WORLD NUCLEAR ASSOCIATION

Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties

2020 revision

Title: Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties
Produced by: World Nuclear Association
Published: March 2020
Report No. 2020/001

© 2020 World Nuclear Association.
Registered in England and Wales,
company number 01215741

This report reflects the views of industry experts but does not necessarily represent those of any of the World Nuclear Association's individual member organizations.

Foreword

In January 2007 the World Nuclear Association established the Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group with the aim of stimulating a dialogue between the nuclear industry (including reactor vendors, operators and utilities) and nuclear regulators on the benefits and means of achieving a worldwide convergence of reactor safety standards for reactor designs.

The Digital Instrumentation & Control Task Force (DICTF) of CORDEL was set up in 2013 to investigate key issues in digital I&C related to the licensing of new and operating nuclear power plants, and to collaborate with the International Electrotechnical Commission (IEC) and the OECD Multinational Design Evaluation Programme (MDEP) Digital Instrumentation and Control Working Group (DICWG)[1].

On the basis of an internal survey and subsequent discussions, the CORDEL DICTF identified the following main issues:

- Safety classification for I&C systems in nuclear power plants.
- Defence-in-depth and diversity (DiD&D)[2].
- Modernization of I&C systems
- Cyber-security

The task force is also considering working on topics such as FPGA and I&C for SMRs in the future. These directions of work are presented in more detail in *CORDEL DICTF 2014-2016 Outlook* [16] and the CORDEL Strategic Plan for 2019-2023 [19].

This first report on *Safety Classification for I&C in Nuclear Power Plants* describes the current status in classification of I&C systems, identifies key causes for difficulties as well as potential solutions. It is important to note that safety classification of systems and components is a multidisciplinary issue, and this document aims to be used as a basis for exchange between those disciplines.

The initial edition of this report on *Safety Classification for I&C Systems in Nuclear Power Plants* was published in September 2015. This 2020 revision takes into account feedback provided by international organizations including the MDEP DICWG. Interaction between the World Nuclear Association working groups and task forces and other intergovernmental and regulatory bodies is a key element to support the CORDEL goal of harmonization and standardization.

The World Nuclear Association would like to acknowledge the central role of Johannes Pickelmann (Framatome, DICTF Chair), Gary Johnson (DICTF Consultant), Mark Burzynski (SunPort) and Warren Odess-Gillett (Westinghouse) in drafting this report and to thank all the CORDEL DICTF members for supporting the activities of the Task Force.

[1] The activities of MDEP's Digital I&C Working Group (DICWG) were transferred to the Working Group on Digital I&C (WGDIC) of the NEA's Committee on Nuclear Regulatory Activities (CNRA) in 2017.

[2] Originally referred to as: diversity and common cause failure (CCF)

Contents

List of Abbreviations and Acronyms

CNRA	Committee on Nuclear Regulatory Activities (OECD-NEA)
DAS	Diverse actuation system
DBA	Design basis accidents
DBE	Design basis event
DEC	Design extension criteria
DICTF	Digital Instrumentation & Control Task Force
DICWG	Digital Instrumentation and Control Working Group
DiD	Defence in depth
DiD&D	Defence in depth and diversity
EUR	European Utility Requirements for LWR Nuclear Power Plants
FSE	Functions, systems and equipment
HMI	Human machine interface
HVAC	Heating ventilation and air conditioning
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INSAG	International Nuclear Safety Group
MDEP	Multinational Design Evaluation Programme (NEA)
MPP	Main plant parameter
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission
PIE	Postulated initiating event
SDO	Standards development organization
SSCs	Structures, systems and components
STUK	Radiation and Nuclear Safety Authority (Finland)
WENRA	Western European Nuclear Regulators Association
WG	Working group
WGDIC	Working Group Digital I&C (OECD-NEA CNRA)
WNA	World Nuclear Association
YVL	Regulatory guides on nuclear safety (Finland)

Definitions

Unless otherwise stated, terminology used is defined according to the IAEA Safety Glossary [7].

Executive Summary

Classification of structures, systems and components (SSCs) according to their safety significance acts as part of the defence-in-depth approach as an essential task in the overall life-cycle of a nuclear power plant. The classification of SSCs specifies their importance to safety, according to the consequences of their failure to perform when required.

The approach for safety classification of instrumentation and control (I&C) systems has been reorganized following the release of the standards IEC 61226 and IAEA SSG-30 in recent years.

The approach for safety classification of instrumentation and control (I&C) systems has evolved in recent years following the release of the standards IEC 61226 and IAEA SSG-30 [2]. Whereas previously, safety classification of an item reflected its importance to safety, nowadays it is derived from the categorization of the safety significance of the process or function carried out by that item. As it can be used by various functions, the classification of a safety I&C system[3] is derived from the highest category of the I&C function to be realized.

The nuclear industry takes a graded approach to safety, meaning that systems with a higher importance to safety should be of demonstrably higher quality, more tolerant of failures, and more resistant to internal and external hazards, than systems with a lower importance to safety. Thus, the safety class of an I&C system and/or its assigned defence-in-depth (DiD) level have a direct impact on the requirements on qualification, quality assurance, independence (through separation and diversity), fault tolerance, system architecture and the extent of engineering documentation.

To achieve a proper safety categorization of I&C functions, it is necessary that the process and safety engineer from the vendor, operator and regulatory authority have a common understanding of the criteria for placing I&C functions into the various safety categories. Amending the categorization of I&C functions at a late stage in the design process presents significant challenges for the project execution if it changes the classification of the system.

This report provides an overview of the generic approach to I&C safety classification (Section 2), the main international standards and guidelines published by the IEC and IAEA (Sections 2.1.2 and 2.2) and a comparison of I&C classification approaches (Section 2.3). The purpose is to identify topics that create difficulty for CORDEL members when developing and applying safety classification for I&C systems in nuclear power plants (Section 3), and to describe the apparent cause of these difficulties.

The relation between plant states and postulated initiating events to safety classification of I&C systems is described in Annex 1.

[3] Following IEC 61513 [10], an I&C system *"encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices."*

1 Introduction

1.1 Background

The need for classification of equipment in nuclear power plants has been recognized since the early days of reactor design and operation (see IAEA SSG-30 [2]). This need has been addressed by IAEA SSR 2/1 requesting that: *"All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance."* (IAEA SSR-2/1 – Requirement 22: Safety classification [1]). Safety classification implies categorization of function and classification of SSCs (systems, structures and components).

Safety categorization is the process of identifying functions important to safety of a nuclear power plant according to their safety significance[4].

Safety classification is the process of assigning a safety class to systems, structures or components according the highest category of function(s) to be realized. Classification of SSCs determines the design, manufacturing and qualification criteria required to ensure that their reliability is commensurate with the safety significance of the functions they perform.

The various national nuclear regulators, standards development organizations (SDOs), and nuclear power plant suppliers aim to ensure that nuclear power plants pose minimal risk to public safety. Safety classification is one of the fundamental safety concepts used to achieve this goal. There are, however, many different ways of implementing safety classification schemes, which results in different criteria being applied to the design and manufacture of SSCs. The different expectations of the various regulators, SDOs, and suppliers has led to additional expense during the development of nuclear power plants, particularly when a plant design that has been accepted in one country is licensed in another country.

1.2 Objective

The objective of this report is to identify and describe the challenging areas with respect to safety classification of I&C systems from CORDEL members' perspective. The Digital Instrumentation & Control Task Force (DICTF) of the World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group is carrying out a number of activities related to safety classification of I&C systems in order to:

- Improve international standards dealing with safety classification of I&C functions, systems, and equipment.Harmonize terms and definitions concerning safety classification of I&C functions, systems and equipment.
- Inform the Working Group on Digital Instrumentation and Control (WGDIC) of the Nuclear Energy Agency's Committee on Nuclear Regulatory Activities (CNRA) about areas where achieving a regulatory consensus on I&C safety classification issues could reduce unnecessary regulatory burdens.
- Ensure that ongoing IAEA work in the area of safety classification takes due account of issues specific to I&C.
- Develop background information to promote harmonization of industry approaches to safety classification for I&C functions, systems and equipment.
- Provide the latest information and practices concerning safety classification.

[4] Parameter for "safety significance" implies criteria's regarding:

- Severity of consequences if the functions is not performed, and
- Plant state (control state / safe state) to be reached by the function.

1.3 From process design to I&C design

The conceptual design of a project begins with safety and process engineers defining the process, safety features, as well as general layout of the installation. The overall plant design is subsequently realized by the individual engineering disciplines: mechanical, electrical, civil and I&C. The interaction between all engineering disciplines is important throughout the engineering life-cycle of a project to ensure comprehensive consideration of the requirements. The relationship between I&C and functional requirements, developed from the basic design, is described in Annex B of IEC 61513 [10].

I&C systems control a plant's mechanical systems. Rules implemented in I&C, when combined with the mechanical systems they control, result in safety functions that cannot be achieved by either the mechanical system or the I&C system alone. In addition, the I&C system must provide operators with information about the status and performance of mechanical and nuclear functions and components. As a consequence of these two features there is not always a direct link between the I&C function and the classification of the supported system.

Reactivity control using control rods in a typical pressurized water reactor is one example. The mechanical designers provide control rods that have two modes of operation: a normal mode which can either withdraw or insert rods and in which the speed of movement is limited by the rate at which the rod drive motor can move; and an 'emergency' mode which cannot withdraw rods but can release them from the drive system so that they drop by gravity to shut down the reactor. The mechanical system is classified as a safety system because if the rods move in any other way than that commanded by the control system, a reactivity accident might occur.

The reactor designers require that the control rod and I&C systems act together to provide a capability to:

- Withdraw and insert the control rods by operator command during normal operation.
- Withdraw and insert control rods under automatic control during normal operation.
- Automatically release the control rods if conditions requiring reactor shutdown occur.
- Automatically release the control rods using diverse means if conditions requiring reactor shutdown occur.
- Release the control rods by manual command of the operator.

Each of these functions has a different degree of safety significance and potential to fail. One I&C system could perform all of these functions, but to provide for defence-in-depth, the functions are allocated among several I&C systems.

The process for identifying and organizing the I&C system to achieve the necessary mechanical and information system functions in a way that provides for economical design, reliable operation, and defence against common cause failure is called the 'I&C architectural design'. Such a process must be applied to every plant function that is controlled by the overall I&C system. Safety classification of I&C systems and components results from consideration of the combined mechanical functions, reactor control functions, and I&C system architectural design.

According to IEC 61513, the design of the I&C architecture shall divide the entire I&C into sufficient systems and equipment to meet the requirements on:

- Independence of the functions in different lines of defence.
- Adequate separation of the systems of different classes.
- Fulfilment of the constraints on the physical separation and electrical isolation arising from the environmental and layout constraints, hazard analysis, and constraints from start-up activities, testing, maintenance and operation.

The elaboration of the I&C architecture and the design of individual I&C systems within this architecture will result in identification and categorization of additional I&C-specific functions and classification of associated systems and equipment.

These requirements are based on the need for the I&C to provide appropriate operation of mechanical components in all operational plant states and accident conditions.

Annex 1 describes the different plant states. Alongside the different plant states the sequence of events is of importance.

2 Generic Approach for I&C Safety Classification

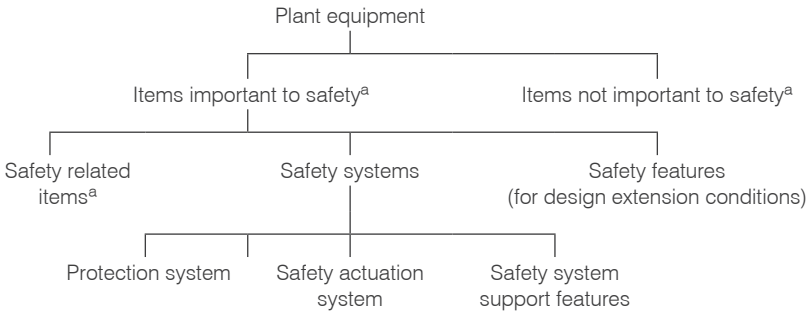
2.1 IAEA Safety Standards

2.1.1 IAEA SSR-2/1 - Safety of Nuclear Power Plants: Design

Requirement 22 of International Atomic Energy Agency (IAEA) Specific Safety Requirements No. SSR-2/1 states:

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

According to the IAEA Safety Glossary [7], I&C systems are divided broadly into two classes: those performing functions that are important to safety and those performing functions that are not important to safety (see Figure 1). An item important to safety is "an item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public."



[a] In this context, an 'item' is a structure, system or component

Figure 1. Generic identification of plant equipment (IAEA Safety Glossary)

I&C systems important to safety are identified based on their I&C safety functions and the definition of systems that perform certain combinations of these functions. The systems important to safety are based on the following fundamental safety functions that are required for all plant states (SSR-2/1 – requirement 4):

- Control of reactivity.
- Removal of heat from the reactor and from the fuel store.
- Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

Within the class 'I&C systems important to safety', there are two main subdivisions:

- **I&C safety systems**. Systems provided to ensure the safe shutdown of the reactor or residual heat removal, or to limit the consequences of anticipated operational occurrences and design basis accidents. Examples of safety systems include reactor trip systems, engineered safety actuation systems and safety system support features such as power supply and HVAC.
- **Safety-related I&C systems**. I&C systems important to safety that are not safety systems. Examples of safety-related I&C systems include: the reactor control and limitation system, the human-machine interface (HMI) panel,

and radiation monitoring systems. (Where the radiation monitoring system provides an input to the safety system it would be safety classified.)

This allocation specifies the baseline for the classification of the safety I&C functions.

IAEA SSR-2/1 [1] also specifies the following main safety classification criteria:

5.34. The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:

a. *The safety function(s) to be performed by the item;*
b. *The consequences of failure to perform a safety function;*
c. *The frequency with which the item will be called upon to perform a safety function;*
d. *The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.*

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

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

Depending on the nation, different codes and standards describe different means for classifying I&C systems and for establishing requirements for functions, systems, equipment, and quality of I&C. At the top level of international standards, the IAEA safety standards reflect an international consensus on what constitutes a high level of safety for protecting people and the environment from harmful effects of ionizing radiation. The IEC takes these standards as reference requirements and recommendations. IAEA SSG-30 [2] and IEC 61226 [11] establish the generic criteria and methods to be used to assign the I&C functions of a nuclear power plant to safety categories.

For the CORDEL Digital I&C Task Force (DICTF), the focus is on the international standards which are described in Sections 2.1.2 and 2.2. The IEC TR 61838 technical report (see Section 2.2.3) proposes methods for using probabilistic risk assessment to support the safety classification process.

It should be noted that – in accordance with IEC 61226 [11] – IEC 61513 [10] distinguishes between the categorization of I&C functions and the classification of I&C systems. IEC 61513 states: "The terms 'categorization' and 'classification' are sometimes synonymously used, even in IEC 61226. For the purpose of clarity in this standard, the term 'categorization' is reserved for the functions and the term 'classification' for the systems."

For discussions that apply to both classification and categorization, the term 'safety classification' represents both.

2.1.2 IAEA SSG-30 - Safety Classification of Structures, Systems and Components in Nuclear Power Plants

IAEA SSG-30 [2] provides recommendations on how to meet the SSR 2/1 safety classification requirements described above. The general approach is to provide a structure and method for identifying and classifying structures, systems, and components (SSCs) important to safety on the basis of their functions and safety significance. According to IAEA SSG-30, safety classification identifies and classifies those SSCs that are needed to protect people and the environment from harmful effects of ionizing radiation, based on their roles in preventing accidents, or limiting the radiological consequences of accidents. The scope is not limited to I&C.

SSG-30 specifies the top-down process for safety classification including the link to the safety design basis. The process distinguishes between the identification of functions necessary to fulfil the main safety objectives in all plant states and the identification of the design provisions necessary to prevent accidents.

Based on the main criteria defined by SSR-2/1, IAEA SSG-30 identifies three different SSC safety classes (1, 2 and 3) and describes generically the rules for classification.

2.1.3 IAEA TECDOC-1787 - Application of the Safety Classification of Systems, Structures and Components in Nuclear Power Plants

IAEA TECDOC-1787 [4] *aims at explaining how to complete the tasks attached to every step of the flow chart given in SSG-30 (…) 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 section 4 "Selection of applicable engineering design rules" which is a fundamental outcome of any classification.

To make certain that the classification of SSCs is established in a consistent manner, TECDOC-1787 emphasises the need to first identify all the safety functions required for each of the plant states. Examples of design and manufacturing requirements associated with the different safety classes to reach the expected levels of reliability and quality are also provided.

TECDOC-1787 provides information for organizations establishing a comprehensive safety classification of SSCs compliant with IAEA recommendations, and supports regulators in reviewing safety classification submitted by licensees.

2.2 IEC standards

2.2.1 IEC 61226 – I&C Important to safety - classification of the I&C functions

IEC 61226 [11] is an international standard that responds to IAEA SSR-2/1 [1] Requirement 22 on safety classification,[5] and approach of IAEA SSG-30.

This standard extends the classification strategy presented in IAEA SSR-2/1, and establishes the criteria and methods, recently updated on the base of IAEA SSG-30, to be used to assign the I&C functions of a nuclear plant to one of three categories, A, B and C, depending on their importance to safety, or to an unclassified category for functions with no direct safety role. The aim of this standard is to:

- Categorize the I&C functions important to safety, depending on their contribution to the prevention and mitigation of postulated initiating events (PIE), and to develop requirements that are consistent with the importance to safety of each of these categories.

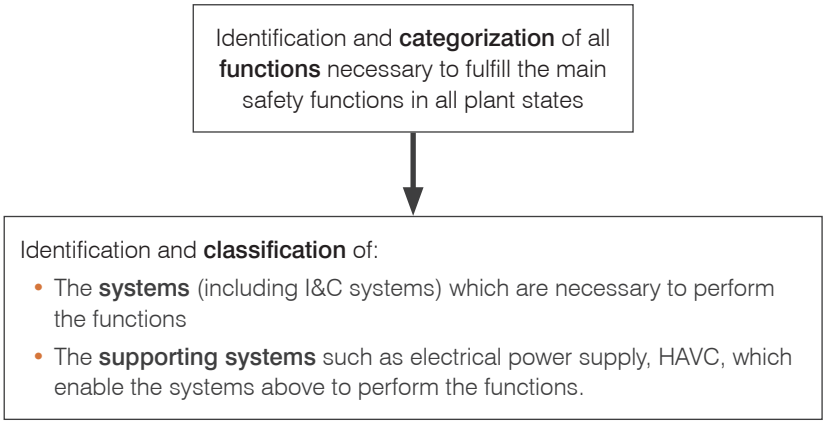


Figure 2. Overall classification scheme of SSCs (IEC 61226 Ed.4.0)

- Classify the I&C SSCs according to the highest category of I&C functions to be performed by each I&C system under consideration of factors (b) and (d) in Section 5.34 of SSR 2/1 for refinement of classification (see Section 2.1.1).
- Assign specification and design requirements to I&C systems and equipment that perform the categorized functions.

IEC standards are also being adopted as harmonized standards by other certifying bodies, thus IEC standards are becoming more important than in the past. Nevertheless, depending on the region, national standards are still in place and in most cases the responsible authority will keep its existing codes and standards, which the vendor has to consider in the specific project life-cycle.

The Edition 4 of IEC 61226 explicitly indicates the "2 phase process" as shown in Figure 2. The new revision follows the general principles given in IAEA safety requirement SSR-2/1 and safety guides SSG-30, SSG-34 and SSG-39.

Note: Working group 6.2 of IEEE Nuclear Power Engineering Committee (NPEC) Subcommittee 6 (SC-6, Safety Related Systems) reviewed and finalized in 2018 a project authorization request for a finer grading of safety classes than 1E and non-1E. During that meeting, IEEE WG 6.2 decided to consider the IEC 61226 concept. For Ed. 4, the IEC declined to have dual logo international standard with the IEEE but joint approach might be considered for Edition 5 of IEC 61226. In the meantime WG 6.2 decided to write a technical paper on the possible application of the IEC 61226 categorization and classification scheme to the US operating nuclear plant fleet.

[5] previously IAEA NS-R-1 5.1

Table 1. Correlation between classes of I&C systems and categories of I&C functions (IEC 61513 [10])

Categories of I&C functions important to safety			Corresponding classes of I&C systems important to safety
A	(B)	(C)	1
	B	(C)	2
		C	3

2.2.2 IEC 61513

IEC 61513 [10] introduces the concept of a safety life-cycle for the overall I&C architecture and a safety life-cycle for the individual systems. Section 5.4.2 of IEC 61513 (Design of the I&C architecture) specifies the correlation between classes of I&C systems and categories of I&C functions (see Table 1).

Annex B of IEC 61513 includes informative data on *Categorization of functions and classification of systems*. The current version identifies differences between the IAEA and IEC which are now obsolete due to the release of IAEA SSG-30. Annex B of IEC 61513 also includes a comprehensive explanation of the relationship between I&C functions and I&C systems, the scope of the nuclear plant process design phase and I&C design phase regarding safety classification.

2.2.3 IEC TR 61838 – I&C Important to Safety - Use of PSA for Classification of Functions

The IEC 61838 [14] technical report[6], *Use of Probabilistic Safety Assessment for the Classification of Functions*, provides a survey of some of the methods by which probabilistic risk assessment results can be used to establish 'risk-based' classification criteria, so as to allow functions, systems and equipment (FSEs) to be placed within the four categories established within IEC 61226.

The safety principles and the usefulness of a risk-based approach to classification are discussed and a description of four different approaches is presented. Two of these approaches are applied to a practical example and the results compared as a means to evaluate the robustness and generality of the risk-based approach.

2.3 Comparison of I&C classification

Table 2 shows the different safety classification schemes used by the main international standards organizations and selected countries having nuclear power programs.[7]

[6] IEC technical reports are not standards.

[7] Such a table gives only a qualitative mapping between the various classification systems.

[8] In this context, an „item" is a structure, system or component

[9] IEEE/NRC does not have a name for items that are important to safety, but not classified as 'safety-related' – Note: IEEE intends to follow IAEA SSG-30 / IEC 61226 (see Note 2 in chapter 2.2.1)

[10] EUR Revision E (December 2016) is revised to follow the SSG-30 principles.

[11] South Africa: Normally safety classification of the country of SSC supplier is adopted.

[12] In the IEEE/US, 'safety-related' designates the highest safety classification. In contrast, IAEA uses 'safety-related' to designate items of a lower importance than 'safety'

Table 2. System safety classifications

Organizations or Countries		Safety Classification of I&C Functions and systems in nuclear plants			
Main international standard organizations					
IAEA Safety Glossary		Items important to safety[8]			Items not important to safety[7]
		Safety systems	Safety-related items[7]		
				Safety features (for DEC)	
IAEA SSG-30	Function	Safety category 1	Safety category 2	Safety category 3	
	System	Safety class 1	Safety class 2	Safety class 3	
IEC 61226		Systems Important to Safety			Systems not Important to Safety
	I&C function	Category A	Category B	Category C	Non-categorized
	I&C system	Class 1	Class 2	Class 3	Non-classified
IEEE		Systems Important to Safety			Non-safety-related
		Safety-related		[9]	
EUR[10]	Safety level of functions / I&C systems	1	2	3	NS (non-safety)
Selected states with nuclear power programs					
Canada		Category 1	Category 2	Category 3	Category 4
China		F1A	F1B	F2	Non-classified
Finland		Class 2	Class 3	EYT/ STUK	EYT (classified non-nuclear)
France		Class 1	Class 2	Class 3	Non-classified
Germany	I&C function	Category 1	Category 2	Category 3	Non-classified
	I&C equipment	E1		E2	
India		IA	IB	IC	NINS
Japan		PS1/MS1	PS2/MS2	PS3/MS3	Non-nuclear safety
Korea		IC-1	IC-2	IC-3	Non-classified
Russia	I&C function	Category A	Category B	Category C	Non-categorized
	I&C system	Class 2		Class 3	Class 4 (Systems not important to safety)
South Africa[11]		Level 1 Direct influence on safety performance	Level 2 Products important to nuclear safety	Level 3 All products of the Nuclear Installation	Non safety or availability related
Switzerland		1	2	3	Non-classified
UK		Class 1	Class 2	Class 3	Non-classified
USA		System important to safety			(not specified)
		Safety related[12]		[8]	

3 Causes of Classification Difficulties

This Section describes the primary difficulties that the DICTF identified for the process of safety classification of I&C functions. To date, the DICTF has identified the following difficulties:

- Inconsistency between international standards and local regulations.
- Ambiguous requirements for safety classification.
- Incomplete rules for I&C function categorization.
- Inconsistent requirements for systems provided specifically as diverse backup to protection systems.

3.1 Inconsistency between international standards and local regulations

Besides the international standards organizations (*e.g.* IAEA and IEC), almost every country that produces nuclear power has local regulations for safety classification. As a result, one difficulty for safety classification is the inconsistency between international and national codes and standards.

The most challenging concern is a combination of insufficiently comprehensive local regulations, and local classification requirements which are different to international standards. This leads to the application of international codes and standards which are different to local requirements in order to fill the gaps.

Example 1 (national versus international)
Through its YVL guides, Finnish regulatory authority STUK assigns the safety-related I&C functions to the YVL safety categories (SC2, SC3, *etc.*). The YVL guides give few requirements for the qualification of components but indicate that the IEC requirements should be applied in Finland. Since the Finnish safety categories and IEC safety categories are inconsistent with each other, it is unclear whether a SC3 categorized function should be realized by a Category B (Class 2) or by a Category C (Class 3) qualified system.

Example 2 (international versus international)
Even between international codes and standards (*e.g.* IAEA and IEC) there are inconsistencies that present challenges for harmonization.

IAEA SSG-30 assigns the functions for main plant parameter controls to Class 3. IEC 61226 however assigns them to Class 2 (except with safety justification of combination of Class 3 functions)[13]. From the I&C standpoint, this could lead to these main plant parameter controls being implemented in a Class 2 system that is independent from the one which is used for 'real' Class 2 functions (DiD Level 3a), leading to an increase in the complexity of the I&C architecture and the sizing.

Example 3 (national versus international)
The US regulatory system and IEEE assign the highest classification to a broader scope of equipment than the IEC methodology. As a result, some equipment that is classified as Category B by the IEC is classified as safety-related/Class 1E in the US/IEEE methodology (*i.e.* highest category). This results in different architecture solutions for the protection system due to the differences in requirements regarding single failure criterion, independence, separation, design to cope with internal common cause failure, and diversification.

3.2 Ambiguous requirements for safety classification

If a requirement is not clearly identified[14], there is room for

[13] The following Category B assignment criterion has been removed in the Ed.4.0 of IEC 61226 item e):
Plant process control functions operating so that the main process variables area maintained within the limits assumed in the safety analysis, if these control functions are the only means of control of these variables. If different means are provided, clause 5.4.4 a) (category B) may apply.

[14] In general, 'clear' means: completely, clearly identified, coherently described, limited to one requirement per sentence/passage, identifiably, standardized, documented, verifiably, backward/forward traceably and consistently.

interpretation. Codes and standards with ambiguous requirements could be interpreted in different ways by the vendor, the utility and the authority. Ambiguous requirements could have a large impact over the duration of the project life-cycle.

Typically, codes and standards include glossaries to clarify the terminology used. Nevertheless, the acceptance criteria are vaguely specified and could be interpreted differently by the stakeholders, especially for topics of main interest (key concepts).

The following key concepts frequently cause trouble in interpretation of requirements:

- Defence-in-depth and diversity (assignment of different I&C systems and provision of diversity within and between systems to reduce the likelihood that common cause failure within the I&C system will cause failure of reactor safety functions).
- Separation (physical separation/ electrical isolation/functional independence /independence of communication).
- Redundancy (level of required redundancy required by *e.g.* N+1/ N+2 criteria).
- Reliability/availability (limits for digital I&C systems).
- Spurious activation (inadvertent actuation of I&C functions).

Depending on the concept, slightly different definitions are given in regulatory documents and standards. Without a harmonized understanding for the top-level concepts, discussions will arise for every upcoming project.

In September 2017 CORDEL DICTF published *Comparison of Definitions of Key Concepts*[15]*, the second report in the series on Safety Classification for I&C in Nuclear Power Plants* [17]. Each of the key concepts is defined by a series of terms and associated definitions in different regulatory documents and reference codes and standards. The report compares the various definitions by: identifying all the terms that are associated with the key concepts; and highlighting any inconsistencies in the different regulatory bodies' definitions of these terms.

For the architecture and system design it is necessary to set up the design based on design constraints. Inconsistent requirements could lead to late design modifications in the project life-cycle.

The technical report IEC TR 61838 [14] (integral part of the fourth level of IEC SC45A documents) proposes in Section 8.2.1.4 that the level of requirements should be linked to the selected category. For key terms such as 'single failure criterion', 'emergency electrical supply' or 'physical separation' a suggestion is given if required, depending on the safety category.

The level of detail of design requirements in standards equates to the hierarchy level of standards. While technical reports (such as IEC TR 61838 and IAEA TECDOCs) provide more specific acceptance criteria, high-level documents (such as IAEA SSG-39, IEC 61513) provide more generic phrases such as 'sufficient' or 'appropriate'. As a result, these high-level documents do not provide measurable requirements and therefore leave the details to the interpretation of the reader. Consequently, it is good practice to have technical reports and guidelines discuss and specify the detailed requirements associated with the high-level requirements. This practice, unfortunately, does not cover all the

[15] A revision of the report on definitions of key concepts was published in 2019.

high-level requirements and so the authority becomes the final interpreter.

The high-level documents make an implicit assumption that there may be many acceptable methods and that the management systems of the designer organizations should result in adequate or appropriate features. If there is a need to establish more detailed recommendations, these should be produced by the industry standards developing organizations (*e.g.* IEC and IEEE).

CORDEL DICTF published in April 2018 its report on *Defence-in-Depth and Diversity: Challenges Related to I&C Architecture* [17]. This looked at the inconsistencies in the definitions of terms, attributes, assessment methodologies, and scope associated with the concepts of 'defence-in-depth' and 'diversity' on I&C architecture designs and the implications of these inconsistencies.

The classification challenges identified in Section 3.1 of this report add to those identified in the April 2018 report.

3.3 Incomplete rules for categorization of 'other I&C functions'

The existing codes and standards for safety classification are focused on the I&C functions required to monitor the main process variables and control the nuclear plant. As I&C is used throughout nuclear plants, rules and regulations are also required to categorize functions important to safety outside of this focus ('other I&C functions'). Criteria for the categorization of 'other I&C functions' discussed below are currently not well documented.

3.3.1 I&C functions for safety system support features

For securing safe operation of the I&C systems important to safety the following support service systems are required:

- Power supply (including auxiliary power sources).
- HVAC (heating, ventilation and air conditioning).
- Fire/smoke detection.
- Extinguishing system (*e.g.* CO_2 extinguishing system).
- Communication system (telephone, plant communication system).
- Access control (I&C rooms, I&C cabinets, manual actions).
- Lighting.

The safety system support features have different levels of potential to affect the safe operation of the I&C systems. The HVAC and power supply support service systems are usually essential to ensure safety during normal operation[16].

The failure of these safety system support features can have a direct impact on the Category A functions (operability of the protection system). According to IEC 61226 - Ed.4:

Section 5.3.2 (Category A):
Category A also denotes functions whose failure could directly lead to accident conditions which may cause high severity consequences and for which no other Category A function exists that prevents such consequences.

Section 5.3.3 (Category B):
Category B also denotes functions whose failure could directly lead to accident conditions which may cause medium severity consequences and for which no other Category A or B function exists that prevents such consequences.

These support service functions should be Category A or at least B according to IEC 61226, it states further[17]:

[16] IAEA SSR 2/1 Requirement 27: Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.

[17] For definition of the factors, see Section 2.1.1

The initial classification shall then be amended, as necessary, to take into account factors (b) and (d) defined in IAEA SSR 2/1. 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 that its expected reliability can be demonstrated. Such a 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.

These time factors could have a significant role in establishing the safety class of the I&C system performing such support system functions.

Example: I&C safety system support features – HVAC
The categorization of the HVAC functions leads frequently to misunderstandings because of the lack of guidance. The HVAC system functions are very important for the safe operation of I&C.

Yet as failure of the HVAC system would not immediately cause the failure of the supported system, guidance is needed to describe the conditions under which the support system may be classified at a level lower than the supported system.

3.3.2 Support service functions for electrical/mechanical systems

Localized I&C functions are often integrated into electrical and mechanical equipment (so called 'black box' systems/self-standing systems/embedded systems, *etc.*). For example, the polar crane in the nuclear island generally has its own I&C for operating and monitoring the crane. Depending on the safety relevance and the consequences of its failure to the plant, the polar crane I&C may need to be assigned to a safety category and designed accordingly.

3.3.3 I&C service functions for main I&C systems

The service functions (*e.g.* self-diagnostic functions – IEC 61513) may be provided for the operation, diagnostics and maintenance of the I&C system itself. These service functions are either built-in features or realized by self-standing systems responsible for managing, for example, the removal from service of a system, fault monitoring, alarm processing, periodic testing or maintenance functions.

As the time to detect and correct failures directly affects the availability of SSCs (*i.e.*, mean downtime[18]) justification of a minimized downtime of SSCs should support the safety classification and design decisions regarding redundancy/diversity.

3.4 Criteria for diverse backup systems

The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents is the application of the concept of defence-in-depth (DiD). The Western European Nuclear Regulators Association (WENRA) report on *Safety of New NPP Designs* [15] includes the refined structure of the DiD levels (see Annex 1) that explicitly deal with diverse backup systems.

Currently, the defence-in-depth structure given in INSAG-10 [8] is widely used. The WENRA proposal is to split the current DiD Level 3 (control of accidents within the design basis) into two subparts: 3a) control of accidents resulting

[18] The 'mean down time' includes the time between the failure and restoration of operation, where not only the pure repair time but also all other delays are taken into account. Often the nuclear industry will use the term mean time to repair (MTTR) to include restoration of system operation after failure. MTTR factors in the availability of spare parts to restore the system.

from postulated single initiating events; and 3b) control of accidents resulting from postulated multiple failure events. In this structure, diverse functions meant to deal with an accident combined with protection system failure might be assigned to level 3b. Other regulators consider common cause failure (CCF) of digital safety systems to be a beyond design basis event. This difference means that there will be profound differences in the requirements for diverse backup systems depending upon which model is used in the country where a plant is being built.

WENRA proposes that, for each DiD level, dedicated I&C systems shall be installed in the plant in order to cope with failures of the previous levels of defence in depth (starting from DiD Level 2 for accident conditions).

For the I&C systems of DiD Level 1, 2, 3a, the scope and allocation of process and safety functions are quite clear.

The need to install dedicated systems for DiD Level 3b and 4 is fairly recent and the existing requirements for those I&C systems differ between codes and standards (national and international).

The requirements for a DiD Level 3b I&C system are mostly based on the discussion of the postulated common cause failure[19] of the DiD Level 3a realized by a digital I&C system platform. Consequently, a so-called diverse actuation system (DAS) is required for the DiD Level 3b.

To ensure adequate independence between DiD Levels 3a and 3b or between Levels 3 and 4, several aspects must be taken into account, particularly diversity [18] and separation[20] [12]. However, depending on when a system is assigned to Level 3b or Level 4, the requirements for a DAS may be very different with regard to:

- Scope of functions.
- Type of I&C platform (hardware versus software).
- Safety classification.
- Manual, instead of automatic, backup.

This leads to some of the inconsistencies between regulators that are described below.

Diverse actuation systems[21]

When digital systems are used to implement protection system functions, it is not uncommon for the analysis described in paragraph 4.32 of IAEA SSG-39 [3] to find that common cause failure (CCF) within the digital protection system might result in unacceptable consequences for certain combinations of CCFs and postulated initiating events (PIEs). When this situation is encountered, a DAS is often provided to back up the protection system.

There is general agreement that a DAS may effectively mitigate the consequences of specific PIEs in conjunction with postulated CCFs of a protection system. There are, however, different approaches to safety classification, the use of digital DASs to back up digital protection systems, and use of manual actuation to mitigate the consequences of protection system CCF.

I&C system classification of DAS

Some regulatory authorities expect that DASs will be classified as safety systems whereas others allow them to be systems of a lower safety classification. Depending on the regulatory authority, the expected level of safety classification is based upon the reliability claims made for the DAS.

[19] The Digital Instrumentation and Control Working Group (DICWG) of the OECD Multinational Design Evaluation Programme (MDEP) published in 2013 a common position on the treatment of common cause failure caused by software within digital safety system [9].

[20] Physical separation, Electrical isolation, Functional independence and Independence of communication

[21] Part of the section has been derived from IAEA SSG-39 [3]

Technology used for DAS
In some cases, the regulatory authorities expect the DAS to be a hardwired system or a system using integrated circuits but not programmable devices (*e.g.*, electrically programmable logic devices or FPGAs). The use of digital systems could be discouraged, but not prohibited by regulatory authorities. Other regulatory authorities allow the use of digital systems if adequate diversity is demonstrated.

Scope of I&C functions to be realized by DAS
For the design of the DAS, the identification of functions to be realized by the diverse I&C system is essential. Codes and standards include different approaches for this topic. IAEA SSR-2/1 [1] requests that analysis of design extension conditions for the plant is carried out. According to IEC 62340 [13] the design of the I&C architecture should tolerate CCF for that subset of design basis events which are to be expected at a frequency that is higher than a specified limit based on this analysis. Table 2 of Annex 1 shows the correlation between the design extension conditions DEC-A and DEC-B with the DiD Level 3b based on the probabilistic frequency of the protection system CCF in combination with the postulated design basis events. These DAS I&C functions could be realized by duplication of the function with the same or graded thresholds for actuation or by equivalent functions with differences in its logic.

Use of manual actions for diverse actuation
Generally, manual actuation may be accepted as a diverse backup for the protection system but the conditions under which manual actuation may be acceptable vary. Accepted practices include[22]:

- When the action is not needed in less than 30 minutes and analysis of human factors has confirmed that a proper decision can be taken and implemented within that time.
- When action is not needed in less than 20 minutes.
- Engineered safety feature actuation, but not reactor trip.
- No restriction on manual action.

While the above illustrates the range of practices among regulatory authorities, a regulator may take a different approach based upon the specific situation proposed.

In 2013 MDEP published a common position on the treatment of CCF caused by software within digital safety systems [9]. In addition to common positions, the document identifies the different regulatory positions regarding the quality and classification of diverse backup systems and use of manual actions.

In 2018, IAEA published TECDOC-1848, *"Criteria for diverse actuation systems for nuclear power plants"* [5]. This publication describes a philosophy where the diverse actuation system (DAS) backs up safety functions performed by the primary protection systems. The purpose is to identify, based on current practices in member states, common criteria for the design and implementation of a diverse actuation system as a backup system to a reactor protection system to implement safety functions. It points out: *"A single harmonized classification scheme is currently not used among all Member States. Depending on Member State requirements, the same or a lower safety classification than the reactor protection system may be assigned to a DAS."*

[22] Disallowing manual action in the first 20 or 30 minutes effectively prevents crediting early operator action as a backup for automatic initiation of safety functions.

4 Differences between IAEA SSG-30 and IEC 61226

IAEA SSG-30 should be seen as the top-level document specifying the general constraints for the safety classification of SSCs in nuclear power plants. IEC 61226 further elaborates the specific requirements for the implementation of SSG-30 as it applies to I&C functions. The IEC SC45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards (such as SSG-30) and in the related IAEA publications (such as TECDOC-1787 [4]).

IAEA SSG-30 provides recommendations and guidance on how to meet the requirements but does not provide criteria for judgement on details. IEC 61226 goes further and provides categories that should be assigned to functions important to safety. Nevertheless, this approach still requires interpretation of the requirements by the vendors and utilities in the realization of the overall I&C systems in the nuclear power plant.

Unfortunately, the classification given by IEC 61226 is not valid for all countries. As shown in Table 2, different classifications for safety categories are in place.

By consideration of the recent IEEE activities (see Section 2.2.1), the coordination of the main SDOs (IEC SC45A WG07 and IEEE WG 6.2) on safety classification would be a significant step for worldwide harmonization of codes and standards.

Neither document gives more than a limited discussion of the difficulties identified in Section 3. The CORDEL DICTF should continue to develop bridges between the needs from vendors and utilities to the SDOs.

5 Promoting consistency between codes and standards for I&C safety classification

IAEA TECDOC-1787, published in 2016, provides an interpretation of SSG-30 (released in 2014) with comprehensive examples. With regard to the classification process (identification of functions and assignment to severity levels, plant states, function category), TECDOC-1787 introduces the methodology for identification and classification of SSCs performing the categorized functions. The safety significance at the I&C component level is expected to be correctly reflected considering the functional role of the component. SSG-30 in combination with TECDOC-1787 forms the basis for a harmonized specification process.

The DICTF supports CORDEL's mission to standardize the design of I&C safety systems through its publications (*i.e.* this report, as well as the reports on *Defence-in-Depth and Diversity* [18] and *Comparison of Definitions of Key Concepts* [17]), and through the contribution of its members on IAEA, IEC and IEEE activities. Over the last few years, DICTF members have contributed to a range of activities, including:

- Presentation of DICTF work during regular exchange meetings with the NEA Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital I&C (WGDIC)
- IAEA conferences and publications (*e.g. Criteria for Diverse Actuation Systems for Nuclear Power Plants* [5] and *Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants* [6]).
- IEC SC45A revision of IEC 61226, based on Category D liaison between the World Nuclear Association and IEC working groups WG03 and WG07.
- Discussions with IEEE WG 6.2 on the implementation of the approach in IAEA SSG-30.

References

[1] International Atomic Energy Agency, *Safety of Nuclear Power Plants: Design*, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), STI/PUB/1715 (February 2016)

[2] International Atomic Energy Agency, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*, IAEA Safety Standards Series, Specific Safety Guide No. SSG-30, STI/PUB/1639 (May 2014)

[3] International Atomic Energy Agency, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, IAEA Safety Standards Series, Specific Safety Guide No. SSG-39, STI/PUB/1694 (April 2016)

[4] International Atomic Energy Agency, *Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants*, IAEA-TECDOC-1787 (April 2016)

[5] International Atomic Energy Agency, *Criteria for Diverse Actuation Systems for Nuclear Power Plants*, IAEA-TECDOC-1848 (June 2018)

[6] International Atomic Energy Agency, *Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants*, IAEA Nuclear Energy Series No. NPT-T-2.11, STI/PUB/1821 (August 2018)

[7] International Atomic Energy Agency, IAEA Safety Glossary, *Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition*, STI/PUB/1830 (June 2019)

[8] International Atomic Energy Agency, *Defence in Depth in Nuclear Safety*, INSAG-10, A report by the International Nuclear Safety Advisory Group, STI/PUB/1013 (June 1996)

[9] Multinational Design Evaluation Programme, Digital Instrumentation and Controls Working Group, MDEP Generic Common Position No DICWG-01, *Common Position on the Treatment of Common Cause Failure Caused by Software Within Digital Safety Systems* (June 2013)

[10] International Electrotechnical Commission, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*, IEC 61513 Edition 2.0 (August 2011)

[11] International Electrotechnical Commission, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*, IEC 61226 Edition 4.0, (2019)

[12] International Electrotechnical Commission, *Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Separation*, IEC 60709 Edition 3.0 (April 2018)

[13] International Electrotechnical Commission, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*, IEC 62340 Edition 1.0 (December 2007)

[14] International Electrotechnical Commission, *Nuclear power plants – Instrumentation and control important to safety – Use of probabilistic safety assessment for the classification of functions*, IEC TR 61838 Edition 2.0 (December 2009)

[15] Western European Nuclear Regulators Association, WENRA Report, *Safety of new NPP designs*, Study by Reactor Harmonization Working Group RHWG (March 2013)

[16] World Nuclear Association, CORDEL Digital Instrumentation & Control Task Force, *2014-2016 Outlook*, CORDEL/DICTF (2014)

[17] World Nuclear Association, CORDEL Digital Instrumentation & Control Task Force, *Safety Classification for I&C Systems in Nuclear Power Plants: Comparison of Definitions of Key Concepts* (September 2019)

[18] World Nuclear Association, CORDEL Digital Instrumentation & Control Task Force, *Defence-in-Depth and Diversity: Challenges Related to I&C Architecture* (April 2018)

[19] World Nuclear Association, CORDEL Strategic Plan 2019-2023 (2019)

Annex 1 | Plant States - Sequence of Events

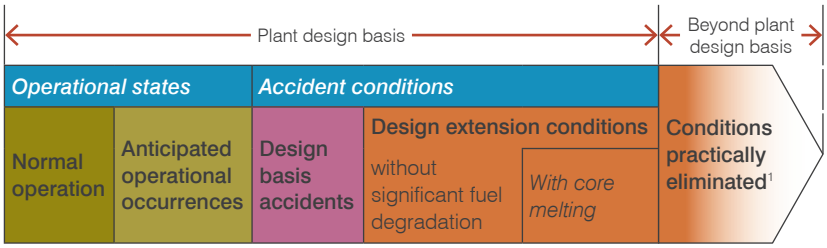
The classification of structures, systems and components (SSCs) is closely linked to the plant states and the postulated initiating events (PIEs) that are considered in the design of a nuclear plant. This aim of this Annex is to reach a common understanding on topics concerning plant states and sequence of events.

After occurrence of a PIE, the safety systems shall initiate immediate actions to bring the plant firstly to a controlled state in accordance with the safety analysis, and secondly to a safe state (if return to normal operation is precluded). IAEA SSG-30 [B] introduces the link between the plant states to be reached after a PIE and the severity of consequences if the function is not performed based on the categorization of safety functions. This Annex includes general points on time and reactor states that are adopted by IEC TR 61838 [F].

Both IAEA and IEC documents use the term 'plant state' for two different subjects: to identify the events considered during plant operation (*i.e.* normal operation, anticipated operational occurrences); and to define the plant status to be reached after an event has occurred (*e.g.*, physical conditions such as temperature, pressure, radiation, *etc.*).

I. Plant states – events considered during plant operation

The plant states (plant conditions) of a nuclear power plant are divided into 'operational states' and 'accident conditions' including the 'normal operation' of the plant, the postulated 'design basis events' and 'beyond design basis accidents' (*i.e.*, design extension conditions). Figure 1 presents the IAEA's definition of plant states.



[1] "Practical Elimination" of very infrequent events as demonstrated *e.g.* by PSA studies

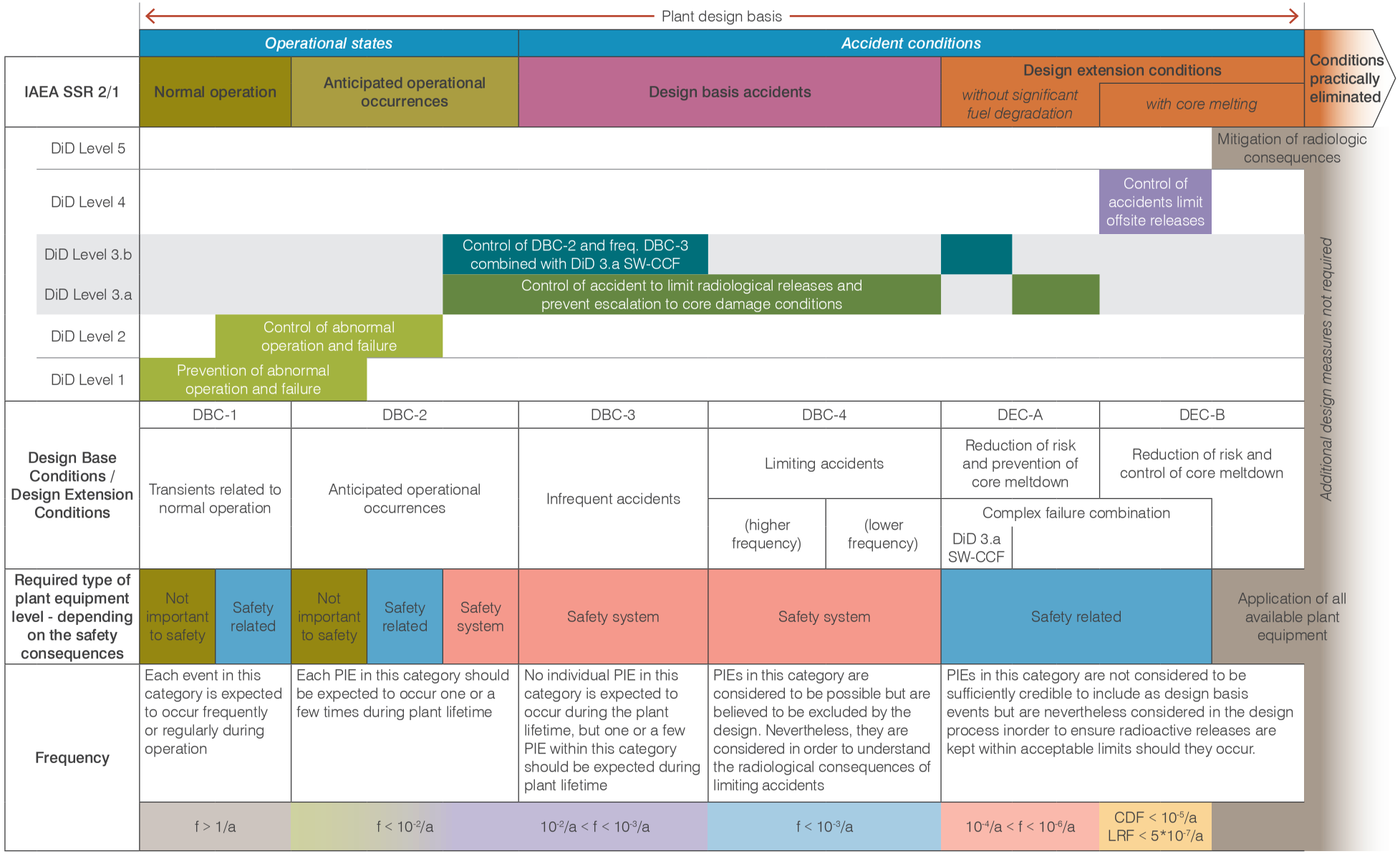
Figure 1. Plant states – according to IAEA SSR 2/1 [A][1]

Table 1 includes a proposal to link events/PIEs to the Western European Nuclear Regulators Association (WENRA) defence-in-depth (DiD) levels [E] and the IAEA/IEC plant states[2]. For DiD Level 3.b, the scope of the diverse actuation system (DAS) function according to the STUK approach (DBC-2 + frequent DBC-3 event) is given. Depending on the regulator the scope of functions may differ.

[1] "Practical Elimination" of very infrequent events as demonstrated *e.g.* by PSA studies

[2] DiD Level 5 is used for emergency preparedness planning purposes

Table 1. Correlation between DiD levels and allocation of events/PIEs



II. Plant states - Time and reactor states-based approach

In Figure 1 the different types of plant state are identified for the accident conditions which form the starting point for the next sequence of events.

Figure 2 provides a generic process after initiation of a PIE. If the safety I&C detects that a plant parameter has deviated from normal conditions, the safety I&C should initiate dedicated measure(s) in accordance with the safety analysis. For events with high severity, the primary target is to reach a controlled state, realized automatically by reactor trip and engineered safety feature actuation system (ESFAS) functions. The controlled state is not a long term safe state for the plant but provides a stable period to allow time for analysis and subsequent actions for the plant to be brought to a safe state. Depending on the complexity and the progression of the PIE, this could be realized by the automatic I&C safety actuation system or by manual means from the main control room. A safe state is a maintainable state in which the plant could be kept over a long period. Plant parameters have to be monitored and the residual heat removal system has to be controlled in order to maintain the safe state.

The time between the initiation of a postulated event and the achievement of reaching the subsequent events plant state (’controlled state’ and ‘safe state’) is of high importance and defined in the plant’s safety analysis. The time frame between the PIE and the ‘actuation of process & safety systems’ corresponds to the response time requirement for the safety I&C plus the response time requirements of the electrical and mechanical SSCs. This sequence of events is mostly likely realized by automatic functions.

Afterwards, depending on the situation inside the plant (corresponding to the level of PIE), the plant could return, from the safe state, to the normal operation state or continue to a cold shutdown state.

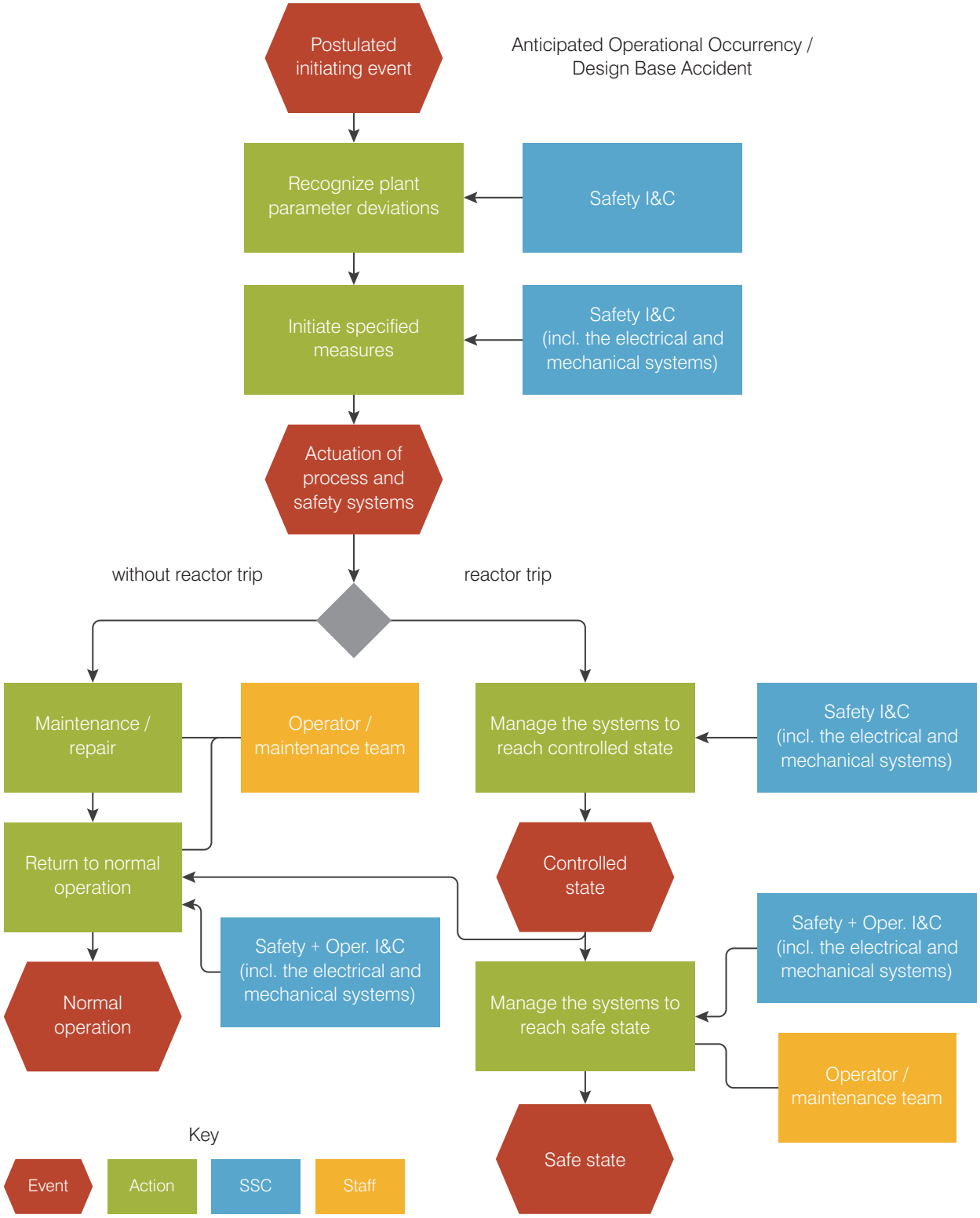


Figure 2. Generic sequence of events/actions/required SSCs after PIE

The need for operator action in the early phase of the PIE sequence should be minimized. The required realization (automatically/manually) of subsequent actions depends on the complexity and time duration of the response.

Based on the recommended time frame to reach the controlled state, the instrumentation and control (I&C) systems for the required process and safety functionality is realized either automatically or manually.

Regarding the application of manual safety actions, the IAEA SSG-39 [C] provides in paragraph 7.18 to 7.26 more detailed criteria which should be taken into consideration in the safety and process design.

IEC TR 61838:2009 [F], *Use of probabilistic safety assessment for the classification of functions*, proposes the correlation between the state of the reactor, the timescale to the safety state, and the 'group of PIEs' (DBCs, DECs, internal hazards) - see Table 2.

Table 2. Time and reactor states approach for safety classification – IEC 61838 [F]

State of reactor	Initiating event	Controlled state (non-hazardous stable state)	Safe state (safe shutdown state)	
Timescale	0h	24h	72h	
PIE group				
DBC	Category A	Category B	Category C	Not classified
DEC	Category C			Not classified
Internal hazards	Category C			Not classified

III. Assignment of safety categories based on plant states/severity of consequences

The current version of IAEA SSG-30 [B] identifies the relationship between functions credited in the analysis of postulated initiating events and safety categories (see Table 3).

Table 3. Relationship between functions and PIE – IAEA SSG-30 [B]

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 AOO	Safety category 1	Safety category 2	Safety category 3
Functions to reach the controlled state after DBA	Safety category 1	Safety category 2	Safety category 3-
Functions to reach and maintain a safe state (transfer from controlled state to safe state)	Safety category 2	Safety category 3-	Safety category 3-
Functions for the mitigation of consequences of a DEC	Safety category 2 or 3	Not categorized	Not categorized

Table 3 shows the correlation, specified by SSG-30 for categorization of functions according to the magnitude of the PIE (AOO/DBA/DEC) and the plant states to be reached (controlled state/safe state), and the severity of consequences (high/medium/low) if the related function is not performed.

IV. Definitions of plant states

IAEA SSR 2/1 [A] defines plant states.

Controlled state: *Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state.* (IAEA SSR 2/1 [A])

Safe state: *Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.* (IAEA SSR 2/1 [A])

IEC 61226 [D] and IEC TR 61838 [F] use the term 'non-hazardous stable state' for controlled state and 'safe shutdown state' for safe state.

Non-hazardous stable state: *State of the plant, where stabilisation of any transient has been achieved, the reactor is subcritical, adequate heat removal is ensured and radioactive releases are limited.*

NOTE: A transient is considered to be stabilised when, for all safety significant parameters, the margins (e.g. between the heat removal capacity and heat generation) are either stable or increasing, or sufficient margin remains to cover all expected physical processes.

Note: The 4th edition of IEC 61226 does not use the term 'non-hazardous stable state'.

V. References

[A] Specific Safety Requirements No. SSR-2/1 (Rev.1), *Safety of Nuclear Power Plants: Design*, International Atomic Energy Agency, STI/PUB/1715, February 2016

[B] IAEA Specific Safety Guide No. SSG-30, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*, International Atomic Energy Agency, STI/PUB/1639, May 2014

[C] IAEA Specific Safety Guide No. SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, International Atomic Energy Agency, STI/PUB/1694, April 2016

[D] IEC 61226:2009 (Ed. 4.0) *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*, International Electrotechnical Commission, July 2009

[E] WENRA Report, *Safety of new NPP designs*, Study by Reactor Harmonization Working Group RHWG March 2013

[F] IEC TR 61838:2009 (Ed. 2.0), *Nuclear power plants – Instrumentation and control important to safety – Use of Probabilistic Safety Assessment for the Classification of Functions*, International Electrotechnical Commission, December 2009

World Nuclear Association
Tower House
10 Southampton Street
London WC2E 7HA
United Kingdom

+44 (0)20 7451 1520
www.world-nuclear.org
info@world-nuclear.org

© 2020 World Nuclear Association. Registered in England and Wales, company number 01215741