DS367 Draft 5.1

Date: 04/11/2008

IAEA SAFETY STANDARDS

for protecting people and the environment

Status: for Member States comments

Reviewed in NS-SSCS

Please submit your comments by 20 March 2009

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

DRAFT SAFETY GUIDE

DS367

New Safety Guide

IAEA
International Atomic Energy Agency

FOREWORD

by Mohamed ElBaradei

Director General

The IAEA's Statute authorizes the Agency to establish safety standards to protect health and minimize danger to life and property — standards which the IAEA must use in its own operations, and which a State can apply to its nuclear and radiation related facilities and activities. A comprehensive body of safety standards under regular review, together with the IAEA's assistance in their application, has become a key element in a global safety regime.

In the mid-1990s, a major overhaul of the IAEA's safety standards programme was initiated, with a revised oversight committee structure and a systematic approach to updating the entire corpus of standards. The new standards that have resulted are of a high calibre and reflect best practices in Member States. With the assistance of the Commission on Safety Standards, the Agency is working to promote the global acceptance and use of its safety standards.

Safety standards are only effective, however, if they are properly applied in practice. The IAEA's safety services — which range in scope from engineering safety, operational safety, and radiation, transport and waste safety to regulatory matters and safety culture in organizations — assist Member States in applying the standards and appraise their effectiveness. These safety services enable valuable insights to be shared and I continue to urge all Member States to make use of them.

Regulating safety in nuclear and radiation related activities is a national responsibility, and many Member States have decided to adopt the IAEA's safety standards for use in their national regulations. For the Contracting Parties to the various international safety conventions, IAEA standards provide a consistent, reliable means of ensuring the effective fulfilment of obligations under the conventions. The standards are also used around the world by organizations that design, manufacture and apply nuclear and radiation related technologies in power generation, medicine, industry, agriculture, research and education.

The IAEA takes seriously the enduring challenge for operators and regulators everywhere — of ensuring a high level of safety in the use of nuclear and radioactive materials around the world. Their continuing utilization for the benefit of humankind must be managed in a safe manner, and the IAEA safety standards are designed to facilitate the achievement of that goal.

CONTENTS

1 INTRODUCTION

BACKGROUND

1.1 The need to classify equipment in a nuclear plant according to its importance to safety has been recognised since the early days of reactor design and operation. The existing safety classification methods for structures, systems and components (SSCs) have evolved taking into account the lessons learnt during tens of thousands of hours of, mainly light water reactor (LWR), operation. Although the concept of safety functions as being what should be accomplished for safety has been understood for many years and examples based on experience have been provided, the process by which these could be derived from the general safety objectives has not been described in earlier IAEA publications. The classification systems accordingly identified the SSCs, mainly from experience and analysis of specific designs, 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 this 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, NS-R-1 [1], published in 2000.

1.3 In developing this Safety Guide, a review of other relevant IAEA publications has been undertaken. This has included the IAEA Safety Requirements publication, Safety of Nuclear Power Plants: Design, NS-R-1 [1], the IAEA Safety Fundamentals, Fundamental Safety Principles, SF-1 [2], and current and ongoing revisions of Safety Guides and INSAG reports, including Safety Assessment and Verification for Nuclear Power Plants, NS-G-1.2 [3], and Defence in Depth in Nuclear Safety, INSAG-10 [4]. These publications have addressed the issues of safety functions and the safety classification of structures, systems and components (SSCs) for nuclear power plants. Information from a significant number of other international and national publications has been considered in developing this Safety Guide.

1.4 The purpose of the safety classification in a nuclear power plant is to identify and classify SSCs on the basis of their safety function and 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.

OBJECTIVE

1.5 The objective of this Safety Guide is to provide guidance on how to meet the requirements for identification of safety functions and classification of SSCs established in the Ref. [1] and to ensure appropriate quality and reliability of SSCs. This Safety Guide proposes a technology neutral approach and issues relating to particular types of reactor are discussed in general terms.

1.6 The recommendations on safety classification as presented in this Safety Guide are intended to be applicable to any plant type, irrespective of the amount of available operating experience. The approach to safety classification presented here is intended to be suitable both for new designs of nuclear power plant and during the periodic safety review of, or upgrades to, existing plants. It is intended to cover all aspects of a nuclear power plant, including the storage and handling of new and spent fuel at the site of the plant, that are included in the plant's safety analysis report. 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 review and assessment.

SCOPE

1.7 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. It has been assumed that all plants have a series of physical or other barriers for the retention of an inventory of radioactive material and that all must meet a set of requirements that govern the safe operation of the plant. Further, all plants are assumed to require 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 was written for nuclear power plants but could be extended to any type of nuclear facility, if the appropriate amendments are made.

STRUCTURE

1.8 Section 2 provides general recommendations on the approach to be adopted in meeting the IAEA requirements on safety classification, and the defence in depth (DiD)

concept for plant safety. Section 2 also introduces the concept of safety functional groups to perform safety functions to prevent and/or mitigate postulated initiating events (PIE). Section 3 describes the steps in the safety classification process. Section 4 provides recommendations on requirements for SSCs based on their safety classification. The tables and the appendices cover a number of issues including flow charts of the process and examples of design requirements. Annex I gives a list of safety functions for light water type reactors, and Annex II provides an example of the possible combination approach for deterministic safety analysis and probabilistic safety analysis results for assessment of adequacy of safety classification during system level design.

2 REQUIREMENTS AND GENERAL APPROACH FOR SAFETY CLASSIFICATION

REQUIREMENTS FOR A SAFETY CLASSIFICATION PROCESS

2.1 The requirements for a safety classification system are established in Ref. [1]. These are repeated in the following paragraphs.

2.2 Ref. [1] in paragraph 4.7 states "A systematic approach shall be followed to identify the structures, systems and components that are necessary to fulfil the safety functions at the various times following a PIE."

2.3 Ref. [1] in paragraph 5.1 states "All structures, systems and components, including software for instrumentation and control (I&C), that are items important to safety shall be first identified and then classified on the basis of their function and significance with regard to safety. They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification."

2.4 Ref. [1] in paragraph 5.2 states "The method for classifying the safety significance of a structure, system or component shall primarily be based on deterministic methods, complemented where appropriate, by probabilistic methods and engineering judgement, with account taken of factors such as:

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

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

(3) the probability that the item will be called upon to perform a safety function;

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

2.5 Ref. [1] in paragraph 5.3 states "Appropriately designed interfaces shall be provided between structures, systems and components of different classes to ensure that any failure in a system classified in a lower class will not propagate to a system classified in a higher class."

FUNDAMENTAL SAFETY FUNCTIONS

2.6 Fundamental safety functions are derived from the need to achieve the fundamental safety objective established in Ref. [2]: "to protect people and the environment from harmful effects of ionizing radiation."

2.7 Ref. [1] in paragraph 4.6 states “To ensure safety, the following fundamental safety functions shall be performed in operational states, in and following a design basis accident and, to the extent practicable, on the occurrence of those selected accident conditions that are beyond the design basis accidents:

(1) control of reactivity;
(2) removal of heat from the core; and
(3) confinement of radioactive material and control of operational discharges, as well as limitation of accidental releases.”

[The intent on the core in (2) is for fuel in the core and spent fuel in the storage.]

PLANT SPECIFIC SAFETY FUNCTIONS

2.8 For each type of nuclear power plant, based on the fundamental safety functions, the plant specific safety functions should be defined to prevent or mitigate postulated initiating events. Plant specific safety functions should be defined at an adequate level of detail that will allow the identification of SSCs that are required for performing these safety functions. In line with Refs. [2] and [4], preventive safety functions prevent abnormal operation or system failures. Mitigatory safety functions control the consequences of abnormal operation or failures that have occurred. A practical example is shown in Annex I.

DEFENCE IN DEPTH AND BARRIERS

2.9 Ref. [1] in paragraph 4.5 states “The objective of the safety approach shall be: to provide adequate means to maintain the plant in a normal operational state; to ensure the proper short term response immediately following a postulated initiating event; and to facilitate the management of the plant in and following any design basis accident, and in those selected accident conditions beyond the design basis accidents.”

2.10 The concept of successive barriers to release of radioactivity is part of the defence in depth strategy. Furthermore, according to paragraph 2.10 of Ref. [1], “Application of the concept of defence in depth in the design of a plant provides a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.”

2.11 The use of the defence in depth concept is required in the design process and it should be applied in the safety classification process. The preventive plant specific safety functions should be allocated to the defence in depth level 1 and the mitigatory plant specific

safety functions to the defence in depth levels 2 – 5 described in Table 1 of Ref. [4] and shown in Appendix I.

SAFETY FUNCTIONAL GROUPS

2.12 Safety functional groups, defined as all the SSCs, including supporting items that work together to perform a plant specific safety function, derived from fundamental safety functions, to prevent or mitigate a postulated initiating event and allocated to one defence in depth level, should be identified.

2.13 The safety functional groups should be categorized according to their safety significance. Safety categorization should be based on the consequences of the failure of the SSCs to perform their assigned safety functions.

2.14 Safety classes of the SSCs should be derived from the relevant safety categories as described by Fig. 1 in Section 3.

2.15 Because not all SSCs within a safety functional group may have an equal contribution towards achieving the desired safety function, appropriate safety classes for the SSCs, which belong to that safety functional group should be derived.

2.16 The safety classification process should ultimately assign design requirements for all SSCs that will achieve the appropriate performance of each safety functional group.

APPLICATION OF THE SAFETY CLASSIFICATION PROCESS

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

2.18 The safety classification process should take the following steps:

(1) identification of plant specific safety functions to prevent or mitigate postulated initiating events based on the three fundamental safety functions;

(2) allocation of the plant specific safety functions to defence in depth levels;

(3) identification of the safety functional groups to perform plant specific safety functions at different defence in depth levels and allocation of SSCs to perform the required functions within these safety functional groups;

(4) assignment of safety functional groups to safety categories based on the consequence of the groups' failure;

(5) assignment of the individual SSCs within safety functional groups to safety classes based on their importance in achieving the plant specific safety functions;

(6) assignment of design requirements to the SSCs based upon their classification.

VERIFICATION AND REVISION OF SAFETY CLASSES

2.19 Safety classification may be an iterative process during the design process. Any preliminary safety class assignments should be finalized using deterministic safety analysis and, where available, probabilistic safety analysis.

2.20 During the plant periodic safety reviews and before modifications, this safety classification method should be applied to determine if there are any changes to the safety functions to be performed.

3 SAFETY CLASSIFICATION PROCESS

3.1 The safety classification process described within this section highlights the significant linkage that exists between safety design, functional analysis and classification. Although the precise nature of the steps taken at each stage could vary according to the regulatory requirements and the plant design, the safety classification process should include the steps outlined in the sub-sections below. The safety classification process should ultimately establish design requirements for all SSCs to achieve appropriate performance of safety functional groups.

SAFETY FUNCTIONS TO PREVENT OR MITIGATE POSTULATED INITIATING EVENTS

3.2 A complete set of plant specific safety functions based on the fundamental safety functions should also be defined during the initial design phase for a new nuclear power plant. For a specific nuclear power plant, a list of plant specific safety functions may already exist. If such a list does not exist, the fundamental safety functions should be broken down into plant specific safety functions and associated supporting functions for each defence in depth level.

3.3 The plant specific safety functions applied to safety functional groups will prevent or mitigate the postulated initiating events that have been identified and should be broken down as required into SSC level safety functions associated with each defence in depth level. For each defence in depth level, the fundamental safety functions should be broken down into a consistent group of plant specific safety functions (e.g. reactivity control may be broken down into a) preventing unacceptable reactivity transients, as defence in depth level 1 function and b) shutting down the reactor, c) maintaining the reactor in safe shutdown condition, both as defence in depth levels 2 and 3 functions). Acceptance criteria for the performance of plant level safety functions should be defined at each defence in depth level. These are refined during the design process to establish a complete set of safety functions.

3.4 For an existing plant the design should be reviewed periodically to ensure that the postulated initiating events and a sufficient list of plant specific safety functions to deal with them are appropriately defined.

3.5 For plant modifications, the sub-set of newly identified or modified plant specific safety functions should be assessed, taking into consideration the affected interfaces with existing safety functional groups.

ALLOCATION OF PLANT SPECIFIC SAFETY FUNCTIONS TO DEFENCE IN DEPTH LEVELS

3.6 Plant specific safety functions to prevent deviation from normal operation as well as to mitigate the consequences of anticipated operational occurrences (AOO) and accidents should be allocated to each of the five defence in depth levels, if appropriate, so that the relevant success criteria can be achieved (see Appendix 1).

3.7 Defence in depth level 1 safety functions should be provided to keep the plant within the normal operational envelope, by preventing failures.

3.8 Defence in depth level 2 safety functions are mitigatory safety functions and should detect, control and recover from failures that occur during anticipated operational occurrences. The assignment of these defence in depth level 2 safety functions should be to return the plant to normal operational conditions as promptly as possible, following an anticipated operational occurrence, before the occurrence can progress to a design basis accident (DBA) or a beyond design basis accident (BDBA).

3.9 Defence in depth level 3 safety functions are mitigatory safety functions and should control accidents within the design basis. Defence in depth level 3 safety functions could be subdivided into defence in depth level 3A and 3B safety functions, as described below.

3.10 Defence in depth level 3A safety functions should establish a controlled state following a design basis accident. A controlled state should be reached as soon as possible, preferably using automatic means, and is reached once the fundamental safety functions are restored.

3.11 Defence in depth level 3B safety functions should:

a) after a controlled state is reached, achieve a safe shutdown state and maintain it as long as necessary following a design basis accident, or

b) minimize the consequences on the remaining barriers from the occurrence of the design basis accident.

In a safe shutdown state, the reactor should remain sub-critical, decay heat should be removed indefinitely and all remaining barriers should remain intact.

3.12 Defence in depth level 4 safety functions are mitigatory safety functions and should control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents. Defence in depth level 4 safety functions could be subdivided into defence in depth level 4A and 4B safety functions, as described below.

3.13 Defence in depth level 4A safety functions should be those mitigatory safety functions required to arrest the progress of beyond design basis accidents, such as in-vessel mitigation before significant core degradation occurs.

3.14 Defence in depth level 4A safety functions should also be used to ensure that fundamental safety functions are maintained as far as possible and should include monitoring of the state of the plant and radiation levels.

3.15 Defence in depth level 4B safety functions should be those mitigatory safety functions required to control the remains of a significantly degraded core, such as ex-vessel mitigation, limiting radiological consequences, controlling further reactivity excursion, removing decay heat as long as required and confining radioactive material.

3.16 Defence in depth level 5 safety functions should include radiation monitoring and meteorological measurements for plume concentration prediction, emergency planning, and mitigation of releases following failures of the confinement safety function. The safety classification of equipment for any recovery or clean-up measures needed should be defined on a case-by-case basis and requirements identified.

3.17 Functions not included within the defence in depth levels described above, should be classified as non-safety.

IDENTIFICATION AND CATEGORIZATION OF SAFETY FUNCTIONAL GROUPS

3.18 Safety functional groups should be categorized primarily according to their safety significance based on the consequences of their failure. The relation of the safety function to defence in depth level reflects the likelihood of the safety functional group being called upon to operate. This should result in “highest” categorization on the safety functional groups where there are potentially the most severe consequences if they fail and which are most likely to be called upon to operate.

3.19 Each plant specific safety function allocated to a defence in depth level, whether preventive or mitigatory should be achieved by a single safety functional group. However, one safety functional group may perform more than one plant specific safety function, depending on the design.

3.20 Each safety functional group should contain all the necessary design features to achieve the desired capability, dependability and robustness.

3.21 The objective of preventive plant specific safety functions is to decrease the probability of failures to where the radiological consequences associated with this failure provide an acceptable risk. Safety functional groups that only prevent the occurrence of an abnormal event should be assigned to defence in depth level 1.

3.22 Where a postulated initiating event occurs which could cause unacceptable consequences, mitigatory actions should be included to decrease the consequences of this event to remain within an acceptable consequence range. Safety functional groups which perform at least one plant specific safety function to mitigate the consequence of a postulated initiating event should be assigned to defence in depth levels 2 to 4. The safety requirements related to each level of defence in depth should be defined. An enveloping safety functional group can be defined to cover several levels of defence in depth, if appropriate.

3.23 The severity level of consequence of failure of the safety functional group to perform its plant specific safety functions should be divided into consequence levels such as the high, medium and low.

3.24 The level of consequence should be considered “high” if the potential consequences of failure to maintain the safety function of either a preventive or mitigatory safety functional groups are radiological releases that challenge or exceed the applicable operational limits or safety acceptance criteria which have to be consistent with regulatory limits established for design basis accidents or similar events.

3.25 The level of consequence should be considered “medium” if the potential consequences are radiological releases in excess of normal operational limits, but certainly less than the design basis accident design limits or related safety acceptance criteria.

3.26 The level of consequence should be considered “low” if the consequences are radiological releases close to but below the normal operational limits. This reflects the uncertainty that may exist in the safety analysis or other parameters associated with plant operation.

3.27 Safety functional groups should be categorized according to Table 1. Safety category 1 is defined to be the most stringent severity level of consequence of failure of the safety functional group to perform its plant specific safety functions.

3.28 The limiting values that are assigned to each of the levels of radiological release will depend on the applicable operational limits or safety acceptance criteria which have to be consistent with regulatory limits for the plant.

Table 1 Relationship between Safety Function Type and Safety Categories of Safety Functional Groups

Safety Function Type	**Safety Functional Group defence in depth DiD Level**	**Severity level of consequence of failure of the safety functional group to perform its plant specific safety functions**		
		High	**Medium**	**Low**
Preventive	**DiD level 1**	Safety Category 1	Safety Category 2	Safety Category 3
AOO Mitigation	**DiD level 2**	Safety Category 1	Safety Category 2	Safety Category 3
Accident Mitigation	**DiD level 3A**	Safety Category 1	Safety Category 2	Safety Category 3
	DiD level 3B	Safety Category 2	Safety Category 3	Safety Category 3
	DiD level 4A	Safety Category 4[1,2]	Safety Category 4	Safety Category 4
	DiD level 4B	Safety Category 4	Safety Category 4	Safety Category 4
Radiological Release Mitigation	**DiD level 5**	Not safety categorized		
Functions not included above		Not safety categorized		

3.29 By assigning safety categories to safety functional groups, a set of common design requirements can be identified that will ensure that the appropriate quality and reliability is achieved. Design measures should be applied consistently within a safety category or using a graded approach for the different safety categories or safety classes. This is considered further in Section 4.

3.30 A deterministic safety analysis should be performed that will cover all postulated initiating events defined during the plant level and system level design. This analysis should

[1] SSCs in safety functional groups assigned to safety category 4 could have a safety class non nuclear-safety or specific requirements.

[2] If sufficient analysis and understanding exists regarding an event phenomena and consequences, the safety category 3 can be assigned.

confirm that the safety functional groups have the appropriate design requirements, are assigned to the appropriate defence in depth level and that the acceptance criteria for each postulated initiating event are met. This analysis should also provide a preliminary estimation of the plant behaviour and of the required systems performances.

3.31 When appropriate design information and performance and reliability data for generic equipment is available, an initial probabilistic safety assessment (PSA) should be performed, as appropriate, at this stage of the design. The purpose of this preliminary PSA is to identify potential additional initiating events (multiple failures, losses of support functions, etc.) and the required safety functions.

ASSIGN STRUCTURES, SYSTEMS AND COMPONENTS TO SAFETY CLASSES

3.32 As indicated in paragraph 3.27, this guide recommends that Safety Class 1 should be assigned to the SSCs which have the most severe consequences if they fail. This is the "highest" safety class for a safety classification scheme with four safety classes (1 - 4), as shown below in Fig. 1.

3.33 SSCs should initially be assigned to the safety class corresponding to the safety category of the safety functional group they belong to; however, some SSCs in a safety functional group may change class.

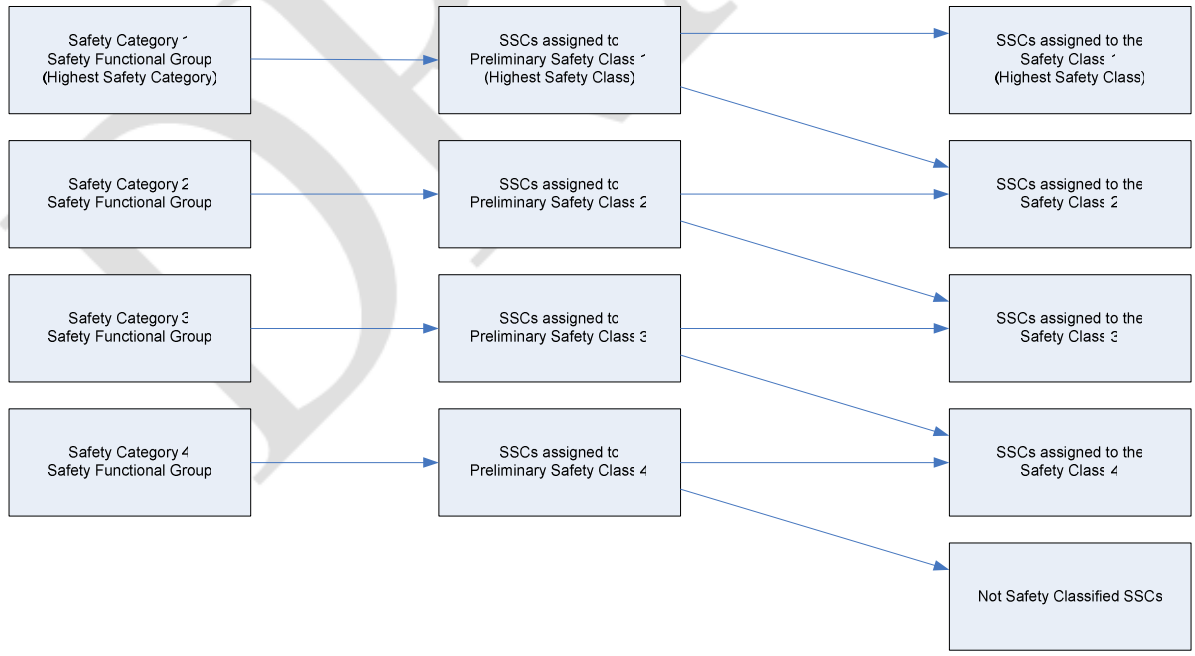

Fig. 1. Assignment of SSCs to Safety Classes

3.34 The safety class may be downgraded if justified by an appropriate safety analysis (See Figure II-1 in Annex II). A downgrade, generally of one level, is possible in the following cases:

(1) SSCs the failure of which would not affect the capability of the safety functional group to perform its plant specific safety function. This may be, for example, a small instrumentation line or sensors monitoring the operation or the status of SSCs performing the safety function but not involved in its control.

(2) SSCs performing auxiliary functions, already in operation at the moment of the postulated initiating event, and not affected by it.

(3) Plant specific safety function performed by more than one diverse SSC, provided the SSC is less likely to be used, it is possible to deploy it and there is sufficient time for it to be deployed.

3.35 If there are SSCs within certain safety functional groups that cannot be accepted to fail (e.g. reactor pressure vessel for pressurized light water reactors), then these SSCs should be allocated to the highest safety class (Class 1), and additional requirements specified on a case by case basis.

3.36 An SSC may be allocated to more than one safety functional group. However, an SSC should be allocated to only one safety class which should be the higher one with more conservative requirements for the SSCs that have been identified.

3.37 No account should be taken of whether a safety functional group contains active or passive SSCs, or a mixture of them, as this has neither effect on the safety category of the group nor on the safety class of the SSCs.

3.38 Any SSC or a part of that SSC whose failure could adversely affect a safety functional group in accomplishing its plant specific safety function, even though it is not part of it, should be classified in accordance with the safety category of that safety functional group. No lowering of classification should occur in this case.

3.39 Where the safety class of connecting or interacting SSCs is not the same (including safety classes to non safety SSCs), the SSCs should be isolated by a safety classified device of the higher classification (e.g., optical isolators or automatic valves) from the effects of failures in the lower safety classification SSC. An exception is where the failure of the SSC

with the lower safety class (including a potential common-cause failure of identical or redundant items) cannot prevent accomplishment of the safety functions of the SSC with the higher safety class.

3.40 The safety classification process, which follows the steps listed in paragraph 2.18, is presented in flowchart form in Appendix II.

VERIFICATION OF THE SAFETY CLASSIFICATION USING DETERMINISTIC AND PROBABILISTIC SAFETY ANALYSIS

3.41 The adequacy of the safety classification should be verified using deterministic safety analysis complemented, as appropriate, by insights from the PSA and supported by engineering judgement. The particular methods involved should depend on the design information available and regulations from the Member State.

3.42 Probabilistic methods should only be used when the PSA has a level of detail adequate to support the classification process.

3.43 The process should confirm that a complete set of postulated initiating events has been defined for the plant and a sufficient set of preventive plant specific safety functions has been provided to prevent the postulated initiating events from happening and, if they do occur, adequate mitigatory plant specific safety functions are available to maintain the fundamental safety functions as far as possible and keep any consequences below acceptable limits. It should, in addition, establish that the requirements for the safety functional groups are properly defined and that the SSCs that comprise them have adequate performance to provide the plant specific safety functions.

3.44 If there are deviations between the PSA results and the deterministic based safety classification of an item then the most conservative safety classification (higher safety class) should be used.

3.45 Safety analysis should confirm, using appropriately conservative assumptions regarding SSC performance characteristics, that the safety functional groups performing all the plant specific safety functions and the SSCs allocated to the group have the adequate design requirements and are assigned to the correct safety category/class and that the operational limits or other safety acceptance criteria which have to be consistent with regulatory limits for each postulated initiating event have been met.

3.46 If the analysis shows that the operational limits and safety acceptance criteria which have to be consistent with regulatory limits are not exceeded and that the reliability targets are met for all the postulated initiating events, the design is acceptable and the set of defined safety functions is complete.

3.47 Ideally, the final goal should be to obtain balance between deterministic and probabilistic based safety classification as this will provide confidence that the classification is correct. In Annex II Fig. II-1 depicts how a balance between deterministic and probabilistic methods could be obtained.

4 SELECTION OF APPLICABLE REQUIREMENTS FOR STRUCTURES, SYSTEMS AND COMPONENTS

4.1 Selection of applicable design requirements is intended to reflect the required quality commensurate with safety function of the SSC. Nationally adopted codes and standards should be applied for design requirements.

4.2 Once SSCs are assigned to Safety Classes, design requirements can be assigned to them placing the "highest" safety class and the most stringent requirements on SSCs where their failure causes the most severe consequences with the greatest likelihood of being called upon to operate.

4.3 The requirements for individual SSCs may be consistent with the entire safety functional group(s) to which it belongs.

4.4 These requirements are related to the three characteristics of capability, dependability and robustness. SSCs should be designed, constructed, qualified, operated, tested and maintained to:

(1) Perform its designated safety function as required, taking uncertainties into account (capability),

(2) Ensure that failures within the safety functional group cannot degrade the ability of the group to perform its designated safety function (dependability), and

(3) Ensure that no operational loads or loads caused by any associated postulated initiating events should be able to adversely affect the ability of the safety functional group to perform its designated safety function (robustness).

4.5 The dependability and robustness of an SSC should be achieved within an acceptable range of probability of failure and its related consequences.

4.6 In Appendix III, Tables 2 and 3 provide examples of design requirements in terms of capability, dependability and robustness.

4.7 When defining the design requirements (e.g. redundancy, diversity, etc.) for safety functional groups, including interactions between information technology, instrumentation & control and other types of system, requirements from the appropriate codes and standards should be included.

4.8 In Appendix III, Table 4 provides examples of design requirements for SSCs of different safety classes, depending on their preventive or mitigatory safety functions.

4.9 The appropriate codes and standards should be used for defining design requirements for all types of SSCs.

4.10 Fire protection and fire suppression requirements should be applied as outlined in Ref. [8] for the design of SSCs and as appropriate, for the maintenance of safety functions.

4.11 The requirements for instrumentation & control and information technology equipment and software should be applied in accordance with the recommendations provided in Refs. [9] and [10].

4.12 Quality assurance or management requirements for procurement, construction, inspection, installation, testing, surveillance, and modification of SSCs should be assigned based on their safety class as outlined in Refs. [11].

4.13 The seismic classification of safety and non-safety class SSCs should be in accordance with the recommendations provided in Ref.[7] .

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

APPENDIX I: ALLOCATION OF SAFETY FUNCTIONS TOLEVELS OF DEFENCE IN DEPTH

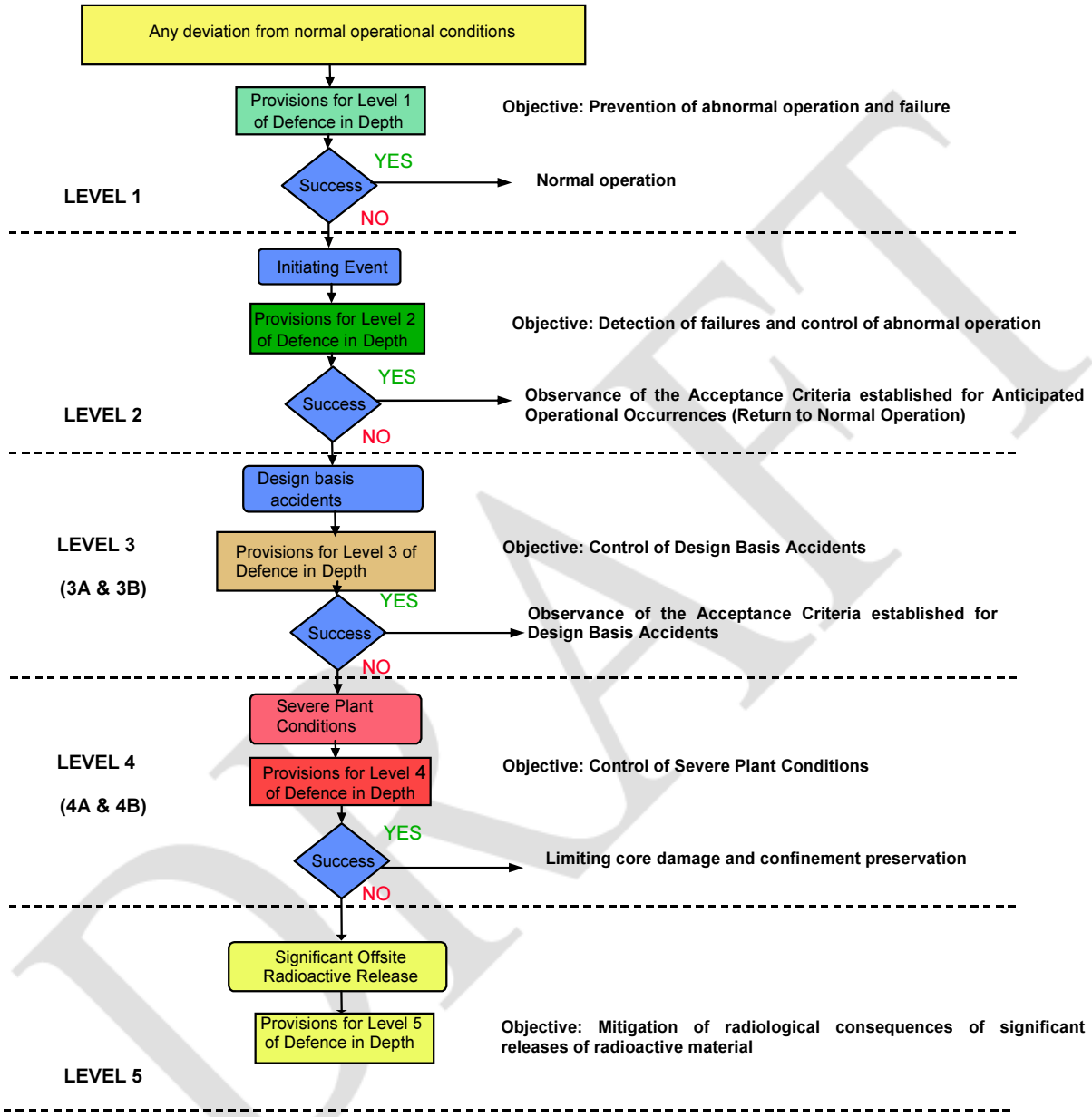

Fig. 2 Logic flow diagram for the allocation of safety functions to levels of defence in depth, showing safety functions and success criteria

APPENDIX II: SAFETY CLASSIFICATION PROCESS

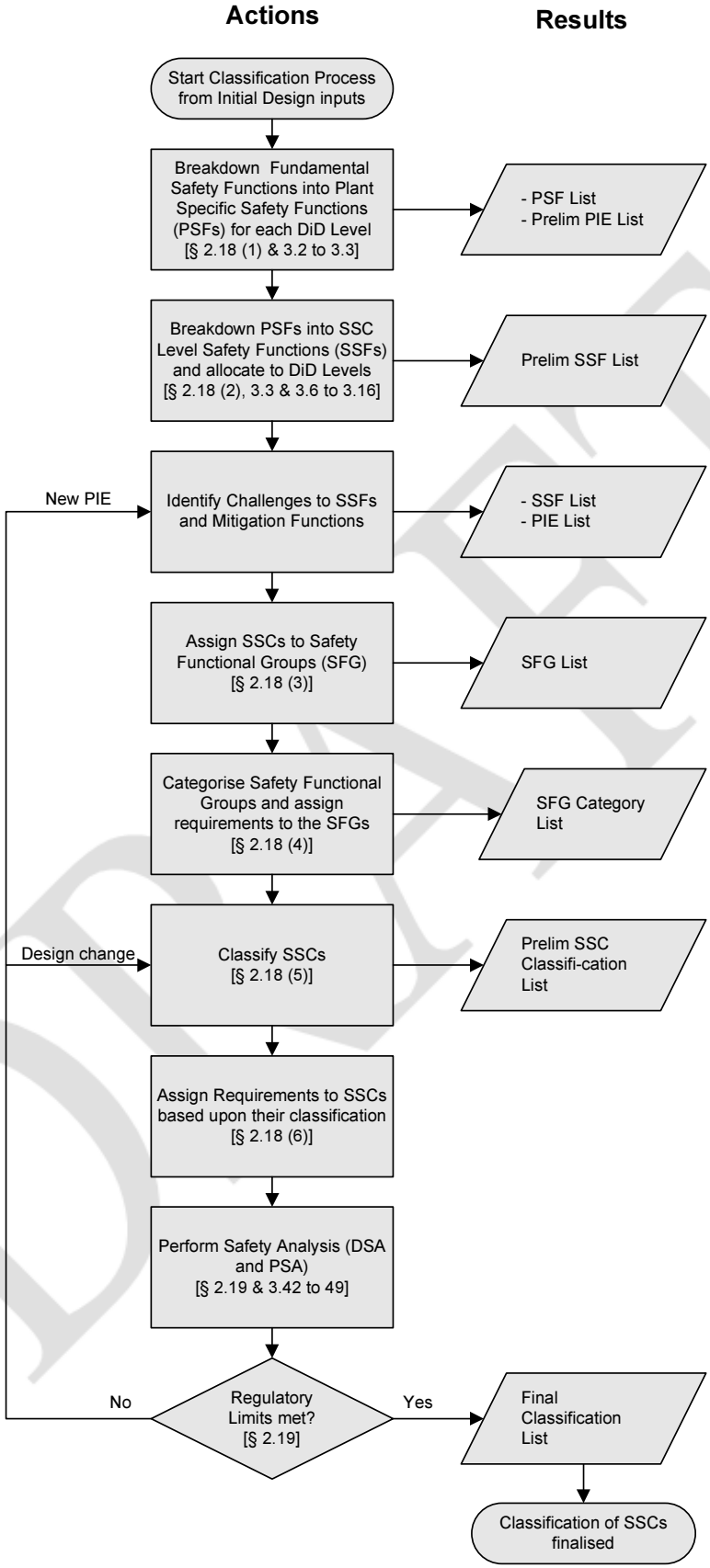

Fig. 3 Detailed flowchart of the safety classification process

APPENDIX III: EXAMPLES OF DESIGN REQUIREMENTS

TABLE 2 EXAMPLE OF REQUIREMENTS FOR SAFETY CATEGORIES

SAFETY **CATEGORY**		**CAPABILITY**	**DEPENDABILITY**	**ROBUSTNESS**
Safety Category-1	Preventive (DiD 1)	Prevent deviation from DBA regulatory limits	Achieve regulatory requirements for DBA	Survive normal operation, AOO, and DBA conditions
	Mitigatory (DiD 2, 3A)	Achieve AOO and DBA regulatory limits as appropriate	Achieve regulatory requirements for AOO and DBA[3] as required	Survive conditions due to normal operation and PIEs to be mitigated
Safety Category-2	Preventive (DiD 1)	Prevent deviation from normal operation regulatory limits.	Achieve regulatory requirements for AOO	Survive normal operation, and AOO conditions
	Mitigatory (DiD 2, 3A, 3B)	Achieve AOO and DBA limits as appropriate	Achieve regulatory requirements for AOO and DBA[1] as required	Survive conditions due to normal operation and PIEs to be mitigated
Safety Category-3	Preventive (DiD 1)	Prevent deviation from normal operating limits	Achieve requirements for normal operation	Survive normal operation conditions
	Mitigatory (DiD 2, 3A, 3B)	Achieve AOO and DBA limits as appropriate	Achieve regulatory requirements for normal operation, AOO, and DBA[1] as required	Survive conditions due to normal operation and PIEs to be mitigated
Safety Category-4	Mitigatory (DiD 4)	Achieve requirements for BDBA and Severe Accidents	Achieve appropriate regulatory requirements	Survive conditions due to normal operation and PIEs to be mitigated

[3] Regulatory requirements may be deterministically developed or probabilistically developed, such as mitigation system dependability target set by National regulatory cut-off probability for a specific event category divided by that specific initiating event probability.

TABLE 3 EXAMPLES OF SSC DESIGN REQUIREMENTS

	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
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 • Independence • Maintainability • Testability

TABLE 4 EXAMPLE OF REQUIREMENTS FOR SSCS BASED ON SAFETY CLASSES

	Preventive Safety Functions (Defence in depth Level 1)				**Mitigatory Safety Functions (Defence in Depth Levels 2 to 4)**			
Requirement	**Safety Class-1**	**Safety Class-2**	**Safety Class-3**	**Safety Class-4**	**Safety Class-1**	**Safety Class-2**	**Safety Class-3**	**Safety Class-4**
Quality Assurance	Nuclear Grade	Nuclear Grade	Commercial Grade or Specific Requirements	Commercial Grade or Specific Requirements	Nuclear Grade	Nuclear Grade	Commercial Grade or Specific Requirements	Commercial Grade or Specific Requirements
Environmental qualification	Harsh or Mild: SSC to be Qualified for all normal operation states and PIEs, depending on location	Harsh or Mild: SSC to be qualified for All normal operation states	Harsh or Mild: SSC to be qualified for All normal operation states	Specific Requirements	Harsh or Mild: SSC to be Qualified for all normal operation states and applicable PIEs	Harsh or Mild: SSC to be Qualified for all normal operation states and applicable PIEs	Harsh or Mild: SSC to be qualified for All normal operation states	Specific SSC to be qualified for All normal operation states and applicable PIEs
Pressure Retaining Components (example codes)[4]	High Pressure: C1 Low Pressure: C2	High Pressure: C2 Low Pressure: C3	High Pressure: C3 Low Pressure: C4	C4	High Pressure: C2 Low Pressure: C3	C3	C4	C4
Electrical (IEEE)	1E	1E	Non 1E	Non 1E	1E	1E	Non 1E	Non 1E
I&C (IEC 61226 Category)[5]	B or C	B or C	B or C	C	A	B	C	C
Seismic	Seismic Category 1	Seismic Category 1	Specific Requirements	Specific Requirements	Seismic Category 1	Seismic Category 1	Specific Requirements	Specific Requirements
Civil Structures (External Events)	Class 1	Class 1	Class 1	Specific Requirements	Class 1	Class 1	Class 1	Commercial

[4] C1 : quality level 1 : for example level 1 of ASME III or RCC-M (Reactor pressure boundary) ; C2 : quality level 2 : for example level 2 of ASME III or RCC-M, (Emergency Core Cooling System…) ; C3 : quality level 3 : for example level 3 of ASME III or RCC-M (Component Cooling Water System, Essential Service Water System …); C4 is a quality class concerning non nuclear grade pressure retaining components with special requirements (for example seismic design, quality requirements…): those components can be designed with whatever pressure retaining component design code taking into the special requirements (fire system…).

[5] Category A denotes the functions that play a principle role in the achievement or maintenance of NPP safety to prevent DBA from leading to unacceptable consequences. Category B denoted functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, especially the functions required to operate after the controlled state has been achieved, to prevent DBAs from leading to unacceptable consequences, or mitigate the consequences of a DBA. Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[2] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, Fundamental Safety Principles, Safety Fundamentals No. SF-1, Vienna (2006).

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

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

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

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

[8] 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).

[9] 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).

[10] 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).

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

ANNEX I: FUNDAMENTAL SAFETY FUNCTIONS FOR LIGHT WATER REACTORS

TABLE II-1[6] EXAMPLE OF FUNDAMENTAL SAFETY FUNCTIONS FOR BOILING WATER REACTORS AND PRESSURIZED WATER REACTORS DERIVED FROM FUNDAMENTAL SAFETY FUNCTIONS[7]

Safety Function	Defence in depth level of Safety Function						
	1	2	3A	3B	4A	4B	5
(1) to prevent unacceptable reactivity transients;	FSF1						
(2) to maintain the reactor in a safe shutdown condition after all shutdown actions;	FSF1	FSF1	FSF1	FSF1			
(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;		FSF1	FSF1	FSF1			
(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;			FSF2	FSF2			
(5) to maintain sufficient reactor coolant inventory for core cooling in and after all postulated initiating events considered in the design basis;		FSF2	FSF2	FSF2			
(6) to remove heat from the core after a failure of the reactor coolant pressure boundary in order to limit fuel damage;			FSF2	FSF2	FSF2		
(7) to remove residual heat in appropriate operational states and accident conditions with the reactor coolant pressure boundary intact;	FSF2	FSF2	FSF2	FSF2			

[6] This list of safety functions is taken from Annex of NS-R-1 [1] .

[7] The fundamental safety functions are FSF1) control of reactivity, FSF2 cooling of the fuel, FSF3confinement of radioactivity

Safety Function	Defence in depth level of Safety Function						
	1	2	3A	3B	4A	4B	5
(8) to transfer heat from other safety systems to the ultimate heat sink;		FSF2	FSF2	FSF2			
(9) to ensure necessary services (such as electrical, pneumatic, hydraulic power supplies, lubrication) as a support function for a safety system;	FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3			
(10) to maintain acceptable integrity of the cladding of the fuel in the reactor core;	FSF3	FSF3	FSF3	FSF3			
(11) to maintain the integrity of the reactor coolant pressure boundary;	FSF2 FSF3	FSF2 FSF3					
(12) to limit the release of radioactive material from the reactor containment in accident conditions and conditions following an accident;			FSF3	FSF3	FSF3	FSF3	
(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;			FSF3	FSF3	FSF3	FSF3	FSF3
(14) to limit the discharge or release of radioactive waste and airborne radioactive material to below prescribed limits in all operational states;	FSF3	FSF3					
(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;		FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	
(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;	FSF3	FSF3					
(17) to remove decay heat from irradiated fuel stored outside the reactor coolant system, but within the site;	FSF2	FSF2					

Safety Function	Defence in depth level of Safety Function						
	1	2	3A	3B	4A	4B	5
(18) to maintain sufficient subcriticality of fuel stored outside the reactor coolant system but within the site;	FSF1	FSF1					
(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.	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3	FSF1 FSF2 FSF3

ANNEX II COMBINATION APPROACH FOR DETERMINISTIC SAFETY ANALYSIS AND PROBABILISTIC SAFETY ANALYSIS RESULTS

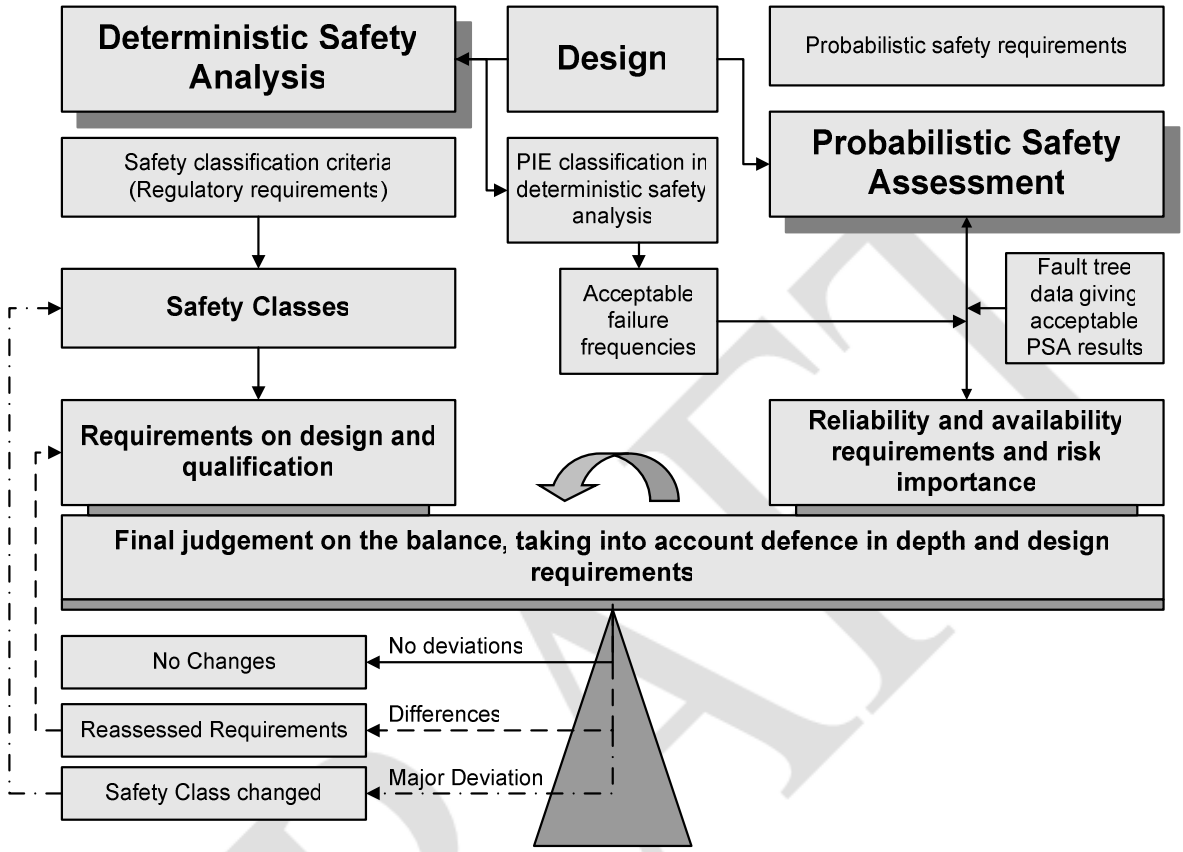

Fig. II-1 Possible approach to combine the results of deterministic safety analysis and PSA for assessment of the adequacy of safety classification during design at the system level

CONTRIBUTORS TO DRAFTING AND REVIEW

BOUSCASSE, M.	Institute for Radiation Protection & Nuclear Safety, France
COE, I.	AMEC, United Kingdom
ERASMUS, L.	Pebble Bed Modular Reactor (Pty) Ltd, South Africa
FIL, N.	OKB Gidropress, Russian Federation
GASPARINI, M.	International Atomic Energy Agency
HAKATA, T.	Nuclear Safety Commission, Japan
HILL, R.	ERIN Engineering, United States of America
IMBRO, G.	US NRC, United States of America
INABE, T.	Japan Atomic Energy Agency, Japan
MATHET, E.	AREVA, France
PETZER, C.	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