the basis of experience and analysis of specific designs that classification schemes identified SSCs that were deemed to be of the highest importance in maintaining safe operation of the facility.

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Reactor (PWR), and Pressure Tube Reactor (PTR) Plants was issued in 1979 as IAEA Safety Series No. 50-SG-D1 and was withdrawn in the year 2000 because the recommendations contained therein were considered not to comply with the IAEA Safety Requirements publication NS-R-1, Safety of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 the SSCs that are ~~essential~~ needed to protect people and environment from harmful effects of ionizing radiation, ~~irrespective of~~ considering 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, operated, tested, inspected and maintained in accordance with established processes that ensure the achievement of the design specifications and the expected ~~required level of~~ safety performance. 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. For the preparation of this Safety Guide, the existing safety classification methodologies applied in operating nuclear power plants and for new designs have been widely reviewed. ~~The general approach and method of classification provided in this Safety Guide reflect the expectations of the regulatory body to justifying a classification~~. Furthermore, this Safety Guide describes the steps of safety classification, which are often not systematically expressed and documented in national classification schemes.

OBJECTIVE

1.6~~7~~. This publication is primarily intended for use by organizations involved in the design of nuclear ~~facilities~~power plants, as well as by regulatory bodies and their technical support organizations for the conduct of regulatory activities. It might be applicable to other nuclear facilities with some adjustments to include the specifity of each type of facility.

1.7~~6~~. 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 accordingly. The engineering design rules for items important to safety at a nuclear ~~facility~~ 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).

~~1.7. This publication is primarily intended for use by organizations involved in the design of nuclear facilities, as well as by regulatory bodies and their technical support organizations for the conduct of regulatory activities.~~

SCOPE

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

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

1.9. The approach proposed in this Safety Guide is intended to apply to new ~~facilities~~ nuclear power plants and might not be fully applicable to existing ~~facilities~~ nuclear power plants that were built with earlier classification principles. The way in which this Safety Guide would be applied to such ~~facilities~~ nuclear power plants is a decision for individual States.

1.10. This Safety Guide is written in technology neutral terms and it is primarily aimed at the design and safety review of nuclear power plants.

STRUCTURE

1.11. Section 2 provides the basis and general approach recommended for identifying the SSCs to be classified and assessing their individual safety significance on which their ranking is established. Section 3 details the safety classification process. Section 4 provides general recommendations on determining the engineering design rules for functions and SSCs on the basis of their safety categories and safety classes respectively. Annex I provides an example of a set of engineering rules for systems performing functions of different safety categories. ~~Annex II provides an example of a set of engineering rules for the design and manufacturing of pressure retaining components of different 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, 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 a 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 ~~are~~ is identified with (*) in the text.

Requirement 27: Support service systems

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

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.

GENERAL RECOMMENDATIONS

2.3. Safety classification is an iterative process that should be carried out throughout the design process and maintained during the plant life time. Any ~~preliminary~~ 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 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 the different

[3] A function is an action performed by a system or systems

levels of defence in depth are considered. The design provisions[4] or any function needed to keep the plant within normal conditions may be associated with the first level of defence in depth and the functions for the control and/or mitigation of anticipated operational occurrences, design basis accidents and design extension conditions, with the second to fifth levels of defence in depth.

2.7. The basis for the classification and the results of the classification should be documented in an auditable record, including a configuration management programme. 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. ~~If the final classification of SSCs is not available prior to granting authorization for a nuclear power plant, it should be demonstrated that a suitable design verification and change control process exists that has been independently validated by the licensee or applicant and the regulatory body.~~

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. This classification process is a top down process that begins with the basic understanding of the plant design, its safety analysis and how the main safety functions are achieved. Using this information, the functions and design provisions 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, following a ~~constant~~ risk approach as described in para. 2.12 and Section 3. The SSCs belonging to the categorized functions are then identified and classified on the basis of their role in achieving the function. ~~The~~ A SSC~~s~~ implemented as design provision~~s~~ can be directly classified ~~directly~~ because the significance of ~~their~~ its failure is ~~direct~~.sufficient enough to assign it to a safety class.

[4] A design provision is a single SSC that maintains the plant within its acceptable operating range, i.e. normal operation. This ensures that radiation doses to workers and the public do not exceed prescribed limits and are kept as low as reasonably achievable in operational conditions. Design Provisions are also needed to prevent accidents not considered in the design basis, to reduce the occurrence of accidents or to limit the effects of hazards. For examples of application, see guidance provided in para 3.9.

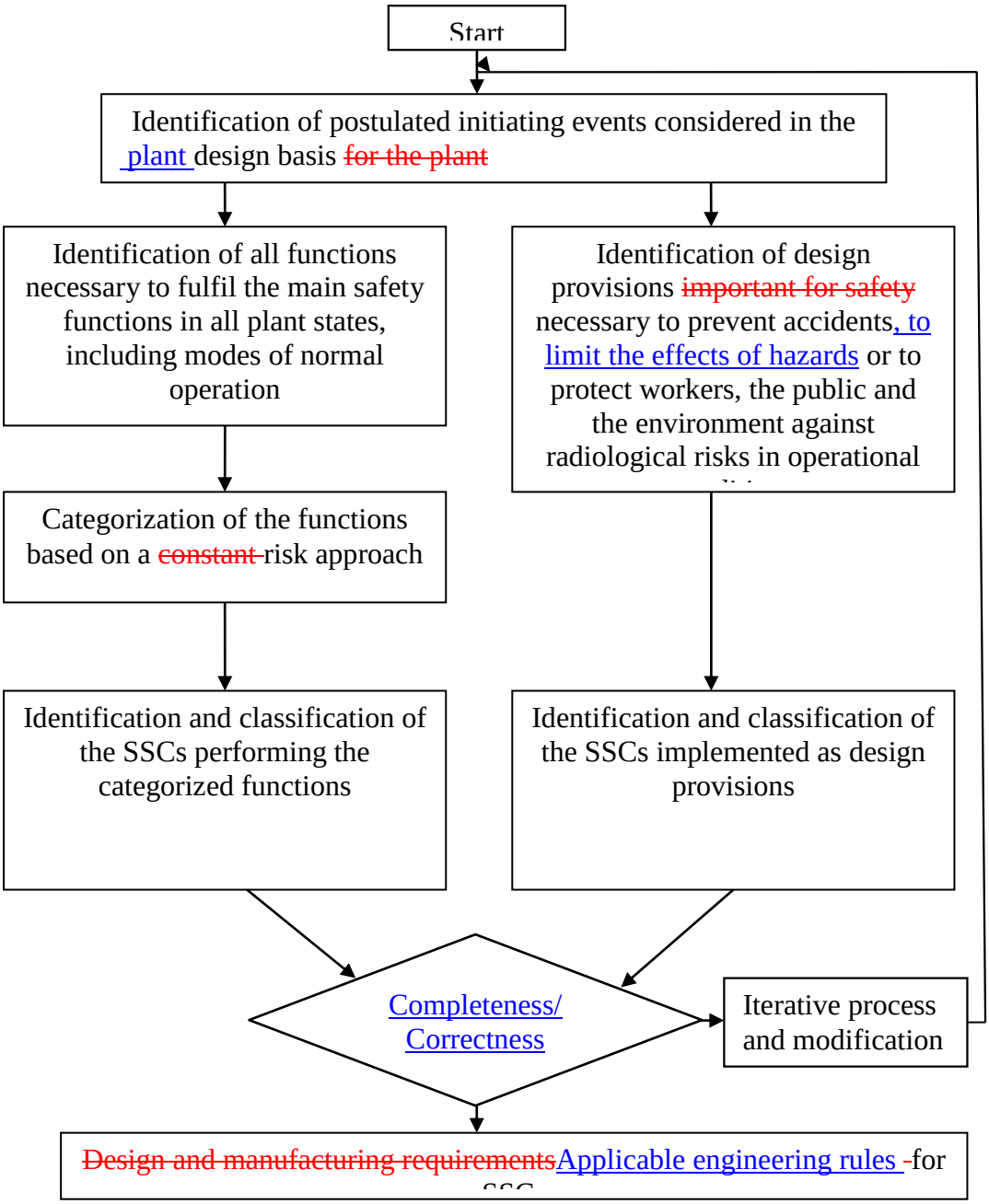

FIG. 1: Flowchart indicating the classification process

2.10. For a specific nuclear facilitypower plant, the following should be taken into account in classifying all SSCs according to their safety significance:

- The design basis of the plant and its inherent safety features;
- The list of all postulated initiating events[5], as required in Ref. [2], Requirement 16.

[5] 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."

- -The frequency of occurrence of the postulated initiating events, as considered in the design basis of the ~~facility~~nuclear power plant, should be taken into account.

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 a ~~constant~~ risk approach, with account taken of the three 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 time following a postulated initiating event at which, or the period of time during which, the function will be required to be performed.

A common basic principle commonly agreed in safety is that~~The constant risk approach is based on the principle that~~ the more likely the event, the lesser its consequences, as illustrated in Fig. 2.

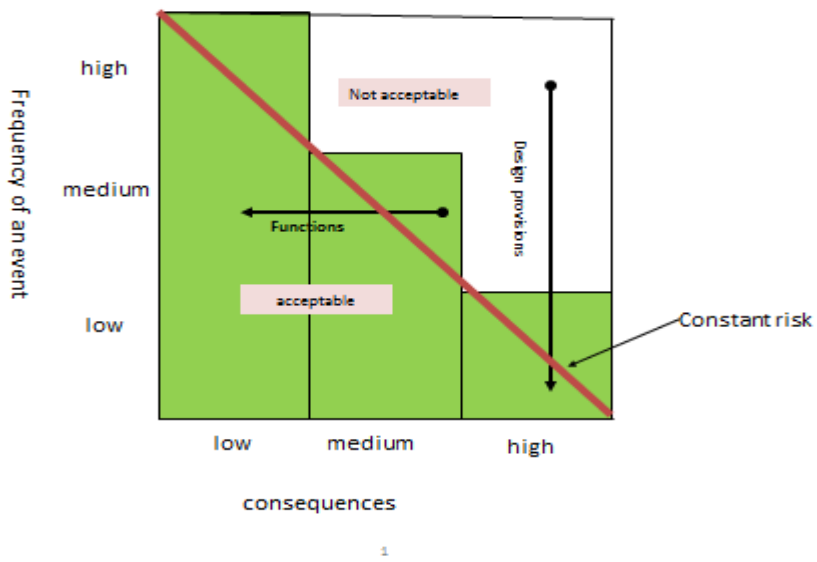

FIG. 2: Diagram indicating the ~~constant risk approach~~basic principle of frequency vs. consequences

2.13. Categorization of the design provisions is not necessary because their safety significance is directly linked to the consequences of their failure. Design provisions ~~are~~ can be directly assigned to a safety class.

2.14. The SSCs performing a function assigned in a safety category should be identified and classified. The SSCs should be primarily classified according to the category assigned to the function that they perform.

2.15. The SSCs implemented as, or designed with, design provisions should also be identified and classified.

2.16. In this Safety Guide three safety categories for functions and three safety classes for SSCs important to safety are recommended, based on the experience of the Member States. However, a larger or smaller number of categories and classes may be used if desired.

2.17. Safety classification is an iterative process that should be carried out throughout the design process. 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.

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' ~~designates~~ includes the primary function ~~or~~ and any supporting function that is 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.

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 in para. 3.4 may be supplemented by other functions such as those designed to reduce the actuation frequency of the reactor scram, and/or engineered safety features in the event of deviation 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 their importance to safety, monitoring for providing the plant staff and the off-site emergency response organization ~~operator~~ with a sufficient set of reliable ~~-~~information in the event of an accident ~~(a design basis accident or design extension condition)~~, 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 ~~multiple~~ additional independent failures from escalating to a severe accident, or to mitigate the consequences of a severe accident, are designated as functions associated with design extension conditions.

IDENTIFICATION OF DESIGN PROVISIONS

3.8. In addition to the functions identified, design provisions are implemented to ensure that the main safety functions are fulfilled under modes of normal operation. These should be

considered in the classification process to ensure that these SSCs, which are also of importance to safety, will be designed, manufactured, constructed, operated tested, inspected and maintained with sufficient quality to fulfil their intended role.

3.9. Design provisions are mainly implemented for the following reasons:

- To protect people (workers and the public) and the environment from harmful effects of radiation in operational conditions (direct radiation, airborne activity and releases of radioactive material);
- To prevent the failure of an SSC not considered in the ~~design basis for~~plant design basis ~~the plant~~ (e.g. rupture of the reactor pressure vessel for LWR);
- To reduce the frequency of failure of SSCs that may cause an accident (e.g. spent fuel pool);
- To limit the effects of hazards considered in the ~~design basis for the plant~~plant design basis[6] (e.g. civil structures of buildings important to safety);
- To prevent a postulated initiating event from developing into a more serious sequence without the occurrence of another independent failure (e.g. anti-whipping device, fixed points, etc.).

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:
    - Lead directly to a release of radioactive material that exceeds the limits for design basis accidents accepted by the regulatory body; or

[6] If the analysis of postulated initiating events performed according to national practice does not include hazards analysis.

- Cause the values of key physical parameters to ~~challenge or~~ exceed acceptance criteria for design basis accidents[7].

For levels of severity designated as 'medium' and 'low', the assessment of the consequences of failure of the function should be made assuming the correct response in due time of all other any independent functions~~that the functions belonging to the subsequent level of defence in depth respond as designed and in due time~~.

- The severity should be considered 'medium' if failure of the function could, at worst:
  - Lead to a release of radioactive material below the limits for design basis accidents accepted by the regulatory body but higher than those established for anticipated operational occurrences; or
  - Cause the values of key physical parameters to exceed the design limits for anticipated operational occurrences, but remain within the design limits specified for design basis accidents.
- The severity should be considered 'low' if failure of the function could, at worst:
  - Lead to an off-site release of radioactive material not exceeding the releases authorized for anticipated operational occurrences ~~normal plant operation~~, but could lead to doses to workers above the authorized limits, or
  - could result in the total loss of one of the three main safety functions.~~.~~

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. In this approach, the conditional probability that the function will be called upon in the sequence of the event may also be considered. However, it should be verified that the ~~probability~~ failure rate at the demand claimed for ~~failure of~~ the function will be achieved with application of the engineering design and manufacturing rules associated to the safety class finally selected.

3.13. With consideration of factors 1 and 2, this approach to classification is in line with the commonly agreed design principle that events with the most significant consequences have

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

the lowest ~~probability~~ frequency of occurrence. However, for the purposes of classification, the greatest importance should be given to maintain constant the risk resulting from the combination of likelihood and consequences (e.g. for functions dedicated to mitigation of the consequences of severe accidents, the engineering rules to be applied ~~are~~ may be less stringent than those applied for functions for mitigation of the consequences of design basis accidents, because the ~~probability~~ risk ~~of the severe accident~~ is lower). Figure 2 illustrates this approach.

3.14. Factor 3 (see para 2.12) reflects the time at which, or the period for which, a function will be required to be performed. The time factor should be considered in the various phases during the evolution of a postulated initiating event: some functions are required to be performed immediately after the accident to bring the reactor under control, while others are necessary for reaching and maintaining ~~a stable and durable~~for a long time a ~~-~~safe state. Where performance of a function may be delayed, provided evidence exists that there is sufficient time for this function to be established, ~~the proposed approach is~~it might be acceptable to ~~assign~~ allow ~~it to~~ a lower category than a function of equal importance that is required to be performed immediately. Generally, it is only acceptable to credit operator actions to establish a function after a sufficient time delay enabling detection of the postulated initiating event and diagnosis and completion of the actions by the operator.

3.15. The categorization recommended in this Safety Guide includes three safety categories supplemented by a non-safety-category.

Safety category 1

> Any automatic function required to be performed ~~immediately~~ to control or mitigate the consequences of 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 automatic function required to respond ~~immediately~~ to control an anticipated operational occurrence or design basis accident and whose failure, when challenged, would result in consequences of ‘medium’ severity; or
>
> Any delayed function (operator action) required to reach and maintain for a long time ~~a stable and durable~~ 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 delayed function required to reach and maintain ~~a stable and durable~~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 scram 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

Monitoring for providing the plant staff and off-site emergency services ~~operator~~ 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, unless already assigned to a higher category.

3.16. The categorization process is 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. Functions that have not been categorized in any of the safety categories are assigned as "non safety 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 of the failure of the function		
	High	Medium	Low
Immediate functions for the control of the consequences of anticipated operational occurrences	Safety category 1	Safety category 2	Safety category 3

Immediate functions for the control/ mitigation of consequences of design basis accidents (for bringing the plant to a controlled state)	Safety category 1	Safety category 2	Safety category 3
Functions for the control of design basis accidents after a controlled state is reached (for bringing the plant to a safe ~~shutdown~~ 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~~4~~)	*~~Usually not implemented, or~~ Nn~~n~~on-safety-category	*~~Usually not implemented, or~~ Nn~~n~~on-safety-category

*Such functions are generally not implemented

CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS

3.17. According to the methodology, once the categorization of functions is completed, the SSC should be assigned to a safety class.

3.18. The approach to safety classification recommended in this Safety Guide is based on three safety classes and one non safety-class.

3.19~~8~~. All SSCs required to perform a function categorized in any of the three safety categories should be identified.

~~3.19. The approach to safety classification recommended in this Safety Guide is based on three safety classes and one non safety-class one non safety class.~~

3.20. Initially, SSCs (including supporting SSCs) identified from the functions should be assigned to the safety class corresponding to the safety category of the function to which they belong. .

3.21. If an SSC contributes to the performance of several functions of different categories, it should be assigned to the class corresponding to the highest of these categories (i.e. the one requiring the most conservative engineering design rules).

3.22. The final safety class is established by means of the detailed classification. The initially assigned safety class (corresponding to the category of the function) of some individual SSCs may be modified, if justified by appropriate analysis, ~~(i.e.~~such as a detailed functional

analysis showing a low contribution of the component to the function, or by a probabilistic insight or engineering judgement~~)~~.

3.23. As explained in para. 2.9, the design provisions ~~are not categorized and the corresponding SSCs may~~can be directly classified according to the severity of consequences of their failure:

- Safety class 1

  Any SSC whose failure would directly lead, from normal operation, to an accident not considered as a design basis accident (design extension conditions or an accident not considered in the plant design basis).

- Safety class 2

  Any SSC whose failure, postulated from normal operation, would directly result in consequences of 'medium' severity, as defined in para. 3.11.

- Safety class 3

  Any SSC whose failure, postulated from normal operation, would directly result in consequences of 'low' severity, as defined in para. 3.11.

- Non Safety Class

  Any SSC necessary to perform a function assigned as non safety category and any SSC implemented as a design provision, not classified in any three safety classes.

3.24. Any SSC that ~~is independent of~~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.

3.25. 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 from a failure of the SSC in the lower safety class.

3.26. 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[8]. Consistency between these approaches will provide confidence that the safety classification is correct. Generally it is expected that probabilistic criteria for safety functions should match those derived deterministically.

If there are differences, further assessment should be performed and a final class should be assigned provided an appropriate justification.

[8] 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 STRUCTURES, SYSTEMS AND COMPONENTS

4.1. Once the safety class of SSCs is established, corresponding engineering design rules should be specified and applied, in accordance with the basic concept that the plant is to be designed such that the most frequent occurrences yield little or no adverse consequences to the public, such that the ~~improbable~~ extreme ~~situations~~events, having the potential for the greatest consequences to the public, have ~~a~~ the lowest probability of occurrence.

4.2. 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 function as required~~, with account taken of uncertainties~~;

b) 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.

~~c)~~ These abilities should take into account uncertainties.

4.3. A complete set of engineering design and manufacturing rules should be specified for safety classified SSCs. These engineering rules should ensure that the SSCs possess all the design features necessary to achieve the required levels of capability, dependability and robustness. These rules should take due account of regulatory requirements relevant to safety classified SSCs.

~~The regulatory body might establish additional requirements for SSCs that are safety classified.~~

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:

- Such design requirements applied at the system level can include e.g. single failure criteria, independence of redundancies, diversity, testability, etc.

- Such design requirements applied for individual ~~SSCs~~ structures and components can include e.g. environment and seismic qualification, manufacturing quality assurance procedures, etc.. They are typically expressed by specifying the code or standard that applies.

4.5. The licensee or applicant should provide and justify the correspondence between the safety class and the set of engineering design and manufacturing rules, including the codes or standard that applies.

4.6. Annex I provides an example of application of this guidance for systems for each of the different safety classes in the design of a PWR plant.

~~4.7. Annex II provides an example of the correspondence between the engineering requirements set out by ASME/RCC-M code and the safety class of a pressure retaining component given by the classification scheme provided in this Safety Guide. A similar correspondence should be established for other types of component (electrical, instrumentation and control, civil structures, handling devices, etc.). Where no code exists, the requirements to achieve the requested capability, dependability and robustness should be specified in the technical specifications of the component.~~

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).

~~[5] AMERICAN NATIONAL STANDARDS INSTITUTE, Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactors Plants, ANSI N18.2-1973, ANSI, Washington DC (1973).~~

ANNEX I

Example of a set of engineering rules for systems performing functions of different safety categories

Function	**Category of function**	**Safety class of system performing the function**	**Redundancy requirement**	**Independence of redundant trains**	**Physical separation of redundant trains**	**Periodic testing**	**Qualification to environmental conditions**	**Quality assurance**
Emergency core Cooling	**Cat. 1**	Class 1	Yes	Yes	Yes	Yes	Harsh or mild, depending on system location.	Nuclear grade
Long term residual heat removal (beyond the function of the emergency core cooling system)	**Cat. 2**	Class 2	Yes	Yes	Yes	Yes	Harsh or mild, depending on system location.	Nuclear grade or specific requirements
Containment depressurization after a severe accident	**Cat. 3**	Class 3	No (active means may be designed redundantly as required by probabilistic safety analysis)	No	No	Yes	Severe accident conditions	Specific requirements
Functions to warn personnel about the risk of radiation exposure beyond the acceptable limits	**Cat. 3**	Class 3	No	No	No	Yes	No	Commercial grade or specific requirements

ANNEX II

Example of a set of engineering rules for design and manufacturing of pressure retaining components of different safety classes

ASME/RCC-M level	Component
1	○ Restricted to any pressure retaining component in safety class 1 whose failure is not considered in the plant design basis and where consequences of its failure might prevent the reactor from being operated safely, or ○ If required by regulations (e.g. for RCPB)
2	○ Any pressure retaining component in safety class 1, unless ASME/RCC-M level 1 applies
3	○ Any pressure retaining component in safety class 2 ○ Any pressure retaining component not already classified in safety class 1 or 2, for which leakage or breakage could lead to doses to workers above authorized limits ○ Some component in safety class 1, if justified

Note 1: Restricting ASME/RCCM level 1 as above indicated and meeting ASME/RCC-M level 2 design and manufacturing requirements is consistent with the best practice in Member States. For both cases, the objective is to justify that thanks to the quality achieved by fulfilling the engineering rules, the probability of failure or of non-response when challenged is low enough to be consistent with the whole plant design objectives. Therefore:

- Where the probabilistic target depends only upon the dependability of the equipment itself, then the highest design and manufacturing criteria required by the code apply; but
- Less stringent design and manufacturing criteria may apply where the probabilistic target combines the probability of the initiating event with the probability of non-response of a system designed to respond.

Note 2: Any deviation to these general principles should be justified by the applicant.

CONTRIBUTORS TO DRAFTING AND REVIEW

Asfaw, K.	International Atomic Energy Agency
Barbaud, J.	Electricité de France, France
Barrett, A.	Nuclear Regulatory Commission, United States of America
Bassing, G.	FORATOM-ENISS Reactor Safety Group, Belgium
Bouscasse, M.	Institute for Radiation Protection and Nuclear Safety, France
Cabasse F.	Electricité de France, France
Coe, I.	AMEC, United Kingdom
Cook, B.	Westinghouse Electric Company, United States of America
Cook, S.	Canadian Nuclear Safety Commission, Canada
El-Shanawany, M.	International Atomic Energy Agency
Erasmus, L.	Pebble Bed Modular Reactor, South Africa
Fil, N.	OKB Gidropress, Russian Federation
Fischer, K.C.	TÜV Nord Systec GmbH & Co. KG, Germany
Froehmel, P.	E.ON Kernkraft GmbH, Germany
Hakata, T.	Nuclear Safety Commission, Japan
Head, J.	General Electric Hitachi
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
Jennings, R.	HSE- Office for Nuclear Regulations, United Kingdom
Jung, I.	Nuclear Regulatory Commission, United States of America
Kadambi, P.	American Nuclear Society Standards Board, United States of America
Klapp, U.	AREVA, Germany

Leong, J.	General Electric Hitachi
Linn, M.	Oak Ridge National Laboratory, United States of America
Miranda, S.	Nuclear Regulatory Commission, United States of America
Moreau, A.	Institute for Radioprotection and Nuclear Safety, France
Petzer, C.	Pebble Bed Modular Reactor, South Africa
Poulat, B.	International Atomic Energy Agency
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
Vayssier, G.	Nuclear Service Corporation, Netherlands
Waas, U.	AREVA, Germany
Wattelle, E.	Institute for Radioprotection and Nuclear Safety, France