



# Safety Classification for I&C Systems in Nuclear Power Plants - Current Status & Difficulties

CORDEL Digital Instrumentation & Control  
Task Force

Title: Safety Classification for  
I&C Systems in Nuclear Power Plants -  
Current Status & Difficulties  
Produced by: World Nuclear Association  
Published: September 2015  
Report No. 2015/008

© 2015 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.

# Contents

Foreword	1
Executive summary	3
1. Introduction	4
1.1 Background	4
1.2 Objective	4
1.3 From process design to I&C design	4
2. Generic approach for I&C safety classification	6
2.1 IAEA SSG-30 – Safety Classification of Structures, Systems and Components in Nuclear Power Plants	7
2.2 IEC standards	8
2.2.1 IEC 61226 (IEC Level 2 document)	8
2.2.2 IEC 61513 (IEC Level 1 document)	8
2.2.3 IEC TR 61838 (IEC Level 4 document)	8
2.3 Comparison of I&C classification	8
3. Causes of classification difficulties	10
3.1 Inconsistency between international standards and local regulations	10
3.2 Ambiguous requirements for safety classification	10
3.3 Incomplete rules for categorization of 'other I&C functions'	11
3.3.1 I&C functions for support service systems	11
3.3.2 Support service functions for electrical/mechanical systems	12
3.3.3 I&C service functions for main I&C systems	12
3.4 Criteria for diverse backup systems	12
4. Differences between IAEA SSG-30 and IEC 61226	14
5. Develop 'bridges' between codes and standards for I&C safety classification	15
6. References	16
Annex 1: Plant states – sequence of events	17
Annex 2: DICTF actions for "Safety Classification for I&C systems in nuclear power plants"	26



# Foreword

In January 2007 the World Nuclear Association established the Cooperation in Reactor Design Evaluation and Licensing Working Group (CORDEL WG) 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 the CORDEL WG was set up in 2013 to investigate key issues in digital I&C related to the licensing of new nuclear power plants, and to collaborate with the International Electrotechnical Commission (IEC) and the Multinational Design Evaluation Programme (MDEP) Digital Instrumentation and Control Working Group (DICWG).

On the basis of an internal survey, the CORDEL DICTF has identified four main issues:

- Safety Classification for I&C systems in Nuclear Power Plant's
- Defense in Depth and Diversity (D3)<sup>1</sup>.
- Field-Programmable Gate Arrays (FPGA): criteria for acceptance
- Reliability predictions

These are discussed in more detail in *CORDEL DICTF 2014-2016 Outlook* [12].

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 Secretariat would like to acknowledge the leadership of Johannes Pickelmann, as Chairman of the Digital Instrumentation and Control Task Force, as well as main drafter of the report. We would also like to thank all the members of the task force for their active support and input into the report. Thanks are also due to Gary Johnson, who provided valuable advice and support to the task force.

<sup>1</sup> Originally referred to as: diversity and common cause failure (CCF)

# List of acronyms

D3	Defence in depth and diversity
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
EUR	European Commission
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
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 [5].

# Executive summary

Classification of structures, systems and components (SSC) 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. Whereas before classification of an item was derived from the safety importance of its system, today it is derived from the categorization of the safety relevance of a process and safety function to be realized by e.g. the I&C system

The nuclear industry's graded approach to safety stipulates that systems having higher safety importance should be of demonstrably higher quality, more tolerant of failures, and more resistant of hazards both inside and outside the plant. Thus the safety class of an I&C system and its assigned defence in depth (DiD) level have direct impact on the requirements on qualification, quality assurance, fault tolerance, system architecture, physical layout within the plant and the extent of engineering documentation.

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

This report provides an overview of the generic approach to I&C safety classification (Section 2), the important international standards and guidelines published by IEC and IAEA (Sections 2.1 & 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. Annex 2 identifies near-term actions that the CORDEL Digital Instrumentation & Control Task Force (DICTF) will undertake to help improve the situation.

As safety classification is closely linked to plant states and postulated initiating events, Annex 1 describes the important areas from an I&C view.

# 1 Introduction

## 1.1 Background

Safety classification is the process of identifying the functions important to the safety of a nuclear power plant and classifying them according to their safety significance. Functional classification determines the design and manufacturing criteria required to ensure that the reliability of plant structures, systems and components (SSCs) 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 topics that create difficulty for CORDEL members when developing and applying safety classification for I&C systems in nuclear power plants and to describe the apparent cause of these difficulties.

The DICTF tasks identified in Annex 2 include activities that are intended to:

- Improve international standards dealing with safety classification of I&C functions, systems, and equipment (FSE).

- Ensure that ongoing IAEA work in the area of safety classification takes due account of issues specific to I&C.
- Harmonize terminology that is important to safety classification of I&C FSE.
- Inform the Digital I&C Working Group of the NEA Multinational Design Evaluation Programme (MDEP) about issues where common regulatory positions may reduce unnecessary regulatory burdens in the area of I&C safety classification.
- Develop background information to promote harmonization of industry approaches to safety classification for I&C FSE.

## 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 continuous 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 [7].

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 of additional I&C-specific FSE, which also must be safety classified.

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

Requirement 22 of IAEA No. SSR-2/1 [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 IAEA NS-G-1.3 [2] 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).

As defined in NS-G-1.3 an item important to safety is an item that is part of a safety group or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public.

I&C systems important to safety are identified on the basis of their necessary 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', two main subdivisions are made as follows:

- **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: protection systems, 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*

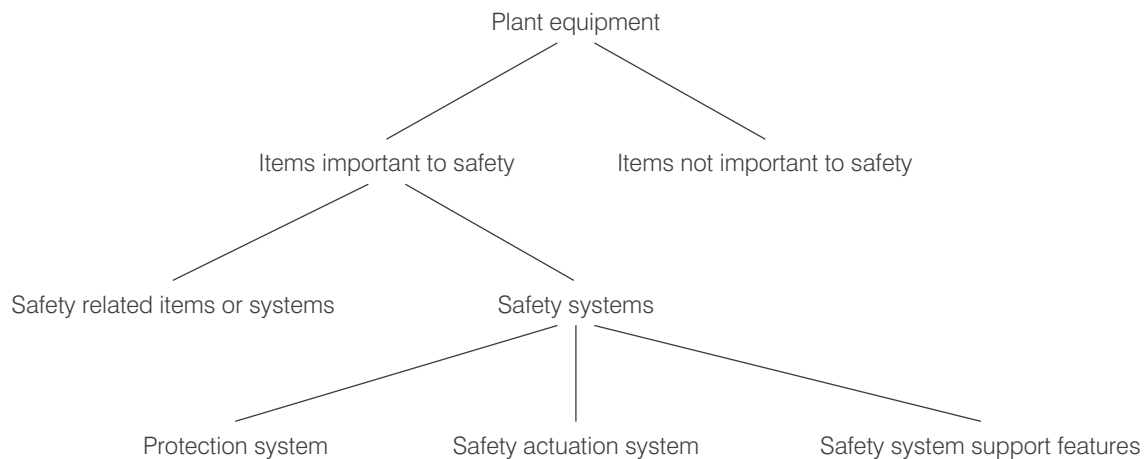


Figure 1: Generic identification of I&C systems important to safety (IAEA NS-G-1.3)

*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 [3] and IEC 61226 [8] 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 and 2.2.

The IEC 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 [8] – IEC 61513 [7] 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 IAEA SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants

IAEA SSG-30 [3] 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 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 safety classes of SSC (1, 2 and 3) and describes generically the rules for classification.

At the time of drafting this report, the IAEA is preparing a dedicated TECDOC to provide guidance on how an organization can establish a comprehensive safety classification of SSCs compliant with the IAEA recommendations.

## 2.2 IEC standards

### 2.2.1 IEC 61226 (IEC Level 2 document)

IEC 61226 [8]<sup>2</sup> is an international standard that responds to the IAEA SSR-2/1 [1] 'safety classification' requirement 22.<sup>3</sup>

It introduces time factors such as:

- The duration that the I&C system is needed once it has been initiated.
- The time for which alternative actions can be taken.
- The timeliness by which hidden faults can be detected and remedied.

This standard extends the classification strategy presented in the IAEA Safety Guide SSR-2/1, and establishes the criteria and methods 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:

- Classify the I&C functions important to safety into categories, 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.
- Assign specification and design requirements to I&C systems and equipment concerned which perform the classified functions.

Table 1: Correlation between classes of I&C systems and categories of I&C functions (IEC 61513 [7])

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

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 classification according IEC 61226 is focused on the I&C process functions. The current version does not include the requirements to classify electrical systems, but this might be considered in the next edition.

### 2.2.2 IEC 61513 (IEC Level 1 document)

IEC 61513 [7] 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 release of IAEA SSG-30. Annex B of IEC 61513 also includes

a comprehensive explanation of the relation 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 (IEC Level 4 document)

The IEC 61838 [10] technical report, *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, the MDEP member states and two countries that are not members of MDEP.

Table 2: System safety classifications<sup>4</sup>

Organizations or Countries		Safety Classification of I&C Functions and Systems in nuclear plants				
Main international standard organizations						
IAEA NS-G-1.3		Systems Important to Safety			Systems not important to safety	
		Safety	Safety-related			
IAEA SSG-30	Function	Safety category 1	Safety category 2	Safety category 3		
	System	Safety class 1	Safety class 2	Safety class 3		
		Systems Important to Safety			Non-classified	
IEC 61226	I&C function	Category A	Category B	Category C		
	I&C system	Class 1	Class 2	Class 3		
IEEE		Systems Important to Safety			Non-safety-related	
		Safety-related	5			
EUR <sup>6</sup>	Safety level of functions / I&C systems	F1A	F1B	F2	NS (non-safety)	
MDEP member states						
Canada		Category 1	Category 2	Category 3	Category 4	
France		F1A	F1B	F2	Non-classified	
Finland		Class 2	Class 3	EYT/ STUK	EYT (classified non-nuclear)	
UK		Class 1	Class 2	Class 3	Non-classified	
United States		Systems Important to Safety			(not specified)	
		Safety-Related	5			
India		IA	IB	IC	NINS	
Japan		PS1/MS1		PS2/MS2	PS3/MS3	Non-nuclear safety
Korea		IC-1		IC-2		IC-3
Russia		Class 2	Class 3		Class 4 (Systems not important to safety)	
Others nuclear states						
Switzerland		1	2	3	Non-classified	
Germany	I&C function	Category 1	Category 2	Category 3		Non-classified
	I&C equipment	E1		E2		

<sup>2</sup> IEC 61226 (3rd edition) is currently under revision and should be read in association with the IAEA guides and IEC 61513.<sup>3</sup> previously IAEA NS-R-1 5.1<sup>4</sup> Such a table gives only a qualitative mapping between the various classification systems.<sup>5</sup> IEEE/NRC does not have a name for items that are important to safety, but not classed as 'safety-related'.<sup>6</sup> EUR is being revised to follow the SSG-30 principles.

# 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.

The IAEA SSG-30 assigns the functions for main plant parameter (MPP) controls to Class 3. IEC 61226 however assigns them to Class 2 (except with safety justification of combination of Class 3 functions)<sup>7</sup>. From the I&C standpoint, this could lead to MPP 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.

For associated DICTF action items see Annex 2.

### 3.2 Ambiguous requirements for safety classification

If a requirement is not clearly identified<sup>8</sup>, there is room for 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. Never-the-less, the acceptance criteria are vaguely specified and could be interpreted differently by the stakeholders,

<sup>7</sup> The following Category B assignment criterion has been removed in the draft 4th edition of IEC 61226 item e):

*Plant process control functions operating so that the main process variables are 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.*

<sup>8</sup> Criterion 'clear' means: completely, clearly identified, coherently described, limited to one requirement per sentence/passage, identifiably, standardized, documented, verifiably, backward/forward traceably and consistently.

<sup>9</sup> IAEA SSR 2/1 – Req. 27: *Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.*



especially for topics of main interest (key words).

The following key words 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 failures 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 e.g.  $N+1/N+2$ ).
- Reliability/availability (limits for digital I&C systems).
- Spurious activation (inadvertent actuation of I&C functions).

Depending on the key word, slightly different meanings are given in regulatory documents and standards.

As long as there is no harmonized understanding for such top level wording, discussions will arise for every upcoming project.

#### **Example: 'separation'**

Codes and standards do not specify in detail what level of 'separation' is required (acceptance criteria) for safety-related applications.

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.

IEC 61226 edition 3.0 from 2009 [8] uses the term 'non-hazardous stable state'. This term is subject to different interpretations depending on local practice.

Note: IEC 61838 [10] proposes in Section 8.2.1.4 that the level of requirements should be linked to the selected category. For key words such as 'single failure criterion', 'emergency electrical supply' or 'physical separation' a suggestion is given if required, depending on the safety category. But, generally standards avoid specific criteria and give instead more generic phrases such as 'sufficient', 'appropriate', etc.. The DICTF should assess to what extent criteria should be introduced into codes and standards.

For associated DICTF action items see Annex 2.

### **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 and operate the main process variables. As I&C is widely spread in 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 support service systems**

For securing safe operation of the safety-relevant I&C systems 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<sub>2</sub> extinguishing system).

- Communication system (telephone, plant communication system).
- Access control (I&C rooms, I&C cabinets, manual actions).
- Lighting.

The support service systems 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<sup>9</sup>.

The failure of these support service systems can directly impact on the Category A functions (operability of the protection system). According to IEC 61226 [8] Section 5.3.3:

*Category B also denotes functions whose failure could initiate a DBE or worsen the severity of a DBE. Because of the presence of a Category A function to provide the ultimate prevention of or mitigation of the consequences of a DBE, the safety requirements for the Category B function need not be as high as those for the Category A function."*

The I&C functions of these support service systems should be at least Category B according to IEC 61226.

Section 5.2 of IEC 61226 refers to IAEA NS-G-1.3 to introduce time factors such as:

- The duration that the I&C system is needed once it has been initiated.
- The time for which alternative actions can be taken.
- The timeliness by which hidden faults can be detected and remedied.

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 support service system – HVAC**

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

As the HVAC support service system is continuously in operation and its failure does not immediately cause 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 down time<sup>10</sup>) justification of a minimized down time of SSCs should support the safety classification and design decisions regarding redundancy/diversity/etc.

For associated DICTF action items see Annex 2.

### **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 WENRA report Safety of New NPP Designs [11] includes the refined structure of the levels of DiD (see Annex 1) that explicitly deal with diverse backup systems.

Currently, the defence-in-depth structure given in INSAG-10 [6] 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 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 failures (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).

<sup>10</sup> 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.

<sup>11</sup> Part of the section has been derived from IAEA SSG-39 [4]

<sup>12</sup> 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.



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 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 Level 3a and 3b or between Level 3 and 4, several aspects must be taken into account:

- Diversity.
- Physical separation – structural or by distance.
- Functional isolation.
- However, depending on when a system is assigned to level 3b or level 4, the requirements for a DAS may be very different in regard to:
- Scope of functions.
- Type of I&C platform (hardware versus software).
- Safety classification.

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

#### **Diverse actuation systems<sup>11</sup>**

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 [4] to find that

common cause failures (CCFs) within the digital protection system might result in unacceptable consequences for certain combinations of CCFs and 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 lower safety classification. Depending on the regulatory authority, the expected level of safety classification is based upon the reliability claims made for the DAS.

#### **Technology used for DAS**

In some cases, the regulatory authorities expect that DASs will be hardwired systems. The use of digital systems is 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 [9] the design of the I&C architecture should tolerate CCF for that subset of DBEs which are to be expected at a frequency that is higher than a specified limit based on this analysis. Table 2 of Annex 1 gives a correlation between the design extended conditions DEC-B and DEC-C to 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<sup>12</sup>:

- 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.

For associated DICTF action items see Annex 2.

# 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 should further elaborate the specific requirements for the implementation of SSG-30 as it applies to I&C functions.

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 realisation of the overall I&C 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.

Neither document gives more than a limited discussion of the difficulties identified in Section 5. The CORDEL DICTF should develop bridges between the needs from vendors and utilities to the standards organizations.

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

IAEA SSG-30 was officially released in 2014. The IAEA is now working on a dedicated TECDOC describing the objectives of SSG-30. At the time of drafting this report, a request for a close relationship with IAEA has been initiated for further exchange.

For IEC 61226 the situation is different. Since the 2009 revision of IEC 61226, several changes occurred in IAEA documents, mainly on SSR 2/1, SSG-30, and SSG-39 as well as IEC publications including IEC 61513. A category D liaison between

the World Nuclear Association and working groups A3 and A7 of the IEC SC 45A has been initiated.

Since the formation of the DICTF, regular exchange meetings with the MDEP DICWG have taken place, where the topic 'Safety Classification for I&C systems in Nuclear Power Plant' has been presented. Further exchange shall be performed after publication of this report.

For associated DICTF action items see Annex 2.

# References

- [1] Specific Safety Requirements No. SSR-2/1, *Safety of Nuclear Power Plants: Design*, International Atomic Energy Agency, STI/PUB/1534, January 2012
- [2] IAEA Safety Guide No. NS-G-1.3, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*, International Atomic Energy Agency, STI/PUB/1116, March 2002
- [3] 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
- [4] IAEA Specific Safety Guide No. SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, (under Revision Draft Safety Guide DS431 -supersedes NS-G-1.1 and NS-G-1.3), International Atomic Energy Agency, Draft M step 10 2014-03-21
- [5] IAEA Safety Glossary, *Terminology Used in Nuclear Safety and Radiation Protection 2007 Edition*, International Atomic Energy Agency, June 2007
- [6] INSAG-10, *Defence in Depth in Nuclear Safety*, International Nuclear Safety Advisory Group (INSAG), 1996
- [7] IEC 61513:2013, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*, International Electrotechnical Commission, 2013-03
- [8] IEC 61226:2009 *Nuclear power plants – Instrumentation and control important for safety – Classification of instrumentation and control functions*, International Electrotechnical Commission, 2009
- [9] IEC 62340:2007, *Requirements for coping with common cause failure (CCF)*, International Electrotechnical Commission, 2007-12
- [10] IEC/TR 61838:2010, *Use of Probabilistic Safety Assessment for the Classification of Functions*, International Electrotechnical Commission , 2010-02
- [11] WENRA Report, *Safety of new NPP designs*, Study by Reactor Harmonization Working Group RHWG March 2013
- [12] CORDEL Digital Instrumentation & Control Task Force, *2014-2016 Outlook*, CORDEL/DICTF(2014)

# Annex 1 | Plant states – sequence of events

The classification of structures, systems and components (SSC) is closely linked to the plant states and the postulated initiating event which are required to be considered in the design of a NPP for safe plant operation. This annex has the intention to get a common understanding regarding topics concerning plant states and sequence of events.

After occurrence of a Postulated Initiating Event (PIE), the safety systems shall initiate immediately actions to bring the NPP first to controlled state and secondly to safe state (if return to normal operation is precluded). IAEA SSG-30 [B] introduces the link between the plant states to be reached after PIE and the severity of consequences if the function is not performed for the categorization of safety functions. This annex includes furthermore generic facts regarding time and reactor states which is adopted by IEC 61838 [F].

Both IAEA and IEC documents uses the term 'plant state' for two different subjects. On the one hand the term is used to identify the events to be considered for plant operation (like Normal Operation, Anticipated operation occurrences) on the other hand the term is used as status of the plant to be reached after an event has occurred (regarding physical conditions like temperature, pressure, radiation, etc.).

## I. Plant states – events to be considered for 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'. Table 1 gives the IAEA's and IEC's different definition of plant states.

Table 1: Plant states – according to IAEA SSR 2/1 [A] / IEC 61226 (Ed.4 Draft)

Operational states		Accident conditions (AC)			
IAEA SSR 2/1					
Normal operation	Anticipated operational occurrences	Design basis accidents (DBA)		Design extension conditions (DEC)	
					significant degradation of reactor core
IEC 61226 (Ed. 4 – Draft)					
Normal operation	Design basis event (DBE)			Design extension conditions (DEC)	
	Anticipated operational occurrences	??? (old: AC not explicitly considered as design basis accident)	Design basis accidents (DBA)	w/o significant fuel degradation	With core melt

<sup>1</sup> DiD Level 5 is used for emergency preparedness planning purposes

Table 2 includes a proposal of a link of events/PIEs to the WENRA defence-in-depth (DiD) levels [E] and the IAEA plant states<sup>1</sup>.

Table 2: Correlation between DiD levels and allocation of events/PIEs

		Operational States (OS)		Accident Conditions (AC)		
IAEA SSR 2/1		Normal Operation	Anticipated operational occurrences	Design basis accidents (DBA)		Design Extension Conditions
				(without significant fuel degradation)		Severe accidents (with core melting)
WENRA	DiD Level 1	Prevention of Abnormal operation and failure				
	DiD Level 2	Control of Abnormal operation and failure				
	DiD Level 3.a			Control of accident to limit radiological releases and prevent escalation to core...	...damage conditions	
	DiD Level 3.b					
	DiD Level 4					Control of accidents with core melt to limit offsite releases
	DiD Level 5					Mitigation of radi.
Design Base Conditions / Design Extension Conditions		DBC-1 Transients related to normal operation	DBC-2 Anticipated operational occurrences	DBC-3 Infrequent accidents	DBC-4 Limiting accidents (higher frequency) (lower frequency)	DEC-A Reduction of risk and prevention of core meltdown
Frequency		Each event in this category is expected to occur frequently or regularly during operation	Each PIE in this category should be expected to occur one or a few times during plant lifetime	No individual PIE in this category is expected to occur during the plant lifetime, but one or a few PIE within this category should be expected during plant lifetime	PIEs in this category are considered to be possible but are believed to be excluded by the design. Nevertheless, they are considered on order to understand the radiological consequences of limiting accidents	DEC-B Reduction of risk and control of core meltdown
		$f > 1/a$	$f < 10$	$10^{-2}/a < f < 10^{-3}/a$	$f < 10^{-3}/a$	$10^{-4}/a < f < 10^{-5}/a$
						$CDF < 10^{-5}/a, LRF < 5 \cdot 10^{-7}/a$

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

In Table 1 the different type of plant states are identified for the accident conditions (AC) which form the starting point for the next sequence of events.

Figure 1 provides a generic process after initiation of a PIE. In case the safety I&C detect that plant parameter deviate from normal conditions, the safety I&C shall immediately initiated dedicated measure(s) to actuate SSCs. For events with high severity to the plant, the primary target is to reach controlled state, realized automatically by reactor trip and ESFAS functions of the protection system. The controlled state is not a solid state for the plant but depending on the plant design it provides alternatives regarding time and measures to bring the plant to safe state. Depending on the complexity and the time behaviour measures could be realized by I&C safety actuation system or by manual means from the main control room. Safe state is equal to a maintainable state in which the plant could be kept over long period. Plant parameter needs to be monitored and residual heat removal system to be controlled.

The time between the initiation of a postulated event and the achievement of reaching the subsequent events ('controlled state' and 'safe state') is of high importance.

The time frame between the PIE and the 'actuation of process & safety systems' correspond to the response time requirement for the safety I&C plus the required response time of the electrical and mechanical SSCs. This sequence of events shall be (mostly) realized by automatic functions. Afterwards, depending on the new situation inside the plant (corresponding to the level of PIE), the plant could be either return to normal operation state or managed to ensure further on the fundamental safety principles.

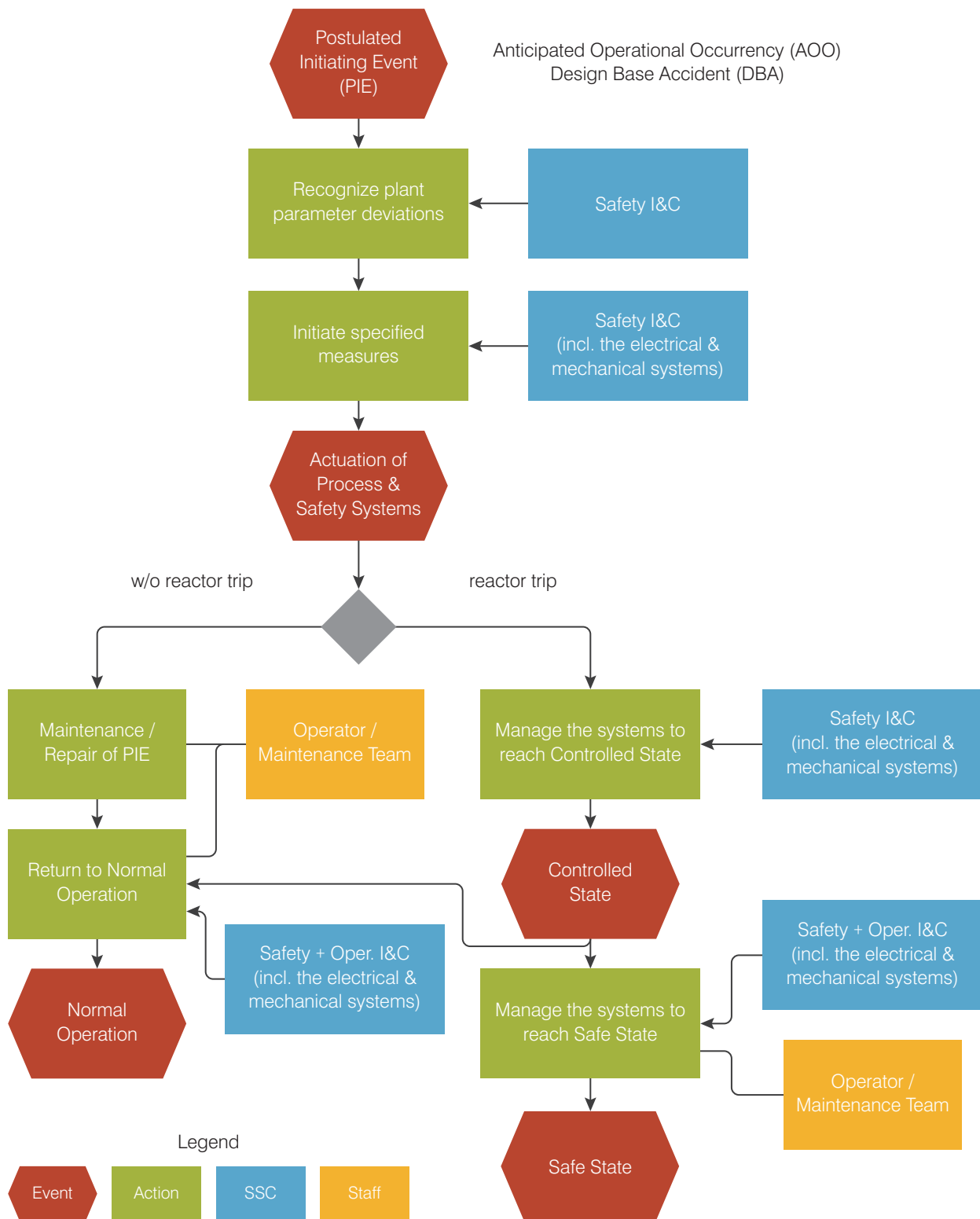


Figure 1: Generic sequence of events/actions/required SSCs after PIE



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

Based on the recommended time frame to reach the controlled state, the instrumentation and control for the required process and safety functionality shall be 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 requests which should be taken considered in the safety and process design.

IEC has drafted in 2009 a technical report concerning the 'Use of Probabilistic Safety Assessment for the classification of functions' – IEC 61838 [F]. This technical report proposes indicative the correlation between the state of the reactor, the timescale and the "group of PIEs" (DBC, DEC, Internal hazards). Table 3 is based on the Table 1 (Classification of I&C FSE†) of IEC 61838 [F].

Table 3: Time and reactor states approach for safety classification – IEC 61838 [F]

	<b><i>I&amp;C FSE to be used in the safety analysis</i></b>			
<i>State of reactor</i>	Initiating Event	Controlled State (Non-hazardous Stable State)	Safe State (Safe Shutdown State)	
<i>Time scale</i>	0h	24h	72h	
<i>PIE group</i>				
<b>DBC</b>	Category A	Category B	Category C	Not classified
<b>DEC</b>	Category C			Not classified
<b>Internal hazards</b>	Category C			Not classified

† FSE – Function(s) and the associated systems and equipment that implement it (them)

### 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 4).

Table 4: 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 4 shows the method specified by SSG-30 for categorization of functions depending on the magnitude of PIE (AOO / DBA / DEC) in relation to the plant states to be reached (controlled stat / safe state) and the severity of consequences (high / medium / low) if the related function is not performed. The use of severity levels supports the process for safety categorization of the required functions. In order to optimize it, a more detailed level of severity (e.g. by probabilistic values) should be identified.

## IV. Definitions of plant states

The following definitions are specified by IAEA. Both IAEA SSR 2/1 [A] and IAEA SSG-30 [B] identifies plant states. The wording is slightly different but with the same intention.

*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])

*The controlled state is for functions where the main focus is on acting automatically or in the short term to considerably reduce the potential for hazard. (IAEA SSG-30 [B])*

*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])

*The safe state tends to focus on longer term functions once the controlled state has been achieved. (IAEA SSG-30 [B])*

IEC 61226 [D]/IEC 61838 [F] uses the term 'non-hazardous stable state' for the 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.*

## V. References

- [A] Specific Safety Requirements No. SSR-2/1, *Safety of Nuclear Power Plants: Design*, International Atomic Energy Agency, STI/PUB/1534, January 2012
- [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*, (under Revision Draft Safety Guide DS431 -supersedes NS-G-1.1 and NS-G-1.3), International Atomic Energy Agency, Draft M step 10 2014-03-21
- [D] IEC 61226:2009 *Nuclear power plants – Instrumentation and control important for safety – Classification of instrumentation and control functions*, International Electrotechnical Commission, 2009
- [E] WENRA Report, *Safety of new NPP designs*, Study by Reactor Harmonization Working Group RHWG March 2013
- [F] IEC/TR 61838:2010, *Use of Probabilistic Safety Assessment for the Classification of Functions*, International Electrotechnical Commission , 2010-02
- [G] American National Standards Institute N18.2, *Nuclear Safety Criteria for the Design of Stationary PWR Plants*, 1973.

# Annex 2 | DICTF actions for “Safety Classification for I&C Systems in Nuclear Power Plants”

<i>Section 3.1 - Inconsistencies between international standards and local regulations</i>		
PP-DICTF-001_AI-1	Each participant in the DICTF shall provide experience and feedback on inconsistencies in safety classification between international standards and local regulations.	<i>DICTF secretariat</i>
PP-DICTF-001_AI-2	The DICTF will encourage the MDEP DICWG to make a more detailed analysis of safety classification requirements among its membership (based on the results of AI-1).	<i>DICTF chairman</i>
<i>Section 3.2 - Ambiguous requirements for safety classification</i>		
PP-DICTF-001_AI-3	<p>The DICTF will develop a working paper on Defence in Depth &amp; Diversity<sup>1</sup> as specified in the CORDEL DICTF 2014-2016 Outlook [14].</p> <p>This paper will include a comparison of the existing definitions and should make a proposal for the generic identification of level of diversity and types of common cause failure. Depending on the safety class and the line of defence-in-depth requested, a proposal for the design should be given. This paper could be used to make recommendations to MDEP, IAEA and the SDOs.</p>	<i>D3 Topic leader (Gregory Droba)</i>
PP-DICTF-001_AI-4	The DICTF will develop a paper that examines the definitions and use of the terms listed in the main text above and will use these results to make recommendations to MDEP, IAEA, and the SDOs.	<i>Consultant (Gary Johnson)</i>
PP-DICTF-001_AI-5	The DICTF will request the MDEP members to provide their definitions of these terms where they exist.	<i>DICTF – chairman (J. Pickelmann)</i>
<i>Section 3.3 - Incomplete rules for categorization of ‘other I&amp;C functions’</i>		
PP-DICTF-001_AI-6	The DICTF will prepare a series of short guides discussing principles for categorization of ‘other I&C functions’.	<i>Consultant (Gary Johnson)</i>
PP-DICTF-001_AI-7	The DICTF will develop proposals to improve the guidance for classifying other I&C functions in order to be considered for the next revision of IEC 61226. These proposals could be discussed in the forthcoming IAEA TECDOC, or included in position papers which may serve as a basis for future international standards.	<i>DICTF - Members</i>

<sup>1</sup> Formally referred to as diversity and common cause failure

<i>Section 3.4 - Criteria for diverse backup systems</i>		
PP-DICTF-001_AI-8	The DICTF will provide a report on identifying the different statements of IAEA, IEC, MDEP and WENRA, including the topic DiD Level 3b (the list will be published on the CORDEL DICTF section of the World Nuclear Association members website).	<i>Safety Classification Topic leader (J. Pickelmann)</i>
PP-DICTF-001_AI-9	The DICTF will request that MDEP develops a common position on safety classification, acceptable diverse technology, radiological acceptance criteria, and use of manual actions for diverse actuation systems.	<i>DICTF Chairman (J. Pickelmann)</i>
<i>Section 5 - Promoting consistency between codes and standards for I&amp;C safety classification</i>		
PP-DICTF-001_AI-10	<p>The draft IAEA TECDOC on SSG-30 will be distributed within the DICTF and discussed to identify comments that should be submitted by CORDEL. Members of the DICTF will participate in the IAEA technical meeting on the TECDOC and provide feedback based on the DICTF positions.</p> <p>DICTF members will participate in the technical review meeting for IAEA SSG-30 TECDOC in 2015 to address the above issues. The working paper(s) on 'safety classification' prepared by the DICTF should be used to communicate the needs identified by vendors and utilities.</p>	<i>DICTF</i>
PP-DICTF-001_AI-11	The first draft of IEC 61226 will be distributed within the DICTF and discussed in order to identify comments that CORDEL participants should consider putting forward to the IEC. DICTF members will participate in the development and review of IEC 61226 to address the above issues. The working paper(s) on 'safety classification' prepared by the DICTF should be used to communicate the needs identified by vendors and utilities.	<i>DICTF - members of SC45A working groups</i>



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

+44 (0)20 7451 1520  
[www.world-nuclear.org](http://www.world-nuclear.org)  
[info@world-nuclear.org](mailto:info@world-nuclear.org)