IAEA TECDOC SERIES

IAEA-TECDOC-1787

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

IAEA
International Atomic Energy Agency

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available at the IAEA Internet site

http://www-ns.iaea.org/standards/

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** consists of reports designed to encourage and assist research on, and development and practical application of, nuclear energy for peaceful uses. The information is presented in guides, reports on the status of technology and advances, and best practices for peaceful uses of nuclear energy. The series complements the IAEA's safety standards, and provides detailed guidance, experience, good practices and examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

APPLICATION OF THE SAFETY CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS IN NUCLEAR POWER PLANTS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

IAEA-TECDOC-1787

APPLICATION OF THE SAFETY CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS IN NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

For further information on this publication, please contact:

Safety Assessment Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
April 2016

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Application of the safety classification of structures, systems and components in nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2016. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1787 | Includes bibliographical references.
Identifiers: IAEAL 16-01034 | ISBN 978–92–0–101116–9 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Safety measures. | Nuclear power plants — Design and construction — Safety measures. | Nuclear industry — Safety measures. | Radiation — Safety measures.

FOREWORD

IAEA Safety Standards Series No. SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, published in 2014, provides guidance on establishing the safety classification of the structures, systems and components (SSCs) of nuclear power plants in compliance with the requirements established in IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design, newly revised in 2016. On the request of some Member States, the Commission on Safety Standards requested the IAEA to consider developing a TECDOC to provide more technical detail in support of the methodology set out in SSG-30.

This publication describes how to complete the tasks associated with every step of the classification methodology set out in SSG-30 — in particular, how to capture all the SSCs to be safety classified. Emphasis is placed on the SSCs that are necessary to limit radiological releases to the public and occupational doses to workers in operational conditions. SSCs are expected to be classified to ensure that that they will be designed, manufactured, installed and operated with established processes in a way that their reliability and quality will be commensurate with their safety significance.

To make certain that the classification of SSCs is established in a consistent manner, this publication emphasises the need to identify first all the required safety functions to be accomplished for all of the plant states. Examples of design and manufacturing requirements associated with the different safety classes to reach the expected reliability and quality are also provided.

This publication provides information for organizations establishing a comprehensive safety classification of SSCs compliant with IAEA recommendations, and to support regulators in reviewing safety classification submitted by licensees.

The IAEA is grateful to the experts who contributed to this publication as participants at the meetings and with their comments to the drafts. The IAEA officer responsible for this publication was B. Poulat of the Division of Nuclear Installation Safety.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The goal of safety classification is to identify and classify structures, systems and components (SSCs) that are needed to protect people and the environment from harmful effects of ionizing radiation, based on their roles in preventing accidents, or limiting the radiological consequences of accidents should they occur. On the basis of their classification, SSCs are then designed, manufactured, operated, tested and inspected in accordance with established processes that ensure design specifications and the expected levels of safety performance are achieved.

IAEA Safety Standards Series No. SSG-30 [1], published in 2014, proposes a comprehensive and consistent approach to capture the SSCs of a nuclear power plant needed to achieve a high level of safety in operational and accident conditions, and to assign those SSCs in a class determined to reflect the safety significance of each of them. Nevertheless a complementary TECDOC aiming at giving more guidance to Member States to apply SSG-30 [1], and to establish their own safety classification was considered to be a useful addition to the Safety Guide.

Specific terms and nuclear terms used in this publication are to be understood as defined in the IAEA Safety Glossary unless otherwise specified in the text.

1.2. OBJECTIVE

This TECDOC aims at assisting any organization in establishing a comprehensive safety classification of SSCs compliant with the IAEA recommendations.

Guidance is provided to capture all SSCs to be classified and to assign each of them to the appropriate safety class to reflect its own safety significance.

To establish a comprehensive and consistent classification this TECDOC indicates the inputs for starting the classification and the different steps to be accomplished. It also provides further information and examples to assist with the understanding of the guidance already provided by the Safety Guide SSG-30 [1].

1.3. SCOPE

Practically, this publication aims at explaining how to complete the tasks attached to every step of the flow chart given in SSG-30 [1] figure 1 detailing the whole classification process, and at supporting guidance by providing examples illustrating what is expected to be done at the different steps.

It also provides further guidance to detail SSG-30 [1] section 4 “Selection of applicable engineering design rules” which is a fundamental outcome of any classification. Indeed safety classification of SSCs is required to ensure that they will be designed and manufactured with established processes in a way that their quality and reliability will be commensurate with their individual safety significance. Best practices and well proven design/manufacturing codes are indicated as examples for the different safety classes.

Later, and on the basis of the classification, a complete set of engineering rules must be specified to ensure that SSCs will be operated so that their specified quality and reliability is maintained during the plant life time. Requirements for the operation of NPP are given in IAEA Safety Standards Series No. SSR-2/2 [7]. Good practices to operate a plant safely is not in the scope of this TECDOC.

1.4. NUCLEAR SAFETY AND SAFETY CLASSIFICATION

According to the IAEA Safety Fundamentals [2], a nuclear facility must be designed, constructed, commissioned, operated and decommissioned with the constant objective to ensure the protection of the workers, public and the environment against the harmful effects of the ionizing radiation. Moreover, in compliance with safety principles 5 and 6 [2], controlling doses and radiation risks within specified limits established by the national regulators is insufficient in itself, and an optimization of the protection is necessary to make doses and radiation risks as low as reasonably achievable.

The application of those safety principles implies the installation of specific systems and components which are in a standby mode during normal operation and whose quality and reliability is largely influenced by the radiological consequences of their failure when they are requested to operate.

Most classified structures, systems and components are those whose failure, when requested to operate, lead to an increase of doses to workers or to the public.

Nevertheless, taking into account that conditions for safe operation of the plant could be significantly affected and degraded by the effects of internal or external hazards, structures, systems and components designed either to prevent or to limit propagation of the effects need to be identified and considered in the safety classification methodology. The recent Fukushima Daiichi accident has shown how large and important the consequences were when the protection of the plant against the effects of natural hazards was incomplete or inadequate. Thus classifying items to ensure plant protection against the effects of hazards is a good practice to stress their importance to safety and to achieve better reliability.

Although the loss of the monitoring for the correct accomplishment of safety functions does not lead to an increase of the radiological consequences, monitoring and display systems need also to be considered in the classification methodology.

2. CLASSIFICATION PROCESS

As the safety of the plant is dependent on the reliability or integrity of its individual structures, systems and components (SSCs), a systematic hierarchy and classification of every individual item is necessary to ensure that every SSC will be designed, manufactured, installed and operated with established processes in a way that its quality and reliability be commensurate with its significance to safety, as required by IAEA SSR-2/1 Safety Standard [3]:

> "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."

Ranking SSCs according to their significance to safety helps to determine the design, manufacturing, construction, commissioning and maintenance requirements to be applied to individual SSCs and to substantiate a graduated approach.

In that sense, classification contributes to ensuring that the structures, systems and components are systematically designed, constructed, and operated with sufficient quality to fulfil the safety functions they perform and, ultimately, the fundamental safety functions.

Classification is a top down process that begins with a basic understanding of the plant design, its safety analysis and how the main safety functions will be achieved.

Figure 1 indicates the main steps to be followed to achieve the classification of SSCs.

Note: Cross references indicated in the flowchart refer to the Safety Guide SSG-30 [1].

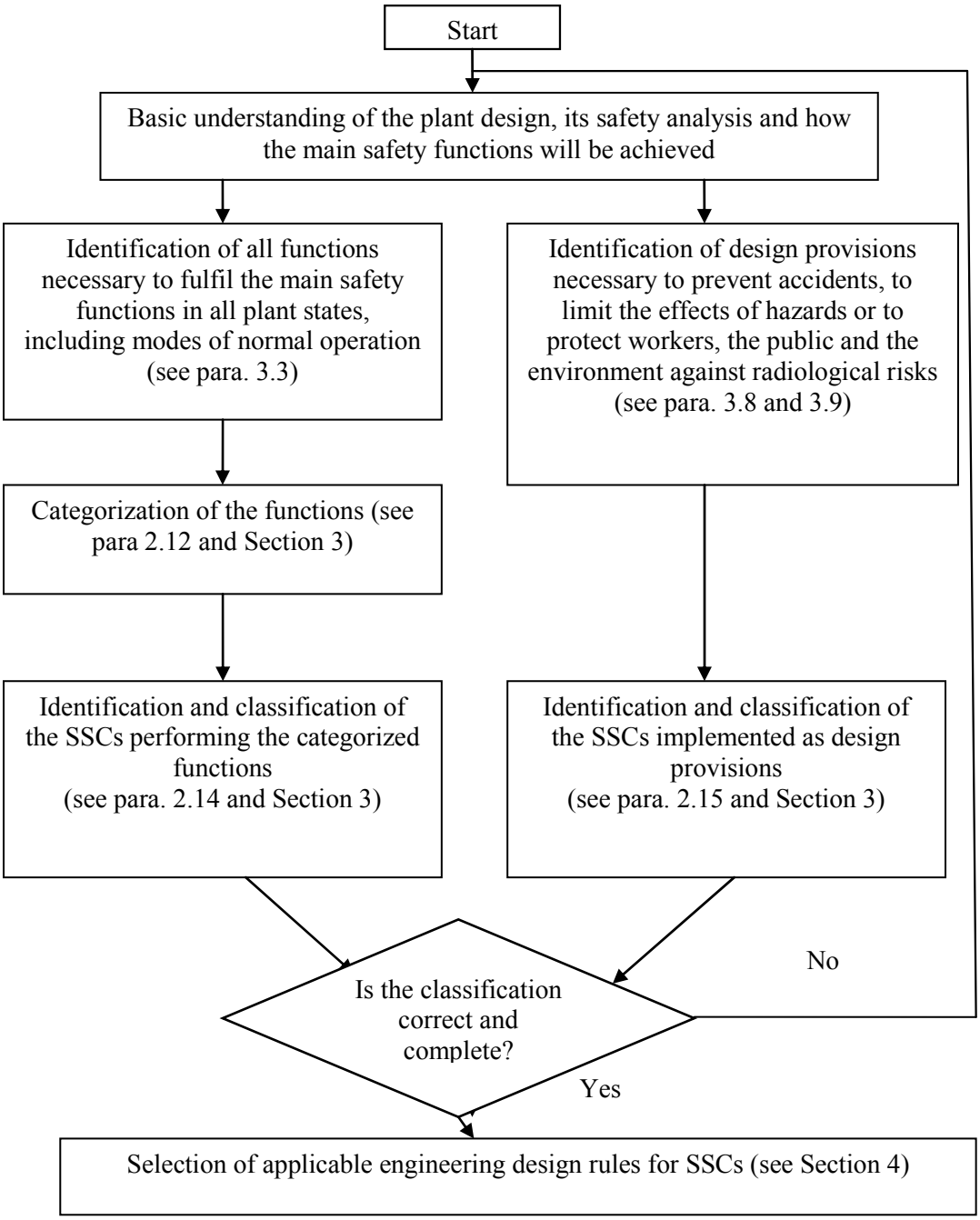

FIG. 1. Flow chart indicating the classification process (taken from SSG-30 [1]).

2.1. INPUTS

Prior to starting the safety classification process, it is necessary to understand how the plant is designed and to know the radiological release limits (consequences) established by the regulatory body for operational conditions and for the different accident conditions.

Classification is an important element in any design process and a good practice is to start to develop classification at the earliest stage of the design development even if the classification

of structures, systems and components (SSCs) cannot be completed as long as the detailed design itself is not completed.

Prior to establishing the classification, the plant states to be considered in the design are defined in accordance with IAEA SSR-2/1 [3], and include accident conditions with core melt. Plant states are usually defined as follows:

TABLE 1. PLANT STATES TO BE CONSIDERED FOR DESIGN

<table>
<tr><th colspan="5">Plant states considered in the design</th></tr>
<tr><td colspan="2">Operational states</td><td colspan="3">Accident conditions</td></tr>
<tr><td rowspan="2">Normal operation</td><td rowspan="2">Anticipated operational occurrences (AOOs)</td><td rowspan="2">Design basis accidents (DBAs)</td><td colspan="2">Design extension conditions (DEC)</td></tr>
<tr><td>without fuel damage</td><td>with core melt</td></tr>
</table>

Normal operation includes power operation, normal shutdown modes and associated transients to operate the reactor from one shutdown mode to another, refuelling mode and fuel handling activities, periodic tests, in service inspection and maintenance activities expected during the equipment lifetime.

Anticipated operational occurrences are events expected to occur during normal operation and that exceed the capability of the control systems and that have the potential to challenge the safety of the reactor. Anticipated operational occurrences also include the loss of the off-site power and minor leakage from a component containing radioactive materials.

Design basis accidents are unlikely and very unlikely events caused by a single failure that must be postulated to demonstrate that no off-site protective measures would be necessary for the public and the environment should they occur.

Design extension conditions are postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions include conditions in events without significant fuel degradation and conditions with significant fuel core degradation up to core melting.

Accidents that would result in early or large radioactive releases must be prevented by design with a high level of confidence, and consequently provisions or means to mitigate their consequences might not be required.

Practically, design extension conditions without significant fuel damage are conditions induced by sequences caused by multiple failures which have a frequency of occurrence that cannot be neglected, and in some cases, comparable with the frequency of some design basis accidents. In general, three types of multiple failures can be considered according to the systems in which they are postulated to take place:

- Initiating events that could lead to a situation beyond the capability of the safety systems that are designed for a single initiating event. A typical example is the multiple tube rupture in a steam generator of pressurized water reactors (PWRs).Multiple failures (e.g. common cause failures in redundant trains) that prevent the safety systems from performing their intended function to control the postulated initiating event (PIE). A typical example is a loss of coolant accident (LOCA) without actuation of the high pressure injection. Among the causes of failure of safety systems, implicitly included are the failures of the supporting systems;
- Multiple failures that cause the loss of a safety system used also to fulfil the fundamental safety functions in normal operation. This applies to designs that use, for example, the same heat transfer chain in accident conditions and during shutdown.

In accordance with Requirement 13 of SSR-2/1 [3] the subdivision/grouping of the plant states into categories is primarily based on an estimate of their frequency of occurrence at the nuclear power plant.

Table 2 below shows indicative values of the frequency of occurrence of individual scenarios considered in the plant state categories. These values are consistent with the generally established acceptable value for core damage frequency for new plants to be below 10^{-5}/y.

TABLE 2. PLANT STATES AND ESTIMATED FREQUENCIES OF OCCURRENCE OF INDIVIDUAL EVENTS

Plant state	Indicative frequency of occurrence
Normal operation	-
Anticipated operational occurrences	$>10^{-2}$ events per year
Design basis accidents	$10^{-2} – 10^{-6}$ events per year
Design extension conditions without core melt	$10^{-4} – 10^{-6}$ events per year
Design extension conditions with core melt	$<10^{-6}$ events per year

Prior to establishing the classification, PIEs considered in the design need to be identified and associated to the different plant states according to their estimated frequency of occurrence or as a result of regulatory requirements. Indeed safety classification aims at identifying and classifying items important to safety that are basically designed to limit the consequences caused by the PIEs, and to return the plant to a safe conditions.

PIEs to be considered include events caused by equipment malfunctioning or failure, operating errors, hazards originating inside the buildings or on site, man-induced hazards originating on the vicinity of the site and natural hazards.

The list of PIEs is expected to be as complete as possible during the initial design stages of the plant design.

Prior to establishing the classification, the reactor design is supposed to have been be developed and documented well enough to understand which functions need to be accomplished in the different plant states, and which system is expected to respond to a PIE, taking into account that the safety category and the safety class is influenced by the probability of the PIE occurring. Those functions need to be defined at an adequate level of

detail, enabling the identification of all of the SSCs necessary for performing the functions. This information is usually available in the plant system description, even preliminary.
Demonstration showing compliance of the design with the acceptance criteria and regulatory limits need to be conducted and documented. Moreover the safety analysis provides information on what systems are requested to operate to meet the requirements and dose limits.

Severity of the radiological consequences is a key parameter in determining the safety category taking into account that a function is assigned to the highest category when the radiological consequences exceed the specified limits authorized for design basis accidents, assuming the total loss of the function when challenged.

Practically the specified limits for the radiological consequences are well known, but the radiological consequences caused by the total failure of a function to be categorized are not always explicit in the safety analysis, simply because its total failure is not systematically postulated.

For cases where the information is not explicit, an estimate of the consequences can be made by a dedicated calculation or engineering judgment.

For example, anticipated operational occurrences combined with the loss of the limitation functions, and anticipated transient without scram (ATWS) are usually considered in the safety analysis report (SAR), but a design basis accident is usually not combined with the total loss of the safety systems.

As the safety classification is first established on the basis of deterministic safety analyses, the availability of a PSA level 1 is not a strict prerequisite for the safety classification. Nevertheless, probabilistic insights derived from PSA level 1 need to be available later to verify the correctness of the classification established on a deterministic basis.

The way in which the concept of defence in depth has been applied to the reactor design is supposed to be clearly understood taking into account that the expected reliability and quality of SSCs are largely influenced by the level of defence in depth to which the SSCs belong. Indeed the defence in depth concept does not be understood as limited to the requirement for the implementation of a number of consecutive barriers and protection levels, but has to be understood as any requirement necessary to achieve the quality and reliability expected for the barriers and for systems ensuring their integrity. Moreover, defence in depth requires, to the extent practicable, for independent systems to accomplish the main safety functions in the different plant states. Therefore, the way in which defence in depth has been implemented needs to be understood in order to understand which systems are intended to operate in a specific plant state.

Example: The heat removal function is requested in every plant state but is generally not accomplished by the same systems in power generation mode, in shutdown modes, or in accident conditions.

To make the categorization easily understandable, and subsequently the classification of the associated systems, it is preferable to break fundamental safety functions into different sub functions reflecting the plant state during which they are necessary.

As explained by paragraph 2.12 of SSG-30 [1], functions are categorized into a limited number of categories on the basis of their safety significance assessed by screening the following three factors:

1. The consequences of failure to perform the function: those consequences are calculated or postulated by using engineering experience and compared to the different limits established by the regulator for the different accident categories. Consequences may also be assessed using some acceptance criteria;
2. The frequency of occurrence of the postulated initiating event for which the function will be called upon: this frequency of occurrence is either the frequency calculated by probabilistic analyses or the plant state category (normal operation, anticipated operational occurrences, design basis accident and design extension conditions) may be sufficient to discriminate the probability of the postulated initiating events;
3. The significance of the contribution of the function in achieving either a controlled state or a safe state.

All of this information is generally obtainable from the plant system description.

2.2. IDENTIFICATION OF FUNCTIONS TO BE CATEGORIZED

A safety classification of the plant structures, systems and components is also necessary to make sure that they will be manufactured and operated according to requirements established commensurately with their safety significance so that the expected level of safety for every SSC is achieved.

Feedback from the current classifications, established in different Member States according to their domestic standards or guides, shows differences mainly on the classification of auxiliary or supporting systems, and on the classification of complementary safety features implemented to mitigate consequences of events originally not considered for the design of the plant.

One of the goals of the new Safety Guide SSG-30 [1] is also to make the whole classification of systems and associated SSCs clearer and more consistent by suggesting defining first the required functions to be accomplished for all of the plant states. Thus function categorization has to be understood as a useful tool for the classification, but not as strictly necessary.

Defining functions also enables identification of all of the systems that have to operate together to accomplish a particular function, and consequently makes the classification clearer and more consistent by assigning all of the systems requested for one function to the same safety class. This proof of consistency did not exist when systems were classified independently.

Categorization of a function, and later, classification of all the systems in a same safety class does not preclude assigning the associated SSCs in different safety classes provided that their individual safety significance is not the same.

Moreover categorization can replace classification when the design is still insufficiently developed as for example at the conceptual stage when all systems are not yet designed.

The proposed classification established by the vendor/designer or the license applicant has to be approved by the regulatory body and consequently has to be understood. As reviewing and approving a safety classification on the basis of a detailed and complete list of SSCs is not practicable, practically, regulators require that the safety principles and the methodology used be submitted and clear.

Providing a categorization of the functions requested for the different plant states substantiates the classification of the systems and components.

Explaining that the function category is a key element for the system classification meets the regulator's expectation.

Paragraph 3.2 of SSG-30 [1]
For the purposes of simplification, the term 'function' includes the primary function and any supporting functions that are expected to be performed to ensure the accomplishment of the primary function.

Paragraph 3.3 of SSG-30 [1]
The functions to be categorized are those required to achieve the main safety functions for the different plant states, including all modes of normal operation. These functions are primarily those that are credited in the safety analysis and should include functions performed at all five levels of defence in depth, i.e. prevention, detection, control and mitigation safety functions.

Paragraph 3.4 of SSG-30 [1]
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.

Paragraph 3.5 of SSG-30 [1]
The list of functions identified may be supplemented by other functions, such as those designed to reduce the actuation frequency of the reactor scram and/or engineered safety features that correct deviations from normal operation, including those designed to maintain the main plant parameters within the normal range of operation of the plant. Such functions are generally not credited in the safety analysis.

Paragraph 3.6 of SSG-30 [1]
Owing to the importance of monitoring to safety, functions for monitoring to provide the plant staff and the off-site emergency response organization with sufficient reliable information in the event of an accident should be considered for safety categorization. This should include monitoring and communication as required under the emergency response plan.

Paragraph 3.7 of SSG-30 [1]
Functions credited in the safety analysis with either preventing some sequences resulting from additional independent failures from escalating to a severe accident, or mitigating the consequences of a severe accident, are included in functions associated with design extension conditions.

The level of details of the functions to be identified depends on the current design development stage. It is recommended to detail functions and sub functions as much as needed to cover all of the different actions to be accomplished by the systems in the different plant states.

The number of functions is usually limited at the conceptual stage but grows when the design is in development.

Table 3 below gives an example of a list of functions that may be used at an early design stage.

TABLE 3. EXAMPLE OF A LIST OF FUNCTIONS USED AT AN EARLY DESIGN STAGE

Fundamental Safety Function	**Functions to be categorized for the different plant states**
Control of Reactivity	**R**1 - Maintain core criticality control
	R2 - Shutdown and maintain core sub-criticality
	R3 - Prevention of uncontrolled positive reactivity insertion into the core
	R4 - Maintain sufficient sub-criticality of fuel stored outside the RCS but within the site
Heat removal	**H**1 - Maintain sufficient RCS water inventory for core cooling
	H2 - Remove heat from the core to the reactor coolant
	H3 - Transfer heat from the reactor coolant to the ultimate heat sink
	H4 - Maintain heat removal from fuel stored outside the reactor coolant system but within the site
Confinement of radioactive material	**C**1 - Maintain integrity of the fuel cladding
	C2 - Maintain integrity of the reactor coolant pressure boundary
	C3 – Limitation of release of radioactive materials from the reactor containment
	C4 – Limitation of release of radioactive waste and airborne radioactive material
Extra	**X**1 –Protection and prevention against effects of hazard
	X2 - Protect of workers against radiation risks
	X3 - Limit the consequence of hazard
	X4 – Plant operation in accident conditions and monitoring of plant parameters
	X5 - Monitor radiological releases in normal operation
	X6 - Limits and conditions for normal operation

Table 4 illustrates, for PWR technology, how the function ‘Control of reactivity’ can be more detailed.

TABLE 4. EXAMPLE OF A LIST OF FUNCTIONS USED IN DETAILED DESIGN

Control of Reactivity	R1 – Maintain core criticality control	R-1.1: Control of RCS boric acid concentration
		R-1.2: Control rod position
		R-1.3: Control reactor power distribution
		R-1.4: Control reactor thermal power
		R-1.5: Control linear power density
		R-1.6: Control pellet-clad interaction risk
		R-1.7: Control departure from nucleate boiling risk
		R-1.8: Limit reactor thermal power
		R-1.9: Limit linear power density
		R-1.10: Limit pellet-clad interaction risk
		R-1.11: Limit departure from nucleate boiling risk
		R-1.12: Reduce reactor power
	R2 - Shutdown and maintain core sub-criticality	R-2-1: Fast negative reactivity insertion into reactor core (reactor trip)
		R-2 2: Injection of high borated water into RCS at high pressure (e.g. in case of anticipated transients without scram)
		R-2 3: Injection of high borated water into RCS at medium and low pressure in case of DBA
		R-2.4: Compensate for reactivity increase during plant cooldown to the safe shutdown state by increasing the boric acid concentration in the RCS
	R3 - Prevention of uncontrolled positive reactivity insertion into the core	R-3.1: Restrict feedwater flow to steam generator (SGs) after reactor trip
		R-3.2: Isolation of feedwater supply to a damaged SG
		R-3.3: Prevent SG draining to RCS in case of SG tube rupture
		R-3.4: Prevent uncontrolled SG depressurization - Stop steam flow to turbine
		R-3.5: Prevent uncontrolled SG depressurization - Stop steam flow to atmosphere
		R-3.6: Prevent uncontrolled SG depressurization - Stop steam flow to main steam system
		R-3.7: Stop RCS forced flow to limit heat exchange in the SG
		R-3.8: Prevent component cooling water flow to RCS through leakage on heat exchanger (at low RCS pressure)
		R-3.9: Stop demineralized water make-up to RCS
	R4 - Maintain sufficient sub-criticality of fuel stored outside the RCS but within the site	R-4.1: Control of spent fuel pool water boric acid concentration

Tables 10–14 provide other examples showing how the functions can be detailed to better tailor the need.

2.3. CATEGORIZATION OF THE FUNCTIONS

According to SSG-30 [1] three factors should be used to categorize the identified safety functions into safety categories according to their safety significance.

Paragraph 2.12 of SSG-30 [1]
The functions should then be categorized into a limited number of categories on the basis of their safety significance, using an approach which takes account of the following three 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 significance of the contribution of the function in achieving either a controlled state or a safe state.

Regarding factor 1), SSG-30 [1] provides guidance to estimate the consequences, and how those potential consequences influence the safety category.

Paragraph 3.11 of SSG-30 [1]
The three levels of severity should be defined as follows:

- The severity should be considered 'high' if failure of the function could, at worst:
  - Lead to a release of radioactive material that exceeds the limits for design basis accidents accepted by the regulatory body; or
  - Cause the values of key physical parameters to exceed acceptance criteria for design basis accidents.
- The severity should be considered 'medium' if failure of the function could, at worst:
  - Lead to a release of radioactive material that exceeds limits established for anticipated operational occurrences; or
  - Cause the values of key physical parameters to exceed the design limits for anticipated operational occurrences.
- The severity should be considered 'low' if failure of the function could, at worst:
  - Lead to doses to workers above authorized limits.

Where more than one of these definitions is met, the highest of the three levels should be applied. The assessment of the consequences is made postulating that the function does not respond when challenged.

For anticipated operational occurrences, in order to avoid 'over-categorization' the assessment of the consequences should be made with the assumption that all other independent functions are performed correctly and in due time.

For the purpose of the categorization of the functions, SSG-30 [1] suggests using the different dose limits established by the regulatory body to characterize the severity of the radiological consequences. Those dose limits are assumed to be known when the classification is established.

Severity may also be characterized by compliance or non-compliance with design criteria. Examples of design criteria that could be used:

- Design acceptance criteria regarding physical parameters (e.g. RCS pressure, fuel cladding temperature, criticality);

- Design acceptance criteria regarding barrier integrity (e.g. departure of nucleate boiling ratio as a decoupling criterion to prevent fuel cladding failure);
- Design criteria regarding the non-aggravation of the accident (e.g. non-aggravation from an anticipated operational occurrence to a design basis accident, non-aggravation from a design extension condition without core melt to a severe accident).

Table 5 gives examples of radiological limits or design criteria that may be used to characterize the severity of consequences.

TABLE. 5 EXAMPLES OF ACCEPTED LIMITS IN DIFFERENT PLANT STATES

Plant state	**Radiological Limits**	**Examples for design acceptance criteria**
Normal plant operation	• Occupational dose limit to plant staff - effective dose: 20 mSv/year - 1.0 mSv per single exposure	• Plant parameters are within the range specified for normal operation.
AOO	• Off-site dose limit for the public effective dose: 1.0 mSv/year	• Should not be the origin of an accident having more serious consequences (e.g. DBA) • No departure from nucleate boiling • Integrity of reactor coolant pressure boundary (RCPB) is preserved • RCS pressure below code limit (e.g. below 100% design pressure)
DBA	• DBA dose limit as accepted by the regulatory body	• LOCA criteria for fuel (peak cladding temperature, oxidation of fuel cladding, etc.) • Acceptable number of fuel rod failures • Containment pressure below 100% design pressure • RCS pressure below limit from well-accepted codes, e.g. 110% design pressure according to ASME code

Practically the assessment of the consequences can be performed as follows:

- The assessment of the safety significance of anticipated operational occurrences related functions is performed assuming that other functions for anticipated operational occurrences (i.e. reactor trip) or for design basis accidents (functions accomplished by the safety systems) will respond as expected, provided that the associated systems are not affected by the initiating event;
- The assessment of the safety significance of functions used to mitigate the consequences of design basis accidents or design extension conditions needs to be performed ignoring the role of other functions allocated to other defence in depth levels.

Regarding factor 2), SSG-30 [1] provides guidance to estimate the frequency for a function to be called upon.

Paragraph 3.12 of SSG-30 [1]
Factor 2 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.

The frequency for a function to be called upon can be assimilated with the frequency of occurrence of the postulated initiating events for which the function is required. For early categorization, if the frequency of occurrence of the PIE is not available, the plant state category can be used. Table 2 gives an indicative relationship between plant states and the frequency of PIEs.

Regarding factor 3), SSG-30 [1] indicates when factor 3) can be used.

Paragraph 3.14 of SSG-30 [1]
Factor 3) concerns functions intended to reach a particular plant state. Generally two plant states are distinguished, namely a controlled state[1] and a safe state[1]. For functions that are performed to achieve a controlled state, the main focus is on automatic actuation or short term actuation, in order to reduce considerably the hazard potential. Functions that are applied to achieve a safe state are longer term functions, and are performed once the controlled state has been achieved. In many cases, for reactors, the functions applied following an accident transient will achieve a controlled state first before achieving a safe state. Typical functions for the controlled state are reactor trip, decay heat removal and safety injection; whereas depressurizing the reactor and connecting up the residual heat removal system to ensure long term decay heat removal function are good examples of functions that are performed to achieve a safe state.

Although factor 3) does not have the same importance as the first two factors for the categorization, its use corresponds to the practice of some Member States. When used, factor 3) aims at discriminating functions requested to be accomplished in the short term after the onset of the accident and functions to be accomplished later. This discrimination takes into account that functions belonging to the first group are expected to be automatically actuated while the functions associated to the second group may be initiated by the operator. The justification to credit factor 3) is that there is some time available to accomplish the functions and therefore, possibilities to recover them exist in the case that the associated systems do not respond immediately.

To properly apply factor 3), it is advised to make the discrimination consistent with the definition of controlled state and safe state.

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

TABLE 6. CHARACTERISTICS OF CONTROLLED STATE AND SAFE STATE IN THE MITIGATION OF AOOS AND DBAS

	For reactor core	**For spent fuel**
Controlled State	• core is subcritical • heat removal is assured for a time sufficient to implement provisions to reach a safe state, e.g. via steam generators for PWR • coolant inventory is stable • radioactive release meets regulatory limits	• fuel storage is subcritical • water level is stabilized and the water inventory is adequate for spent fuel cooling and shielding • radioactive release meets regulatory limits
Safe State	• the core is subcritical • residual heat removal is assured on a long term basis, for example via residual heat removal heat exchanger • reactor coolant inventory is recovered • radioactive releases are controlled and acceptable	• fuel storage is subcritical • water level is stabilized and the water inventory is adequate for spent fuel cooling and shielding spent fuel pool cooling is established on a long term basis • radioactive releases are controlled and acceptable

Categorization of the functions is established taking into account the three factors as suggested by Table 1 of SSG-30 [1] repeated in Table 7.

TABLE 7. RELATIONSHIP BETWEEN FUNCTIONS CREDITED IN THE ANALYSIS OF POSTULATED INITIATING EVENTS AND SAFETY CATEGORIES (TABLE 1 IN SSG-30 [1])

Functions credited in the safety assessment	**Severity of the consequences if the function is not performed**		
	High	**Medium**	**Low**
Functions to reach the controlled state after an AOO	1	2	3
Functions to reach the controlled state after a DBA	1	2	3
Functions to reach and maintain a safe state	2	3	3
Functions for the mitigation of consequences of DEC	2 or 3 (see para. 3.15 in SSG-30 [1])	NC	NC

Regarding the categorization of functions used in the mitigation of design extension conditions paragraph 3.15 of SSG-30 [1] states that the following functions should be assigned to category 2.

Paragraph 3.15 of SSG-30 [1]
Any function that is designed to provide a backup of a function categorized in safety category 1 and that is required to control design extension conditions without core melt.

According to the plant state categories, design extension condition functions are required either to prevent a situation caused by multiple failures (e.g. PIE combined with multiple failures making the safety systems unable to accomplish their intended functions) from escalating to a core melt accident, or to mitigate a core melt accident within acceptable radiological consequences.

Consequently, the consequences of the failure of a design extension condition function when challenged are always 'high' consequences. However, as the frequency for a function to be called upon is also a factor to be considered for the categorization, SSG-30 [1] suggests the following categorization:

- Functions used in severe accidents are expected to have the lowest frequency of use and therefore may be categorized in category 3 with specific and appropriate design requirements. Such a categorization is consistent with the current practice of Member States;
- Functions necessary to cope with multiple failure conditions and acting as a backup to a failed category 1 function may still have a frequency of use that is comparable with the frequency of a rare design basis accident (refer to Table 2). Assigning these functions also to category 3 would not properly reflect their safety significance. SSG-30 [1] recommends therefore assigning these functions to category 2 (one grade less than the category of the function they are backing up);
- Functions that are used in multiple failure conditions but that are not required in the short term after the onset of the accident may be assigned to category 3.

Implemented as a backup of a function necessary to mitigate a design basis accident without escalation to a core melt, the relevant design extension condition safety features are expected to have a sufficient reliability so that their probability to fail when called upon is consistent with the objective of the core damage frequency.

With the update of SSR-2/1 [3], made after the Fukushima Daiichi accident, requirements aiming at increasing the reliability of the heat transfer chain to the ultimate heat sink as a whole, or of the on-site AC and DC sources have been enhanced. As a result, additional systems of components are expected to be installed to cope with the most likely CCF. The category 3 may be assigned to the functions accomplished by those new systems provided that they are not necessary in the short term. An example to illustrate this issue is the additional set of emergency diesel generators installed at some plants to cope with a station blackout (SBO), or the diverse heat transfer chain. Indeed, during SBO conditions the objective is to preserve the fuel integrity and the reactor coolant pressure boundary integrity but not to operate the plant to the safe shutdown conditions. Consequently that additional set of diesel generators is not requested to be designed with the same performances as the main

diesel generators. Moreover, the coping time available is sufficient to make use of operator actions.

TABLE 8. SAFETY FUNCTION CATEGORIES

a) Safety category 1

Definitions	**Example**
Any function required to reach the controlled state after an AOO or a DBA and whose failure, when challenged, would result in consequences of 'high' severity.	Automatic and fast reactor trip; Core cooling for Design basis accident.

b) Safety category 2

Definitions	**Example**
Any function required to reach the controlled state after an AOO or a DBA and whose failure, when challenged, would result in consequences of 'medium' severity;	Functions associated with limiting off-site releases in DBAs (e.g. filtered HVAC) provided their failure would not directly lead to releases above authorized limits;
Any function required to reach and maintain a safe state for a long time and whose failure, when challenged, would result in consequences of 'high' severity;	Residual heat removal in the long term;
Any function designed to provide a backup of a function categorized in safety category 1 and required to control DEC without core melt.	Diverse actuation trip function as a backup of the reactor trip function.

c) Safety category 3

Definitions	**Example**
Any function actuated in the event of an AOO or DBA and whose failure when challenged would result in consequences of 'low' severity;	Functions designed to prevent the use of safety systems in AOOs (e.g. normal and auxiliary pressurizer spray);
Any function required to reach and maintain a safe state for a long time and whose failure, when challenged, would result in consequences of 'medium' severity;	Service water filtration (if necessary in the longer term).
Any function required to mitigate the consequences of DEC, unless already required to be categorized in safety category 2, and whose failure, when challenged, would result in consequences of 'high' severity;	Containment heat removal in case of a severe accident;

Definitions	Example
Any function designed to reduce the actuation frequency of the reactor trip or engineered safety features in the event of a deviation from normal operation, including those designed to maintain the main plant parameters within the normal range of operation of the plant;	The reactor power control in an AOO to avoid emergency shutdown; Control the water level of the pressurizer by normal charge or letdown flowrate to avoid safety inject; Control the pressure of the pressurizer by spray and heater to avoid opening the safety release valve of the pressurizer; Control the water level of the SG by normal feedwater to avoid auxiliary feedwater run; Control the pressure of the SG by the steam turbine bypass system to avoid opening the main steam safety valve.
Any function relating to the monitoring needed to provide plant staff and off-site emergency services with a sufficient set of reliable information in the event of an accident (DBAs or DEC), including monitoring and communication means as part of the emergency response plan (DID level 5), unless already assigned to a higher category.	Emergency feedwater tank level monitoring; Safety injection tank pressure detection; Emergency communication, emergency lighting function;
The function which is used for limiting the effects of internal/external hazards.	Fire extinguishing; fire containing by closure of fire dampers on demand of a fire detection system.

2.4. EXAMPLES OF CATEGORIZATION OF THE FUNCTIONS (FOR PWR)

As previously mentioned, the majority of functions to be categorized can be derived from the accident analysis. The following sections provide four examples illustrating this approach.

TABLE 9. EXAMPLES OF PIES TO BE CONSIDERED TO IDENTIFY FUNCTIONS

Section	Postulated Initiating Event	Plant state
2.4.1	Loss of off-site power (<2h) during power states	Anticipated operational occurrence
2.4.2	Small break LOCA (⩽50cm²) during power states	Design basis accident
2.4.3	Anticipated transient without scram (due to blockage of control rods)	Design extension condition without core melt
2.4.4	Severe Accident	Design extension condition with core melt

2.4.1. Loss of off-site power (LOOP) <2h during power states

Plant state:
This event is classified as an anticipated operational occurrence expected to occur during the plant lifetime.

Following this anticipated operational occurrence the objective is to resume power operation. Thus, for the purpose of safety classification it is sufficient to analyze the event up to the controlled state.

Approach:
It is assumed that a safety analysis for the event is already available. This analysis will then also allow for identification of the safety functions necessary to control the event.

Paragraph 3.10 of SSG-30 [1] explains that the functions required for fulfilling the main safety functions should be categorized according to their safety significance. To derive this significance it is recommended to analyze the severity of consequences that could arise if the safety function would not be performed. The levels of severity are defined in §3.11 of SSG-30 [1].

In addition paragraph 3.11 of SSG-30 [1] states:
For anticipated operational occurrences, in order to avoid 'over-categorization', the assessment of the consequences should be made with the assumption that all other independent functions are performed correctly and in due time.

With respect to the implementation of the defense in depth principle it is proposed to interpret this statement as follows:

- The assessment of the safety significance of anticipated operational occurrences related functions can be performed assuming that other functions for anticipated operational occurrences (i.e. reactor trip) or for design basis accidents (functions accomplished by the safety systems) will respond as expected, provided that the associated systems are not affected by the initiating event;
- The significance of an anticipated operational occurrence related safety function cannot be lowered due to the fact that an independent design extension condition safety function would also be available to control the event.

Additional guidance for the analysis of anticipated operational occurrence related safety functions is given in paragraph 3.15 of SSG-30 [1], especially:

Safety category 1

- Any function that is required to reach the controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of 'high' severity:

Safety category 2

- Any function that is required to reach a controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of ‘medium’ severity:

Safety category 3

- Any function that is 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;
- Any function that is designed to reduce the actuation frequency of the reactor trip or engineered safety features in the event of a deviation from normal operation, including those designed to maintain the main plant parameters within the normal range of operation of the plant.

Analysis:
For a typical PWR the safety analysis for a short LOOP event will demonstrate that the following safety functions are achieved until a controlled plant state is reached.

TABLE 10. EXAMPLES OF IDENTIFIED FUNCTIONS FOR A LOOP

Main Safety Function	**Safety Function**		**Category and Explanation**	**Example SSCs performing the function**
Control of reactivity	R-2 Shutdown and maintain core sub-criticality	Fast negative reactivity insertion into reactor core	**Cat. 1** (Consequences are 'high' as key physical parameters would be beyond acceptance criteria for DBAs)	Scram system, reactor trip signal from protection system
	R-3 Prevention of uncontrolled positive reactivity insertion into the core	Prevent uncontrolled SG depressurizatio n - Stop steam flow to main steam system	**Cat. 2** or **Cat. 3** (Consequences are at most 'medium' as the reactivity transient in case of failure of the function would be covered by DBAs like 'main steam line break')	Turbine trip system, turbine trip signal
Heat removal	H-1 Maintain sufficient RCS water inventory for core cooling	Primary make-up to compensate for RCS leakages in normal operation	**Cat. 3** ('low' consequences as failure of this function would at most lead to engineered safety feature actuation system actuation, e.g. actuation of the emergency core cooling system)	Volume control system and supporting SSCs
	H-2 Remove heat from the core to the reactor coolant	Heat transfer from reactor core to steam generators (natural circulation)	**Cat. 1** ('high' consequences in case of failure)	
	H-3 Transfer heat from the reactor coolant to the ultimate heat sink	Steam release to the atmosphere	**Cat. 1** ('high' consequences in case of failure)	Main steam safety valves and supporting SSCs
		Feedwater supply to the steam generators	**Cat. 1** (if secondary side water inventories are not sufficient in a short LOOP event and 'high' consequences are to be postulated in case of failure of the function) **Cat. 3** or even **NC** (if secondary side water inventories are sufficient in a short LOOP event)	Auxiliary feedwater system and supporting SSCs
Confinement of radioactive substances	C-2 Maintain integrity of the Reactor Coolant Pressure Boundary	Limitation of primary pressure increase below design pressure	**Cat. 3** ('low' consequences if the pressurizer relief valve would be actuated upon failure of this function)	(Auxiliary) pressurizer spray system and supporting SSCs

2.4.2. Small Break Loss of Coolant Accident (≤50cm²) during power states

Plant state:
A small break in the reactor coolant system induces a discharge of primary coolant into the containment. It results in a loss of coolant inventory and thus in a reactor coolant system pressure decrease. This accident might lead to the uncovering of the fuel assemblies and to cladding failure by departure from nucleate boiling. It also induces a possible core heat-up, containment loads by overpressure due to mass and energy release as well as dynamic mechanical loads on reactor coolant system components and the associated supports and structures as well as on reactor pressure vessel internals.

SBLOCA is classified as a design basis accident that the plant is expected to withstand without acceptable limits for radiation protection being exceeded.

Approach:
It is assumed that a safety analysis for the event is already available. This analysis will then also allow for identification of the safety functions necessary to control the event.

Paragraphs 3.10, 3.11 and 3.15 of SSG-30 [1] give the necessary guidance to categorize these functions according to their safety significance.

The severity of consequences is assessed without crediting mitigation possibilities provided by design extension condition functions.

For design basis accidents all functions necessary to transfer the plant into the safe state need to be identified and categorized in order to ensure completeness of the safety classification.

Guidance for the categorization of the identified functions is given in IAEA SSG-30 [1], §3.11 and §3.15, especially:

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

Safety category 2:
- Any function that is required to reach a controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of ‘medium’ severity;
- Any function that is required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of ‘high’ severity;

Safety category 3:
- Any function that is 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;
- Any function that is required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of ‘medium’ severity;

Analysis:
In this example the following simplified plant response to a SBLOCA event is assumed (various features which are specific to certain reactor designs are not considered, e.g. containment spray, switchover of the ECCS suction to sump recirculation mode, etc.).

From the initiating event to the controlled state:

- The break on the reactor coolant system induces a loss of coolant. As it is assumed to be not compensable by the normal primary make-up system it results in a primary pressure and inventory decrease;
- Reactor trip is actuated, e.g. on low RCS pressure;
- Turbine trip and main feedwater system isolation are actuated after reactor trip and the secondary side pressure is limited by steam generator relief devices;
- The high pressure pumps of the emergency core cooling system (ECCS) are also automatically actuated, e.g. on low RCS pressure. The reactor coolant pumps are tripped. The steam generators are fed by the auxiliary service water system;
- Containment pressure and temperature increase due to the mass and energy release from the reactor coolant system into the containment. Containment penetrations of systems not necessary for accident mitigation are automatically closed, e.g. upon a high containment pressure signal;
- The injection capacity of the emergency core cooling system is initially insufficient to compensate for the break flowrate, such that reactor coolant inventory and pressure continue to decrease. The break flowrate decreases as the void fraction in the cold legs increases. Refilling of the reactor starts when the ECCS flowrate exceeds the break flowrate; e.g. when the break flow changes to single-phase steam.

Afterwards a controlled state is reached as follows:

- The reactor core is subcritical;
- Decay heat removal is ensured via the secondary side (the break flow in a SBLOCA event does not allow for decay heat removal through the break);
- Confinement of radioactive substances inside the containment with closed containment penetrations.

From this analysis the following safety functions are identified and categorized according to their safety significance.

TABLE 11. EXAMPLES OF IDENTIFIED FUNCTIONS FOR A SMALL LOCA AT POWER OPERATION (TO REACH THE CONTROLLED STATE)

Main Safety Function	**Safety Function**		**Category and Explanation**	**Example SSCs performing the function**
Reactivity control	R-2 Shutdown and maintain core sub-criticality	Fast negative reactivity insertion into the reactor core	**Cat. 1** ('high' Consequences as key physical parameters would be beyond acceptance criteria for DBA)	Scram system, Reactor trip signal from protection system
Heat removal	H-1 Maintain sufficient RCS water inventory for core cooling	Safety Injection into reactor coolant system	**Cat. 1** ('High' consequences as excessive core uncovering would occur if the function is not fulfilled)	High-pressure emergency core cooling system and supporting SSCs
		Stop forced primary flow	**Cat. 1** (If this function is necessary to prevent excessive core uncovering	Reactor coolant pump circuit breakers and supporting SSCs
	H-2 Remove heat from the core to the reactor coolant	Heat transfer from reactor core to steam generators (natural circulation)	**Cat. 1** ('High' consequences in case of failure)	
	H-3 Transfer heat from the reactor coolant to the ultimate heat sink.	Steam release to the atmosphere	**Cat. 1** ('High' consequences as decay heat removal is not ensured via the break flow in a SBLOCA event)	Main steam safety valves and supporting SSCs
		Feedwater supply to the steam generators	**Cat. 1** (High' consequences as decay heat removal is not ensured via the break flow in a SBLOCA event)	Auxiliary feedwater system and supporting SSCs
Confinement of radioactive substances	C-3 Limitation of release of radioactive materials from the reactor containment	Isolation of containment penetrations	**Cat. 1** (assuming releases above limits for DBAs if this function would not be performed)	Containment isolation system and supporting SSCs

From the controlled state to the safe state:

- A secondary side cooldown is manually initiated from the main control room in order to reduce the primary pressure to conditions for connection of the residual heat removal system;
- In order to ensure that the reactor core is subcritical at low temperatures the boric acid system is also manually started**;**
- The residual heat removal system pumps are manually started once the primary and secondary pressure conditions allow for it.

Afterwards a safe state is reached as follows:

- The reactor core is subcritical;
- Durable decay heat removal is ensured by the reactor residual heat removal system and the heat transport chain;
- Confinement of radioactive substances inside the containment with closed containment penetrations.

From this analysis the following safety functions are identified and categorized according to their safety significance:

TABLE 12. EXAMPLES OF IDENTIFIED FUNCTIONS FOR A SMALL LOCA AT POWER OPERATION (TO REACH THE SAFE STATE)

Main Safety Function	**Safety Function**		**Category and Explanation**	**Example SSCs performing the function**
Reactivity control	R-2 Shutdown and maintain core sub-criticality	Injection of high borated water into RCS at medium and low pressure.	**Cat. 2** (Any function required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of 'high' severity). Note: Potential consequences are considered 'high' as the manual cooldown needs to be finalized before secondary side water reserves are depleted.	Emergency core cooling system and supporting SSCs
Heat removal	H-1 Maintain sufficient RCS water inventory for core cooling	Injection of water into reactor coolant system.	**Cat. 2** (Any function required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of 'high' severity).	Emergency core cooling system and supporting SSCs
	H-3 Transfer heat from the reactor coolant to the ultimate heat sink.	Controlled steam release to the atmosphere (secondary side cooldown).	**Cat. 2** (Any function required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of 'high' severity).	Main steam relief trains and supporting SSCs
		Feedwater supply to the steam generators.	**Cat. 2** (Any function required to reach and maintain a safe state for a long time and whose failure, when challenged, would result in consequences of 'high' severity).	Auxiliary feedwater system and supporting SSCs
		Primary side heat removal at low pressure	**Cat. 2** (Any function required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of 'high' severity).	Residual heat removal system and supporting SSCs

2.4.3. Anticipated transient without scram (due to blockage of control rods)

Plant state:
This multiple failure event is classified as a design extension condition without core melt.

In order to cope with a postulated loss of the scram function diversified features for reactor shutdown are implemented into new reactor designs. The objective is to reach a controlled plant state and to limit radiological consequences below design basis accident limits despite the loss of the Category 1 function.

Approach:
It is assumed that a safety analysis for the event is already available. This analysis will then also allow for identification of the safety functions necessary to control the event.

Regarding the identification of the safety functions to be categorized it is sufficient to focus on the diversified features necessary to cope with the multiple failure event (other functions called in the event response are already identified in the analysis of anticipated operational occurrences and design basis accidents).

Guidance for assessing the safety significance of the identification and for the categorization is given in paragraph 3.15 of SSG-30 [1]:

Safety category 2:
- Any function that is designed to provide a backup of a function categorized in safety category 1 and that is required to control design extension conditions without core melt.

Safety category 3:
- Any function that is 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.

Analysis:
Anticipated transient without scram (ATWS) following the anticipated operational occurrence 'Loss of main feedwater in power states' is taken as an example for the analysis.

The following simplified plant response is assumed:

- After loss of main feedwater flow, the inventory of the SGs decreases whereas reactor coolant system temperature and pressure increase;
- Reactor trip and turbine trip are actuated, e.g. on low SG level or high reactor coolant pressure. However, due to the stuck control rods the scram function is not effective. The reactor power is only reduced due to moderator effect;
- Some control rods are still in high position whereas the reactor trip signal has been actuated ('ATWS signal'). Upon detection of this deviation the pumps of the boric acid system are started automatically and inject highly borated water into the reactor coolant system;
- The secondary side pressure increase following the turbine trip is automatically limited by SG relief devices. The automatic actuation of the pressurizer safety valves limits the primary side pressure increase and ensures that the reactor power is significantly reduced by formation of steam bubbles in the reactor core which reduces the moderator effect;

- The secondary side heat removal is ensured by the steam generator relief devices. The steam generators are fed by the pumps of the auxiliary feedwater system actuated on very low steam generator level;
- Later on, when the injected boron from the boric acid system reaches the reactor core, the power further decreases. In the long term, the core sub-criticality is ensured by the boron injection.

From this analysis the following safety functions are identified and categorized according to their safety significance.

TABLE 13. EXAMPLES OF IDENTIFIED FUNCTIONS FOR ATWS

Main Safety Function	**Safety Function**		**Category and Explanation**	**Example SSCs performing the function**
Reactivity control	R-2 Shutdown and maintain core sub-criticality	Injection of high borated water into RCS at high pressure.	**Cat. 2** (This function serves as a backup of the Cat. 1 function 'insertion of negative reactivity into the reactor core').	ATWS signal; boric acid system and supporting SSCs
Heat removal	H-3 Transfer heat to the ultimate heat sink	Steam release to the atmosphere	**Cat. 3** (Any function required to mitigate the consequences of DECs, unless already required to be categorized in safety category 2, and whose failure, when challenged, would result in consequences of 'high' severity). *Note: Only the role of the function in a DEC sequence is categorized here. The final category of this function will likely be determined by its safety significance in postulated DBAs.*	Main steam safety valves and supporting SSCs
		Feedwater supply to the steam generators.	**Cat. 3** (Any function required to mitigate the consequences of DECs, unless already required to be categorized in safety category 2, and whose failure, when challenged, would result in consequences of 'high' severity). *Note: Only the role of the function in a DEC sequence is categorized here. The final category of this function will likely be determined by its safety significance in postulated DBAs.*	Auxiliary feedwater system and supporting SSCs
Confinement of radioactive substances	C-2 Maintain integrity of the reactor coolant pressure boundary	Discharge coolant from the reactor cooling system.	**Cat. 2** (Together with the injection of boric acid this function serves as a backup of the Cat. 1 function 'insertion of negative reactivity into the reactor core').	Pressurizer Safety Valves and supporting SSCs

2.4.4. Severe Accident

Plant state:
This event belongs to the design extension conditions with core melt.

In order to prevent large or early radioactive releases to the environment the objective is to maintain the confinement function. New reactor designs provide specific features to ensure integrity of the containment in the course of accident sequences with core melt.

Approach:
In contrast to events on other DID levels there usually is not a single accident analysis available that would allow for identification of the safety functions necessary in severe accidents. Instead the design of the different severe accident features is usually based on a set of deterministic and/or probabilistic analyses from which the necessary information can be taken.

Paragraph 3.15 of SSG-30 [1] gives the necessary guidance for categorization of the functions identified:

Safety Category 3:
- Any function that is 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.

The functions necessary to mitigate severe accidents are therefore assigned to Category 3.

Analysis:
Table 14 lists a typical set of safety functions for which dedicated severe accident features are provided in new designs.

TABLE 14. EXAMPLES OF IDENTIFIED FUNCTIONS FOR ACCIDENT WITH CORE MELT

Main Safety Function	**Safety Function**		**Category and Explanation**	**Example SSCs**
Confinement of radioactive material	C-3 Limitation of release of radioactive materials from the reactor containment	Isolation of containment penetrations.	**Cat. 3** (Any function that is 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.)	Containment isolation system and supporting SSCs.
		Prevention of unfiltered containment leakages		Filtered ventilation systems in auxiliary buildings and supporting SSCs
		Maintain containment integrity –Melt retention		Core catcher and corium cooling system and associated supporting SSCs
		Maintain containment integrity - Management of combustible gases.		Hydrogen recombiners and supporting SSCs
		Maintain containment integrity - Prevention of direct containment heating		Primary circuit depressurization system and supporting SSCs
		Maintain containment integrity - Heat removal from containment and limitation of containment pressure increase.		Containment heat removal system (and/or containment venting system) and supporting SSCs.

2.5. IDENTIFICATION AND CLASSIFICATION OF SSC PERFORMING CATEGORIZED FUNCTIONS

The objective of safety classification is to link the safety significance of functions to design requirements (capability, reliability and robustness) of the SSCs performing these functions.

The safety significance at the component level is expected to be correctly reflected considering both the functional role and the barrier confinement role (if relevant) of the component.

All SSCs performing the categorized functions need to be identified and classified once the categorization of the safety functions is completed.

The identification and classification of SSCs is made in two sub steps. The classification starts at the system level and continues to the component level.

2.5.1. System Classification

Paragraph 3.17 of SSG-30 [1]

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

Once the safety functions are categorized, taking into account the results from Table 7, the systems necessary for the accomplishment of each safety function need to be identified including systems providing support to equipment of the front line system.

Systems are then assigned to a safety class corresponding to the safety category of the function they perform. The basis for this assignment is outlined in paragraph 3.19 of SSG-30 [1] and has the following implication:

- Safety Category 1 → SC1
- Safety Category 2 → SC2
- Safety Category 3 → SC3

2.5.2. Structures and Components Classification

To determine the classification at the component level, the four factors given in SSG-30 [1] should be considered.

Paragraph 2.2 of SSG-30 [1]
a) The safety function(s) to be performed by the item;
b) The consequences of failure to perform a safety function;
c) The frequency with which the item will be called upon to perform a safety function; and
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.

That analysis requires that SSCs (pumps, tanks, valves, instrumentation, heat exchangers, pipes, etc.) participating in the fulfilment of the safety functions are identified and their individual contribution to the accomplishment of the function understood.

First, the factors a) and c) are used to determine a preliminary safety class of the items that participate in the fulfilment of the safety functions. This is outlined in SSG-30 [1].

Paragraph 3.19 of SSG-30 [1]
By applying factors a) and c) defined in paragraph 2.2, SSCs (including supporting SSCs) that are designed to carry out identified functions should initially be assigned to the safety class corresponding to the safety category of the function to which they belong. In the approach recommended in this Safety Guide, three safety classes are proposed consistent with the three categories recommended in paragraph 3.15 of SSG-30 [1].

Factor a) represents an identification of the items that contribute to the fulfilment of a safety function. Items that are not contributing are considered as NC. However, the possible impact of these items in case of a failure needs to be considered. This is outlined in SSG-30 [1].

Paragraph 3.24 of SSG-30 [1]

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

This means that, items not contributing to the accomplishment of a safety function might be classified according to the consequence of their failure.

Factor c) reflects the frequency which the item will be called upon to perform a safety function. This frequency is expected to be in the same magnitude as the probability of the function to be called upon. Since the probability of occurrence of the initiating event is considered in the categorization of the functions, this factor is already implicitly considered.

The assignment of preliminary safety classes to the items that participate in the fulfilment of safety functions is summarized below.

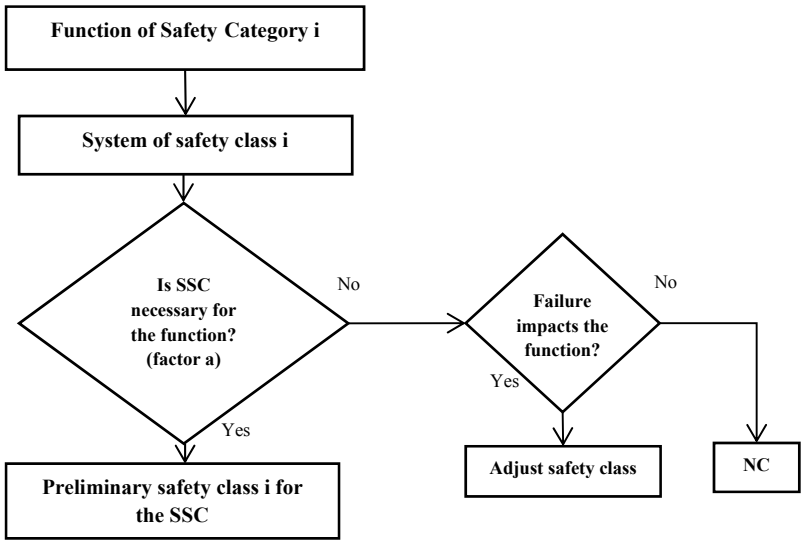

FIG. 2. Steps to determine the safety class of an SSC.

The preliminary safety classes could be adjusted taking factors b) and d) into consideration, as suggested in SSG-30 [1].

Paragraph 3.20 of SSG-30 [1]
The initial classification should then be amended as necessary to take into account factors b) and d) defined in paragraph 2.2. For factor d), consideration of the time following a postulated initiating event before the function is called upon may permit the SSC to be moved into a lower class, provided its expected reliability can be demonstrated. Such demonstration may use, for example, time to repair or maintain the SSC, or the possibility of using alternative SSCs within the time window available to perform the required safety function.
At that step of the classification process, factor b) reflects the consequences of a component failure with respect to the accomplishment of the categorized function. The preliminary

safety class of an item may be adjusted by one level if it can be demonstrated that a failure of this specific item would not jeopardize the accomplishment of the safety function. Factor b) however cannot be used to downgrade the safety class of redundant components implemented to meet the single failure criterion.

Factor d) reflects the time following a postulated initiating event at which, or the period for which, the item will be called upon to perform the function. The preliminary safety class of an item may be adjusted if it is demonstrated that the item is not needed early in the sequence after the initiating event.

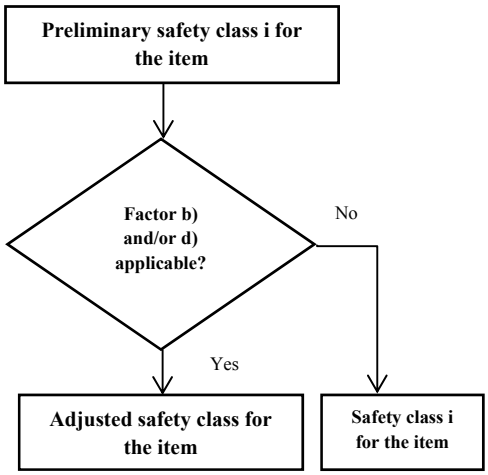

FIG. 3. Further steps to determine the safety class of an SSC.

E.g. factor b) may be used to adjust the safety class of small piping connected to the main components.

Last, as outlined in Section 3.21, SSCs that contributes to the performance of several functions of different categories should be assigned to the class corresponding to the highest of these categories (i.e. the one requiring the most conservative engineering design rules).

Components containing radioactive materials:
It is important to keep in mind that a component may have a confinement barrier role in addition to its functional role. The importance of the barrier role is reflected by assigning the SSC to a barrier safety class. This barrier safety class is determined by assessing the severity of the radiological consequences of the failure of the component within the NPP or off-site as explained in Section 2.7. Finally, the safety class assigned to the component considers the two roles. For those components, the more stringent safety class between the functional class and the barrier safety class should be selected. Practically, for determining the safety class, due account of the barrier role should be given for components assigned in a functional safety

class 2 or 3 (component with a functional safety class 1[2] is already assigned in the highest safety class).

The safety class of the electrical part of pressure retaining equipment corresponds to its functional safety class.

This whole process to establish a classification at the component level is indicated in Appendix.

Paragraph 2.17 of SSG-30 [1]
Based on the experience of Member States, in this Safety Guide three safety categories for functions and three safety classes for SSCs important to safety are recommended. Other approaches utilizing a larger or smaller number of categories and classes may be used provided that they are aligned with the guidance provided in paragraph 2.12 and 2.15 of SSG-30.
According to Member States practices, classification of some specific components, (e.g. electrical components, building and civil structures) is established with fewer safety classes.

Interfaces between components with different safety classes:
Recommendation to determine the safety class of the interface between components of different safety classes is provided in SSG-30 [1].

Paragraph 3.25 of SSG-30 [1]
Where the safety class of connecting or interacting SSCs is not the same (including cases where an SSC in a safety class is connected to an SSC that is not classified), interference between the SSCs should be 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.

As an example, connecting two pipes of different safety classes requires an appropriate interface to ensure that a failure occurring on the pipe with the lowest class does not cascade to the pipe with the highest safety class. For the isolation devices the following additional requirements apply:

- The isolation device(s) inherits the highest safety class of the two sections of the system which it separates;
- If the isolation device is redundant, the same requirements apply to the two isolation devices and to the piping in between.

Although the paragraph 3.25 of SSG-30 [1] applies to the interface between items of different safety classes, practically, this recommendation also applies where the two items are manufactured according to different code quality requirements. As an example, connecting two pipes of different quality groups requires an appropriate interface to ensure that a failure occurring on the pipe with the lowest quality group does not cascade to the pipe with the highest quality group (see Table 18).

---

[2]) The barrier safety class of components part of the reactor coolant pressure boundary should be safety class 1 (see Section 2.7)

2.6. DESIGN PROVISIONS

Paragraph 2.9 of SSG-30 [1]
Using this information, the functions and design provisions (see paragraph 3.9) required to fulfil the main safety functions are systematically identified for all plant states, including all modes of normal operation. An SSC implemented as a design provision should however be classified directly, because the significance of its postulated failure fully defines its safety class without any need for detailed analysis of the category of the associated safety function.

Paragraph 2.13 of SSG-30 [1]
Categorization of the functions provided by design provisions is not necessary because the safety significance of the SSC can be directly derived from the consequences of its failure. The SSCs implemented as design provisions can therefore be directly assigned to a safety class without the need for a further analysis of safety function categories.

While the term 'function' is generally easily understood and systems, structures and components designed to accomplish a specific function also are easily identifiable, the meaning of the term 'design provision' needs some clarification to be well understood.

For classification purposes, it is fundamental to recognize that plant equipment includes a number of components that contribute to safety without being explicitly designed to accomplish one of the three fundamental safety functions. As also relevant to safety, those components are expected to be safety classified to better stress their importance to safety. SSG-30 [1] provides guidelines to capture those components.

Table 15 provides helpful general consideration to understand what structures or components need to be captured as 'design provision' by comparison with SSCs considered as participating to a function.

TABLE 15. DIFFERENCE BETWEEN 'FUNCTION' AND 'DESIGN PROVISION'

Function	**Design Provision**
Generally accomplished by a safety functional group consisting of several SSCs (including supporting systems)	Generally linked to a single SSC or to a limited number of SSCs
Generally called upon during an event (i.e. the function is actuated after the occurrence of the event) Note: Some functions are also used in normal operation (e.g. control of main plant parameters).	Not called upon during an event but provides its inherent characteristics during all operational and accidental plant states (i.e. typically, the design provision is not actuated by an I&C signal).

Paragraph 3.8 of SSG-30 [1]
The safety of the plant is also dependent on the reliability of different types of features, some of which are designed specifically for use in normal operation. For the purpose of this Safety Guide, these SSCs are termed 'design provisions'. Such design provisions need to be identified and may be considered to be subject to the safety classification process, and hence will be designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained with sufficient quality to fulfil their intended role.

So when establishing the safety classification, all design provisions that participate in safety need to be considered.

Paragraph 3.9 of SSG-30 [1]
Practically, design provisions are largely design dependent but the following list can be used as a general guidance for different types of reactors:

- Design features that are designed to such a quality that their failure could be practically eliminated. For these design features, the plant design does not require an independent safety system to be available to mitigate the effects of their failure. Examples of these are the shells of reactor pressure vessels or steam generators. These design features can be readily identified by the unacceptable level of consequences that can be expected should they fail;
- Features that are designed to reduce the frequency of accidents. Examples of these are piping of high quality whose failure would result in a design basis accident;
- Passive design features that are designed to protect workers and the public from harmful effects of radiation in normal operation. Examples of these are shielding, civil structures and piping;
- Passive design features that are designed to protect components important to safety from being damaged by internal or external hazards. Examples of these are concrete walls between components that are built specifically for this purpose;
- Features that are designed to prevent a postulated initiating event from developing into a more serious sequence. Examples of these are anti-whipping devices and fixed points.

Design provisions are generally implemented to ensure that the goal desired for a function is achieved, or to achieve a safety goal on its own. Various types of components are included in the group ‘design provisions’:

- SSCs which might not be captured by the process of functional categorization and however which largely contribute to the safety, as for example:
  - Spent fuel storage racks contribute to the main safety function ‘Control of the reactivity’;
  - Reactor pressure vessel internals contribute to the main safety function ‘Heat removal’;
  - Shielding to protect workers against radiation contributes to the main safety function ‘Confinement of radioactive material, shielding against radiation’;
  - Fuel handling equipment;
- Mechanical components necessary for the normal operation of the plant without specific role in the mitigation of postulated accident conditions, which contain radioactive materials and may lead to radiological consequences in case of failure (leakage or rupture) of the component (e.g. components of waste treatment systems, or components of systems controlling release of effluents). Such components have clearly a role in the protection of the workers, the public and the environment against harmful effects of radiation; and therefore, are generally manufactured according to specifications and quality requirements giving confidence that the expected reliability of their integrity is achieved;
- Buildings and civil structures.

Buildings may be important to safety due to two different factors:

- They contribute directly to the confinement of radioactive materials;
- They house SSCs that perform safety functions and protect these SSCs against internal or external hazards.

As suggested by SSG-30 [1] item 3.9, classifying buildings and structures applying the 'design provision' methodology is appropriate taking into account that buildings and structures are passive design elements. This approach will take due account of the internal structures (and not only the external parts of the building), in order to fully address the risks imposed by hazards such as missiles, fire or flooding.

Buildings should be considered as consisting of three types of structures:

- Structures which contribute to the retention or confinement of radioactive releases;
- Structures which contribute to the building structural integrity;
- Structures, located inside the building, which do not contribute to the structural integrity of the building, but are designed for specific purposes (e.g. biological shielding, anti-missile barrier, removable concrete walls, platforms).

Note: in accident conditions, the integrity of confinement barriers and the limitation of the radiological releases may require the operability of some venting/filtering systems or HVAC systems. The safety class of these systems should preferably be determined according to the 'function approach'.

Table 16 provides examples showing that both functions and design provisions may be necessary to fulfill a same safety objective.

TABLE 16. EXAMPLES OF FUNCTIONS AND DESIGN PROVISIONS

	Examples for associated 'functions'	**Examples for associated 'design provisions'**
Protect workers against the harmful effects of radiation	Activity monitoring, ventilation systems for managing airborne radioactive material	Passive design features that are designed to protect workers and the public from harmful effects of radiation in normal operation. Examples of these are shielding, civil structures and piping
Avoid failure of 2nd barrier	Overpressure protection in the reactor coolant circuit	Piping of high quality whose failure would result in a design basis accident
Limit effects of internal/external hazards, e.g. fire	Fire extinguishing; fire containing by closure of fire dampers on demand of a fire detection system	Structural elements to separate fire compartments
Limit effects of internal/external hazards, e.g. internal flooding	Isolation of broken fluid system parts	Flooding pits or flaps in doors implemented to ensure dedicated water flow paths. Watertight doors to prevent flood spreading
Limit effects of internal/external hazards, e.g. airplane crash	Airplane crash: none	Structures and buildings designed to withstand the loads
Prevent a postulated a design basis accident (DBA) from developing into a more serious sequence	Emergency core cooling	Pipe whip restraints, fixed points.
Prevent heavy load drop	Motion limiting safety functions (implementing motion detectors, safety brakes)	Mechanical parts ensuring the structural integrity of lifting devices, such as bridge girders, trolleys, hooks, ropes

2.7. CLASSIFICATION OF STRUCTURES AND COMPONENTS ASSOCIATED WITH THE DESIGN PROVISIONS

Paragraph 3.23 of SSG-30 [1]
As explained in SSG-30 [1] paragraph 2.9, design provisions can be directly classified according to the severity of consequences of their failures:

- Safety class 1 - Any SSC whose failure would lead to consequences of 'high' severity;
- Safety class 2 - Any SSC whose failure would lead to consequences of 'medium' severity;
- Safety class 3 - Any SSC whose failure would lead to consequences of 'low' severity.

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

Generally, the safety class of a design provision can be directly derived from consequences in case of failure. Consequences can be radiological or be a degradation of the protection of the safety classified systems. The safety class can be established as follows:

- A passive design feature whose radiological consequences of the failure cannot be kept below the limits established by the regulatory body with reasonable means should be in safety class 1 (e.g. fuel storage racks);
- A passive design feature that is essential for keeping the design basis accident analyses presented in the safety analysis report bounding should be safety class 1 (e.g. anti-whipping devices for primary loops for PWR);
- Mechanical components not captured in Section 2.5 (SSCs performing a categorized function), which contain radioactive materials (e.g. components of waste treatment systems, or components of systems controlling release of effluents) and may lead to radiological consequences in case of failure (leakage or rupture). The safety class is determined by assessing the severity of the radiological consequences of the failure of the component within the NPP or off-site. Equipment whose failure could lead to radiological consequences exceeding the occupational dose limits established for the field operators should be at least safety class 3 or higher if the radiological consequences are more severe;
- Passive design features that are designed to protect workers and the public from harmful effects of radiation in normal operation should be safety class 3, provided that their failure leads to consequences of low severity (exceedance of accepted occupational dose limits for the plant staff);
- Design provisions to limit propagation of the effects of hazards (not already addressed in the building classification) whose failure could challenge the assumptions made in the hazard analysis should be assigned in safety class 3 at least in a deterministic way. If the direct consequence is a radiological release, the safety class should be determined on the basis of the severity of the radiological release.

Reactor Coolant Pressure Boundary:
Taking into account the importance for safety of the reactor coolant system in all plant states, and that the consequences of the failure of the reactor pressure vessel cannot be mitigated with feasible means, the reactor coolant pressure boundary (RCPB) is designed according to the highest standards. All components which are part of the RCPB are therefore considered for classification as one ‘design provision’ at safety class 1 for which the highest quality requirements apply.

As a good practice, the principle to apply the highest quality requirements should be extended to pipes whose double ended break (2A break) is not postulated as a design basis accident.

Building and civil work:
Safety related buildings and civil structures are for:

- Providing a protection of safety functions/systems/components against the effects of external or internal hazards;
- Providing a protection of workers against direct radiation;
- Providing a barrier to the release of radioactivity.

Basically buildings and civil works are considered as design provisions and therefore may be directly assigned to a safety class by assessing the severity of consequences of their failure. Nevertheless considering practices in many Member States, buildings and civil works are often divided in safety class 1 and non-classified (NC), with the following definition:

- Building or civil structure required for the accomplishment of one of these three purposes above are assigned to class 1[3];
- Building or civil structure housing system or equipment safety necessary for the mitigation of design basis accidents and design extension conditions are assigned to class 1;
- Others buildings or civil structures are assigned in class NC.

2.8. COMPLETENESS AND CORRECTNESS OF THE SSC CLASSIFICATION

Paragraph 3.27 of SSG-30 [1]
The adequacy of the safety classification should be verified by using deterministic safety analysis, which should be complemented by insights from probabilistic safety assessment and/or supported by engineering judgment.

Paragraph 3.28 of SSG-30 [1]
The contribution of the SSC to reduction in the overall plant risk is an important factor in the assignment of its safety class. Consistency between the deterministic and probabilistic approaches will provide confidence that the safety classification is correct. Generally, it is expected that probabilistic criteria for safety classification will match those derived deterministically. If there are differences, however, further assessment should be carried out in order to understand the reasons for these and a final safety class should be assigned, which should be supported by an appropriate justification.

Probabilistic insights can outline, or not, the contribution of equipment in the accomplishment of safety functions. In both cases there is a need to reconsider the safety class established on the basis of a deterministic approach. Indeed it may happen that the contribution of a component to safety has been over- or underestimated following the deterministic rules to be applied for design. Decision to change the safety class is generally made once the reason for a different appreciation of the role of the SSC is understood.

[3] Decision to assign building or structure in class 1 is informed by the severity of the consequences of the failure as indicated by Para. 3.23 of SSG-30 [1] and reminded in Section 2.7 of this TECDOC.

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

As required by IAEA Safety Standard SSR-2/1 Requirements 22 and 23 [3]:

All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance (SSR-2/1, Req. 22 [3]).

The reliability of items important to safety shall be commensurate with their safety significance (SSR-2/1, Req. 23 [3]).

Therefore, once the safety classes of the SSCs have been established, corresponding engineering design rules will have to be specified and applied. Engineering design rules are the relevant national or international codes, standards and proven engineering practices that are applied, as appropriate, to the design of SSCs to meet the overall objective that the most frequent postulated initiating events yield little or no adverse consequences, while more extreme events (those having the potential for the greatest consequences) have a very low probability of occurrence.

Depending on its safety significance, reflected by its safety class, each SSC is designed, manufactured and operated according to appropriate engineering rules defined to give confidence that its capability, reliability and robustness will be adequate.

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

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

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

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

> Design requirements applied at the system level may include specific requirements, such as single failure criteria, independence of redundancies, diversity and testability, but also general requirements for environmental, seismic and hazard qualification.
>
> Design requirements applied for individual structures and components precise the needs with regard to environmental and seismic qualification, and manufacturing quality assurance procedures. They are typically expressed by specifying the codes or standards that apply.

3.1. REQUIREMENTS APPLICABLE TO SYSTEM

Practically, capability and reliability of systems performing a categorized function is achieved by meeting design requirements relevant for the safety class of the system. Table 17 gives a set of typical generic design requirements for systems.

TABLE 17. EXAMPLES OF TYPICAL SAFETY REQUIREMENTS FOR SYSTEMS

System safety class	**Single failure criterion**	**Physical & electrical separation**	**Emergency power supply**	**Periodic tests**	**Protected against or designed to withstand hazard loads**	**Environmental qualification**
SC1	Yes	Yes	Yes	Yes	Yes	Yes
SC2 (1)	Yes (1)	Yes	Yes	Yes	Yes	Yes
SC2 (2)	Not required (3) (4)	Yes for redundant equipment	Yes	Yes	Yes	Yes
SC3 (5)	Not required (6)	Yes for redundant equipment	Yes	Yes	Yes	Yes
SC3 (7)	Not required	Not required	According to functional analysis	Yes (8)	According to functional analysis	According to functional analysis

(1): Systems necessary to reach and maintain a safe state. Reaching a safe state should be possible despite one single failure.

(2): Systems designed for design extension conditions as a backup of a system assigned to safety class 1. Independence from the safety class 1 system is necessary.

(3): System designed as a backup of a system assigned to safety class 1 already provides an alternate means to accomplish the same safety function as that performed by the safety class 1 system. Nevertheless, reliability of such system needs to be adequate to meet the total core damage frequency (CDF) target.

(4): Might be needed for I&C backup system to prevent spurious actuation (e.g. for the diverse actuation system).

(5): Systems designed to mitigate the consequences of design extension conditions but not assigned to safety class 2.

(6): Compliance with the single failure criterion is not required in design extension conditions. However redundant active components might be necessary to achieve the reliability expected for the function to be accomplished by the system (e.g. active components of systems required to preserve the containment integrity in case of a severe accident with core melt).

(7): Systems not required meeting the acceptance criteria established for design basis accidents or design extension conditions but that are in the group of systems important to safety according to the IAEA Safety Glossary. A common set of requirements to be

systematically applied cannot be established, but the relevant and specific requirements are generally defined on the basis of a functional analysis supplemented by probabilistic insights.

(8): Unless necessary for normal operation.
Redundant divisions of a single safety system need to be independent and separated from each other to prevent a failure in one redundancy from propagating to the non-affected redundancies, or the loss of all of the redundancies caused by a hazard. Independence and separation of systems belonging to different levels of defence are also fundamental design elements for achieving a high level of safety, and are therefore expected to be implemented adequately between the different levels of defence. However, independence of levels of defence is a complex issue taking into account that full independence is not practically feasible, and is therefore not addressed in this TECDOC.

Moreover, seismic requirements and environmental qualification are essential to ensure the integrity of buildings and structures or the operability of components if required in case of an earthquake or during accident conditions with harsh ambient conditions. General guidance to specify adequately the requirements is given in Sections 3.2.2 and 3.2.3 below.

Any system designed to mitigate the consequences of an accident is expected to be designed according to requirements ensuring its operability when challenged. Nevertheless, qualification requirements are defined at the individual component level taking into account the relevant environmental conditions at the component location and its mission time.

3.2. REQUIREMENTS APPLICABLE TO INDIVIDUAL STRUCTURES OR COMPONENTS

3.2.1. Generic Consideration

By assigning a safety class to every individual SSC, a set of design and manufacturing requirements needs to be established to meet the requested quality and reliability objectives.

Adequate and proven codes or standards need to be used for the design and manufacturing of the structures and components to ensure that they will be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected according to their safety significance. These industry codes and standards indicate the methodologies, rules and criteria to be used for procurement, design, construction, inspection and testing of components.

Generally, design/manufacturing requirements and codes to be used are defined for a type of equipment (civil structure, pressure retaining equipment, electrical or I&C equipment). For specific equipment, requirements may be directly defined in the equipment specification.

Moreover, QA programmes need to be applied at the different stages of component life (design, construction, installation, inspection, testing, operation, modification).

3.2.2. Seismic Requirements

Apart from the safety classification (which is the main part of purview of the SSG-30 [1]), it is also important to understand and factor in the requirements related to classification of SSCs

with respect to the importance of their integrity/performance/failure during a seismic event. This will help the users to bring out the detailed classification and comprehensive design requirements for SSCs from a holistic point of view.

As a basic principle, structures, systems and components of a nuclear power plant necessary to assure capability for shut down, decay heat removal and confinement of radioactive material need to be designed to remain functional throughout the plant life in the event of an earthquake. Moreover, to limit radiological releases in a design basis accident, safety systems are required to keep their operability during and after an earthquake. The same safety approach is also recommended by the IAEA SSR-2/1 [3] for systems designed to mitigate the consequences of a core melt accident.

The seismic categorization is expected be appropriate to capture all of the SSCs of the NPP and to assign a seismic category to each of them. Generally, categorization includes several seismic categories and one non-seismic category.

In the IAEA Safety Guide NS-G-1.6 [6], two levels of earthquakes (SL-1 level earthquake and SL-2 level earthquake) have been defined based on the severity of the ground motion. SL-2 is associated with the safe shutdown earthquake (SSE) and corresponds to the severity to be considered for licensing the plant. SL-1 corresponds to a less severe, more probable earthquake level that normally has different safety implications.

Independently of the seismic categorization implemented by Member States, requirements for the behavior of the building, structure and component during and after an earthquake should be clearly established and specified. Usually, the behavior is specified in terms of operability, functional capability, structural integrity and stability. Justification of the specified behavior is part of the seismic qualification and can be made by analytical analyses, tests or a mix of calculations and tests. Stress limits not to be exceeded for the different requirements are generally provided by the construction/manufacturing codes.

As an example, components that ensure a safety function needed to bring the plant to a safe state and maintain it during and after an earthquake are liable to ‘operability’ for the severest level of design basis earthquake (SL-2). Such case will encompass the mechanical and structural constituents including the associated and essential electrical and I&C components.

‘Functional capacity’ is generally adequate for passive mechanical components (e.g. piping), necessary to accomplish a function in case of earthquake.

‘Integrity’ is generally adequate for mechanical components assuring only a confinement role in case of earthquake (e.g. piping system/tanks/containment).

Components that do not perform a safety function but whose failure (if they were not robust against an earthquake) in a seismic event could prevent other safety components (either due to a cascading effect or due to its proximity) from completing their required safety function should meet seismic requirements commensurate with the implication. The seismic requirements to be applied to such cases can be ‘stability’ or ‘integrity’ depending on the type of potential hazard induced by the earthquake.

Loads and load combinations and associated stress limits to be met are not systematically part of seismic categorization but need to be defined on the basis of the accident category which the system is intended to operate, its role and its mission time.

In relation to the safety classification proposed by the Safety Guide SSG-30 [1], seismic requirements are expected to be established considering the following:

- Safety class 1 systems designed to mitigate consequences of design basis accident are expected to keep the operability in place in case of earthquake of level SL-2;
- Safety class 2 systems designed to reach and maintain safe state after design basis accident are expected to keep the operability in place in case of earthquake of level SL-2;
- The operability of safety class 2 systems designed as a backup of a safety class 1 system may not be needed, provided that an earthquake is not part of a combination of failures considered as a design extension condition for which the backup is designed;
- Safety class 3 systems designed to mitigate consequences of a severe accident are expected to keep the operability in place in case of earthquake of level SL-2;
- The spent fuel pool cooling systems are expected to keep the operability in place in case of earthquake of level SL-2;
- Buildings with a confinement function or housing safety classified SSCs are expected to keep the structural integrity in case of earthquake of level SL-2.

3.2.3. Environmental qualification

Identification of qualification requirements:
Qualification of equipment contributes to provide evidence that safety classified equipment is able to fulfill its required function(s) during accident conditions (design basis accidents or design extension conditions), despite the harsh environmental conditions (pressure, temperature, moisture, irradiation) prevailing prior to or at the time they are requested to operate. Specifications need to be defined taking into the following factors:

- The location of the item (environmental conditions are building dependent);
- The mission(s) of the item in accident conditions.

For example, the role or the mission of an isolation valve may be to be operable, or to be leak-tight, or simply that its status ‘open’ or ‘closed’ needs to be displayed to the operator.

The mission time of the item depends on whether it is needed only in the short term of the accident, or, on the contrary, whether it is necessary to reach and/or maintain a safe state

Bounding environmental conditions need to be determined in the different buildings to establish conservative profiles against which the items have to be qualified, taking due account of their mission and their mission time. Nevertheless, in order to prevent the qualification from becoming too complex for the industry, the practice is to limit the number of combinations of those factors in a reasonable number of categories.

In any case, sufficient margins have to be taken during the entire classification process, particularly for the mission times to be considered.

Note: the effects of ageing, such as the cumulative effects of the environmental conditions corresponding to normal operating conditions before the occurrence of the accident conditions, also have to be taken into account in the qualification of equipment.

Location:
The zones to be considered are those in which the environmental conditions may be harsh during an accident, and where components required to accomplish safety functions are located as for example:

- Reactor building;
- Auxiliary building;
- Fuel building (if relevant).

Severity of environmental conditions:
For a given zone, accidents to be considered to specify qualification requirements are:

- Accidents without harsh environmental conditions.

No qualification is necessary, but ability for a component to perform its function during its lifetime may need some justification. In particular, this justification must consider the ageing of the equipment in normal conditions (e.g. ageing irradiation):

- Accidents with harsh environmental conditions in pressure and temperature, but for which the irradiation is comparable to the ageing irradiation;
- Accidents with harsh environmental conditions including both significant irradiation and abnormal pressure and temperature;
- Accidents with significant irradiation, but normal pressure and temperature conditions.

Mission time:
The duration of the mission time may also be used as an additional factor to establish specifications for the qualification, taking into account that the mission time of a component can be short or long (e.g. some sensors are just necessary to initiate the reactor scram but components necessary for the containment cooling need to be operable in the long term). So not requesting qualification in the long term for all equipment may be acceptable provided the mission time is clearly indicated. The mission time is usually determined on the basis of a functional analysis.

3.2.4. Pressure Retaining Equipment

Well-established codes defining design and manufacturing requirements for pressure retaining equipment in nuclear power plants are available, as for example:

- American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code, Section III, Division 1, “Rules for Construction of Pressure Vessels” [4];

- French Association for Design, Construction and In-Service Inspection Rules for Nuclear Island Components (AFCEN), “Design and Conception Rules for Mechanical Components of PWR Nuclear Islands” (RCC-M) [5];

- Safety Standards of the German Nuclear Safety Standards Commission (KTA).

Note: The scope of application of a code should be restricted to the domain of equipment for which the code is established and practically applied (proven experience).

As usual the safety classification of pressure retaining components is established in compliance with the classification principles established by the national regulatory body. It is essential to supplement the classification with a clear relationship between the safety class and the set of requirements established by the code. On the basis of that relationship between safety class and code, the classification submitted by the applicant is accepted or disputed by the regulatory body.

.

TABLE 18. RELATIONSHIP BETWEEN SAFETY CLASS AND CODE REQUIREMENTS FOR PRESSURE RETAINING EQUIPMENT

Safety Class	Safety classified pressure retaining equipment items	Code requirement	Example of SSCs	Comments
SC1	• Safety class 1 design provisions whose failure, in normal operation, would directly lead to 'high' consequences	ASME Code, Section III, Division 1, Subsection NB RCC-M1	Reactor pressure vessel, steam generator outer shells, piping to which leak-before-break or break preclusion principles are applied	
	• Any pressure retaining component that cannot be isolated from the reactor coolant system by two isolation valves in series and whose failure would result in a non-compensable leakage by the normal water make-up system		RCPB piping > DN 25	Assigning the RCPB to the highest code requirements is not strictly required according to the SSG-30 [1] definition of 'high' consequences (the deterministic safety analysis for loss of coolant accidents [LOCA] should demonstrate that radiological consequences remain within acceptable limits) It is, however, common practice in many Member States to strengthen DID level 1 by choosing the highest quality requirements for the entire RCPB (except small-bore connecting lines)
	• Components providing Cat. 1 functions unless codes like ASME Level 1 or RCC-M1 are already applied based on the rule above	ASME Code, Section III, Division 1, Subsection NC or ND RCC-M2 or RCC-M3 (depending on their safety barrier class)	Emergency core cooling system, containment isolation system, reactor shutdown system	ASME ND or RCC-M3 is acceptable for components that: • are subject to small service loads (moderate operating pressure and temperature) • do not contain high radioactive fluids, even in accident conditions Examples: Service water pump system, auxiliary feedwater system portions isolated from steam generator pressure and temperature

SC2	• Safety class 2 design provisions whose failure, in normal operation, would directly lead to 'medium' consequences • Any parts of the RCPB whose failure would result in leakage that is compensable by the normal water make-up system • Components providing Cat. 3 functions with a safety barrier class 2	ASME Code, Section III, Division 1, Subsection NC RCC-M2	Residual heat removal system Non-isolable primary piping < DN25	The residual heat removal system performs a Cat. 2 function but recirculates primary water in normal shutdown operation and provides therefore also an important barrier role ('medium' consequences in case of pipe failure)
	• Components providing Cat. 2 functions	ASME Code, Section III, Division 1, Subsection ND RCC-M3	Spent fuel pool cooling system	
SC3	• Safety class 3 design provisions whose failure, in normal operation, would directly lead to 'low' consequences • Components providing Cat. 3 functions with a safety barrier class 3	ASME Code, Section III, Division 1, Subsection ND RCC-M3	Systems containing radioactive fluids in normal operation, e.g. chemical volume and control system, waste processing systems	
	• Components providing Cat. 3 functions unless specific codes and requirements are applied for specific reasons	Conventional codes like: • European Pressure Directive 97/23/EC • ASME Code, Section VIII, Division 1 for pressure vessels • ANSI B31.1 for piping	Systems providing make-up to feedwater tanks in postulated design extension conditions	Systems providing functions for severe accident management should be subject to specific requirements reflecting the role and the environmental conditions of the components in postulated severe accident scenarios. Guidance from codes like ASME or RCC-M are expected to be taken where appropriate. As an example, ASME Level 2 or RCC-M2 may be applied for pressure retaining parts, confining radioactive materials in case of a severe accident.

3.2.5. Supports

Design and manufacturing requirements of supports are determined on the principle that support is as important as the component being supported. Requirements for the support are indicated by the code used for the supported component. Examples:

- Supports for RCC-M1 components: the requirements of the dedicated RCC-M subsection are applied (Volume H, requirements for S1 supports);
- Supports for RCC-M2 components: the requirements of the dedicated RCC-M subsection are applied (Volume H, requirements for S2 supports).

ASME III Division 1, Section III, subsection NF should be used when ASME code is applied.

The supports of other electrical equipment (cables, connections, electrical cabinets, etc.) are handled in the code that is relevant for electrical components (e.g. IEEE or RCC-E).

The design rules for supports or support components which are embedded in concrete are handled in the code that is relevant for the civil works.

3.2.6. Electrical Systems

Electrical equipment includes various types of equipment like AC and DC power sources, transformers, switchgears, electrical distribution systems and protection devices.

Those components are classified as explained in Section 2.5 and Appendix considering the functional safety class only.

Examples of the correspondence between the safety class of electrical equipment items and codes are provided in the Table 19:

TABLE 19. RELATIONSHIP BETWEEN SAFETY CLASS AND CODE REQUIREMENTS FOR ELECTRICAL EQUIPMENT

Safety class	Safety classified electrical equipment items	Code requirement	Example of SSCs	Comments
SC1	• Electrical equipment supporting Cat. 1 or functions	IEEE: 1E RCC-E: C1	On site AC power supply system, uninterruptible DC power supply system	
SC2	• Electrical equipment supporting Cat. 2 functions in DBAs		Electric drives supporting Cat. 2 functions	
	• Electrical equipment supporting Cat. 2 functions implemented as a backup for a Cat. 1 function	RCC-E: C1 IEEE: Specific requirements	Electric drives supporting backup of Cat. 2 functions	The IEEE codes do not stipulate explicit requirements for equipment used in design extension conditions without core melt. Additional specific requirements are typically defined.
SC3	• Electrical equipment supporting Cat. 3 functions	IEEE: non 1E RCC-E: C3 + specific requirements	Alternate AC power sources Uninterruptable power supply system for severe accidents Electric drives supporting Cat. 3 functions	Equipment used in severe accidents is expected to be qualified for the harsh environmental conditions resulting from severe accidents.

3.2.7. I&C Equipment

I&C equipment includes the different I&C systems for the operation of the plant in normal operation and the control of the plant in the different plant states, including the monitoring of the plant parameters for normal operation and accident conditions.

Those components are classified as explained in Section 2.5 and Appendix 1 considering the functional safety class only.

The engineering requirements to be applied to I&C systems and components are usually defined in the relevant I&C industry standards (e.g. IEC Standards or IEEE code).
Both IAEA SSG-30 [1] and IEC 61226 aim at meeting the overall classification requirements given in IAEA SSR-2/1 [3] (IAEA SSG-30 [1]). Categories and classes from IC SSG-30 [1] fit together as follows:

IAEA Category 1 (-> safety class 1)	-->	IEC Category A (-> class 1)
IAEA Category 2 (-> safety class 2)	-->	IEC Category B (-> class 2)
IAEA Category 3 (-> safety class 3)	-->	IEC Category C (-> class 3)

APPENDIX

Process to establish classification of items important to safety

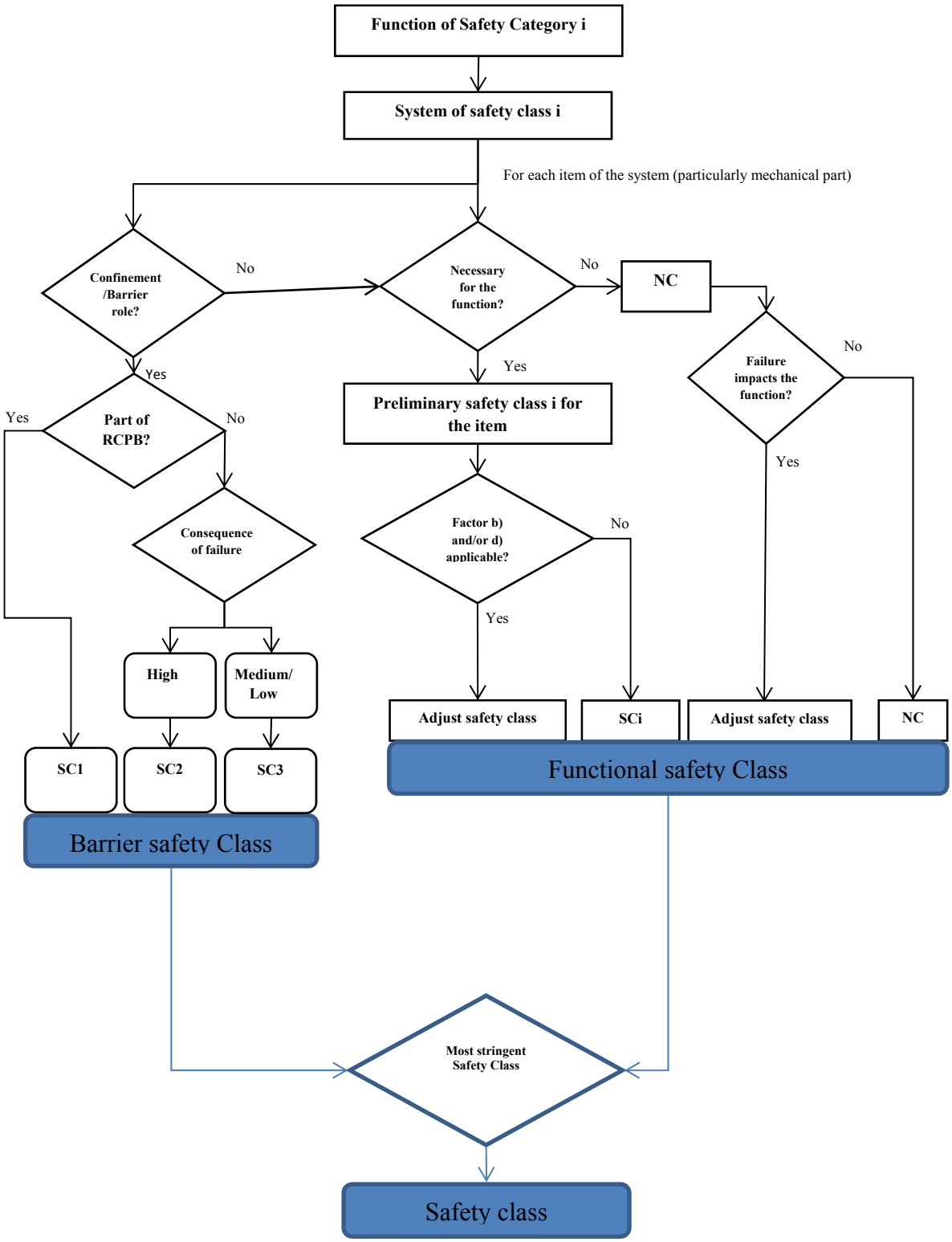

FIG. 4. Classification of SSCs (once the categorization of functions is complete).

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear power plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[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, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev.1), IAEA, Vienna (2016)

[4] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, ASME Boiler and Pressure Vessel Code, Section III, Division 1, Rules for Construction of Pressure Vessels, ASME, New York, NY (2013).

[5] ASSOCIATION FRANÇAISE POUR LES REGLES DE CONCEPTION, DE CONSTRUCTION ET DE SURVEILLANCE EN EXPLOITATION DES MATERIELS DES CHAUDIÈRES ELECTRO-NUCLEAIRES: Design, Construction and In-Service Inspection Rules for Nuclear Island Components Design and Conception Rules for Mechanical Components of PWR Nuclear Islands (RCC-M), Paris (2012).

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

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants, Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2, IAEA, Vienna (2011)

ABBREVIATIONS

AC	Alternating current
AOO	Anticipated operational occurrence
ASME	American Society of Mechanical Engineers
ATWS	Anticipated transient without scram
CCF	Common cause failure
DBA	Design basis accident
DC	Direct current
DEC	Design extension condition
DID	Defence in depth
ECCS	Emergency core cooling system
HVAC	Heating, ventilation and air conditioning
I&C	Instrumentation and control
LOCA	Loss of coolant accident
LOOP	Loss of off-site power
NPP	Nuclear power plant
PIE	Postulated initiating event
PSA	Probabilistic safety assessment
PWR	Pressurized water reactor
QA	Quality assurance
RCPB	Reactor coolant pressure boundary
RCS	Reactor coolant system
SBO	Station blackout
SSCs	Structures, systems and components
SG	Steam generator
TECDOC	Technical document

CONTRIBUTORS TO DRAFTING AND REVIEW

Cabane, F.	Électricité de France, (EDF), France
Claes, A.	Vattenfall AB, Sweden
Klapp, U.	Areva, Germany
Kumar, N.	Nuclear Power Corporation of India, Ltd (NPCIL), India
Podlesnykh, A.	JSC "Rosatom Overseas", Russian Federation
Poulat, B.	International Atomic Energy Agency
Shang, C.Z.	China Nuclear Power Design Co., Ltd, China
Si, H.Y.	China Nuclear Power Design Co., Ltd, China
Toth, C.	Hungarian Power Companies LTD, Hungary
Yabda, I.	Tractebel Engineering (GDF Suez), Belgium

Consultants' Meetings

Vienna, Austria: 7–10 April 2014; 16–20 June 2014; 3–6 November 2014

IAEA
International Atomic Energy Agency

No. 24

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

BELGIUM
Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC
Suweco CZ, s.r.o.
SESTUPNÁ 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FRANCE
Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 43 43 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY
Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY
Librotrade Ltd., Book Import
Pesti ut 237. 1173 Budapest, HUNGARY
Telephone: +36 1 254-0-269 • Fax: +36 1 254-0-274
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

INDIA
Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://www.bookwellindia.com

ITALY
Libreria Scientifica "AEIOU"
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: http://www.libreriaaeiou.eu

JAPAN
Maruzen-Yushodo Co., Ltd.
10-10, Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: http://maruzen.co.jp

RUSSIAN FEDERATION
Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: http://www.secnrs.ru

UNITED STATES OF AMERICA
Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders for both priced and unpriced publications may be addressed directly to:

IAEA Publishing Section, Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

International Atomic Energy Agency
Vienna
ISBN 978–92–0–101116–9
ISSN 1011–4289