Kosmowski Kazimierz T.
Gdańsk University of Technology, Gdańsk, Poland

Defence in depth conception in nuclear power plants and requirements for instrumentation and control systems

Keywords

nuclear power plants, defence in depth, instrumentation and control systems, functional safety

Abstract

The aim of this article is to identify and discuss some issues of the safety systems' design for nuclear power plants equipped with the light water reactors using a defence in depth (D-in-D) conception. Because the functional safety solutions play nowadays an important role for the risk control, the basic requirements for the instrumentation and control systems are specified with regard to relevant international standards. For the design purposes the safety functions are categorized into three categories. The I&C systems implementing these functions are assigned to one of three classes that conform to defined design, manufacturing and qualification requirements. These systems are designed to implement functions of relevant categories. Additional design requirements are discussed, including hardware and software aspects, to achieve and maintain the required reliability commensurate with the importance of the safety functions to be performed to reduce risk.

1. Introduction

The primary means for preventing and mitigating the consequences of accidents is "defence in depth" (D-in-D) that is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment.

The *instrumentation and control* (I&C) systems [14] support each of mentioned above levels of defence in depth and each of the barriers identified. In traditional I&C designs, different systems often supported each of the defence lines. Strong independence should be provided between safety systems and safety-related systems. The *engineered safety features* (ESF), such as actuation systems and reactor trip systems, use different actuation logics. In addition, the signal and functional diversity are to be provided so that shared data and environment would not jeopardize multiple lines of defence.

The design of computer-based I&C systems faces now new problems which, if not properly dealt with, may jeopardize independence between lines of defence or independence between redundant elements within a line of defence. The architecture of most computer-based I&C systems is fundamentally different from that of traditional one [4]-[5].

Considering the safety of nuclear power plants (NPPs) at the design stage requires understanding the relations between the safety objectives of given NPP and the requirements for the overall architecture of the I&C systems important to safety as well as the requirements concerning the individual systems.

Some general issues and analyses to be undertaken include: categorisation of functions and classification of systems, separation of systems to become more independent, hardware reliability and software aspects of computer-based systems, defence against dependent failures, e.g. common cause failures (CCFs), and the control room design including relevant interfaces.

Generally, the protection systems are classified as *preventive* and *mitigatory* safeguards that implement relevant safety functions. Some examples of generic safety functions are presented and discussed later on.

The appropriate design of the I&C architecture enables structuring the HMI and the main control room, supplementary control points, local control panels and the emergency control centre, with defined degree of redundancy and the user friendliness necessary to accommodate the constraints from plant operation and maintenance.

The aim of this article is to identify and discuss selected issues of the safety systems' design for

nuclear power plants equipped with the light water reactors in the framework of the D-in-D conception.

2. Defence in depth in industrial hazardous plants and main protection functions

In *Figure 1* the conception of defence in depth (D-in-D) in hazardous plants is presented. The primary means of preventing and mitigating the consequences of potential accidents is thus D-in-D that is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could affect the people or the environment. Five lines of defence in depth are illustrated in this figure for realization of following general functions [19], [23] to:

1) Prevent disturbances, system failures and deviations from normal operations, and keep installation integrity.
2) Detect and intercept deviations from normal operating states to prevent anticipated operational occurrences from escalating to accident conditions.
3) Control the consequences of accident conditions.
4) Confine toxic or radioactive material in the event of severe accidents.
5) Mitigate the consequences of radioactive release.

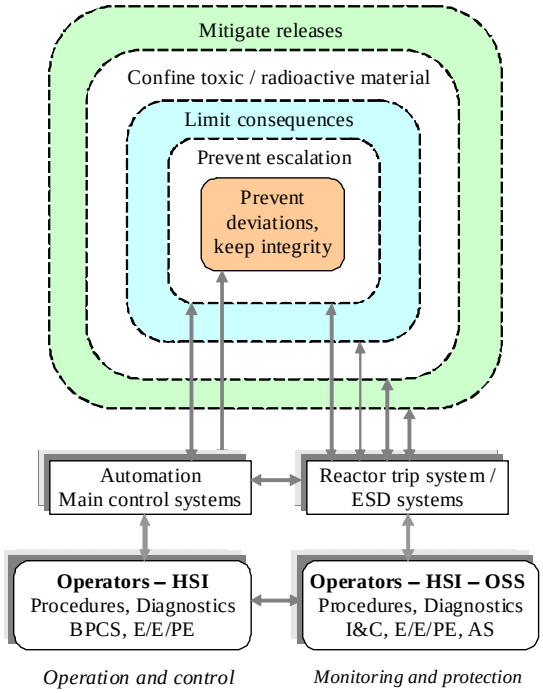

Figure 1. Conception of defense in depth in hazardous plants

The *instrumentation and control* (I&C) systems support each of the above levels of defence in depth and each of the barriers identified. In traditional I&C designs, different systems often supported each of the lines of defence. Strong independence should be provided between the safety systems and safety-related systems. The *engineered safety features* (ESF) actuation systems and reactor trip systems use different actuation logics. In addition, signal and functional diversity are to be provided so that shared data and environment would not jeopardize multiple lines of defence.

The *human system interface* (HSI) and an *operator support system* (OSS) must be designed with regard to relevant methods of *human factors engineering* (HFE) to be effective, reliable and safe [1]. In the process sector, the safety-related systems are named the *safety instrumented systems* (SIS) [13] and in all sectors the electric / electronic / programmable electronic (E/E/PE) systems [12].

The SIS can perform a safety function of *emergency shut-down* (ESD). The main control systems were named the *basic process control systems* (BPCS) [13]. The *alarm system* (AS) can be designed within BPCS or as a separated system having its own the sensor subsystem, the logical subsystem and indicators within the HSI [20].

The design of computer-based I&C systems faces now new problems which, if not properly dealt with, may jeopardize independence between lines of defence or independence between redundant elements within a line of defence. The architecture of most computer-based I&C systems is fundamentally different from that of traditional I&C [4]-[5].

In computer-based systems one or a few computers sometimes process all signals for one channel of both reactor trip and engineered safety features actuation functions. Furthermore, these components must process not only one signal that could induce a failure, but many. It thus constitute a potential for the CCFs that require careful consideration.

Therefore, a failure of an individual component may affect several functions and degrade operation of the I&C supporting two or more lines of defence. The scope of failures in computer-based systems may therefore be greater than in traditional systems unless the computer-based system is carefully designed to avoid this and analysed to identify potential vulnerabilities and confirm that they have been appropriately addressed [4]-[5].

Figure 2 shows a simplified functional overview of the I&C in a NPP. To ensure a safe and reliable plant operation under all plant conditions, the I&C systems have to monitor and control hundreds or thousands of plant parameters. Thus, nuclear power plant I&C systems are complex. Subdividing the plant's I&C according to its functions facilitates understanding of the entire system. The important role plays the human system interface (HIS) to make the plant state

supervision and control more effective and reliable by a team of human operators [3], [22].

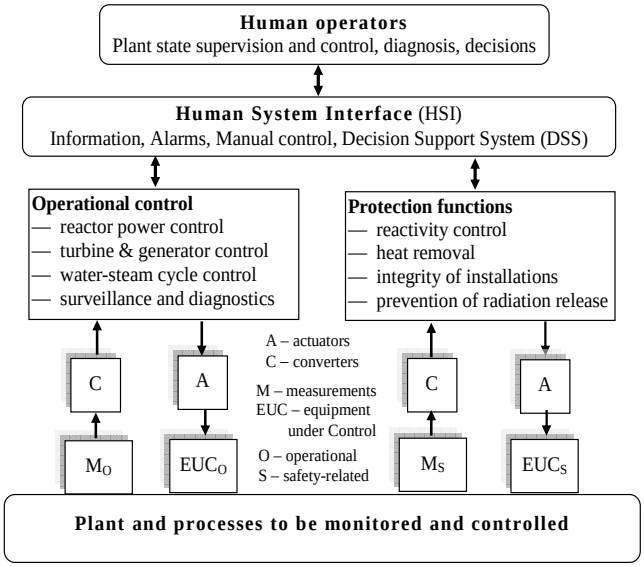

Figure 2. Main operational and protection functions in a nuclear power plant

3. Selected topics of functional safety analysis in nuclear power plants

3.1. General requirements concerning the safety systems

Considering the safety of nuclear power plants (NPPs) at the design stage requires to understand the relations between the safety objectives of the NPP and the requirements for the overall architecture of the I&C systems important to safety as well as the requirements concerning the individual systems. Some general issues and analyses to be undertaken include: categorisation of functions and classification of systems, separation of systems to become more independent, hardware reliability and software aspects of computer-based systems, defence against common cause and dependent failures, and the control room design.

The I&C systems important to safety may be implemented using conventional hard-wired equipment, computer-based (CB) equipment or by using both types of equipment (hybrid I&C systems) [4]-[5], [14]. The I&C systems may also use electronic modules based on complex integrated electronic components such as ASICs (*Application Specific Integrated Circuits*) or FPGAs (*Field-Programmable Gate Arrays*). Depending on the scope and functionality of these components, they may be treated according to the guidance for conventional electronic equipment, or similar to the CB equipment. A part of the guidance for CB equipment is applicable also to the design of equipment with complex electronic components including e.g. re-using of pre-existing designs.

Thus, it is required to evaluate respectively potential design errors in software and complex hardware designs. The scope of the I&C design and its operation in life cycle includes [14]:

A. Specification of requirements for overall I&C: defining requirements for the I&C functions, and associated systems with equipment derived from the safety analysis of the NPP, the categorisation of I&C functions, the plant lay-out and operational context; structuring the overall I&C architecture to divide it into a number of systems that implement I&C functions; identifying of criteria including those related to defence in depth (D-in-D), and to minimise the potential for common cause failure (CCFs); planning the overall architecture of the individual I&C systems.
B. Realisation and planning of the individual I&C systems, particularly the CB systems – this includes differentiation of requirements according to the safety category of the I&C functions to be implemented; the requirements on the system planning include some additional aspects concerning: quality, security, integration, validation, installation, operation, and maintenance.
C. Overall integration and commissioning.
D. Overall operation and maintenance.

Thus, the scope of required analyses includes some basic elements of general functional safety concept given in IEC 61508, however without clearly stated requirements as regards determining the SILs of safety functions and their verifying in probabilistic modelling process of safety systems. This can be explained that the idea of I&C safety stems from the plant safety design base and the plant design framework according to some widely accepted safety principles, formulated in publications of the International Atomic Energy Agency (IAEA) [3]-[8].

A number of individual safety principles have been defined in several IAEA reports and documents including: 75-INSAG-3 (integrated overall safety approach), INSAG-10 [3] (defence in depth in nuclear safety), and IAEA NS-R-1 with regard to *postulated initiating events* (PIEs) to be considered and successive physical barriers to keep radiation exposure to workers, public and the environment within specified limits [8].

Following such approach, the plant design base is specified with regard to appropriate quality and safety level for the plant functions and systems that are necessary to maintain the plant in a normal operating state, and to ensure the correct response to all defined PIEs, and to facilitate the long-term safety

management of the plant following an accident. The I&C design process requires the following inputs from the plant safety design base [14]:

A. the defense in depth (D-in-D) concept of the plant and the groups of functions provided to address PIEs sequences in order to fulfill the safety objectives (in cases where the reliability of a function is required to be very high, the requirements specification for the plant and the I&C stipulate different lines of defence for the same PIE);
B. the functional and performance requirements of the functions of the plant important to safety needed to meet the general safety requirements;
C. the role of automation and prescribed operator actions in the management of anticipated operational occurrences including accident conditions;
D. the human operator task analysis with defining which functions should be assigned to the operators and which to machine (rather a safety-related system);
E. the variables to be displayed for the operator to be used in taking manual control actions;
F. the priority principles between automatic and manually initiated actions, taking into account functional categories and relevant control rooms or other locations.

In the design of I&C some constrains are to be taken into account that concern [14]:

- issues of security;
- operation and maintenance;
- in service testing and maintenance of the I&C systems.

The strategy of in service testing and maintenance proposed can influence the level of redundancy in the I&C systems, e.g. instead of 2oo3 the configuration 2oo4.

In *Table 1* the categories of I&C functions and classes of I&C systems important to safety are presented according to the standard IEC 61226:2009 [11] (*Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*).

Table 1. Categories of I&C functions and classes of I&C systems important to safety

Categories of I&C functions			Classes of I&C systems
A	(B)	(C)	1
	B	(C)	2
		C	3

For category A functions the design of the I&C architecture of systems and subsystems includes a *single failure criterion* (SFC) for all permitted configurations of the systems and the plant. The specification of overall requirements defines any potential dependency between functions which generate constrains on the assignment of functions to I&C systems [14]. This includes:

- the combination of functions to be monitored to control protective actions;
- the combination of functions ensuring defence in depth;
- the combination of functions which constitute a safety group.

The interfaces with the plant and interconnections between the I&C systems are defined as part of the architectural design in order to identify:

- sharing of measurement signals by different functions important to safety;
- the voting of, and priority between, actuation signals from different systems;
- signal paths and equipment that are common to automatic or manual actuation functions in different lines of defence.

The appropriate design of the I&C architecture enables structuring the *human machine interface* (HMI) and the main control room, supplementary control points, local control panels and the emergency control centre, with defined degree of redundancy and the user friendliness necessary to accommodate the constraints from plant operation and maintenance. It includes the priority principles between automatic signals and manually initiated control signals as well as the priority principles between the different HMI systems during normal, abnormal, accident, and post accident operation. It will ensure that relevant information including characteristics of the HSI and time available to the operator for manual control action is consistent with the requirements of the plant design base.

A starting point for human-factor oriented assessment is the analysis of operator tasks and their performance requirements, leading to a proper integration of displays and controls, especially for tasks to be executed more frequently, under time pressure or with increased risk in case of human error. Issues of the human-centered design of control room and safety goal oriented human actions based on the task analysis are discussed in a work [22].

The assignment of functions to systems should be made in such a way to minimise the complexity of class 1 systems. System complexity may be reduced by considering the design approaches as follows:

- avoiding complex algorithms and processing that cannot be clearly defined and validated;

- reducing the number of different functions that are implemented in a system;
- using simple design features to limit the impact of potential complex fault conditions.

However, any reduction in complexity should not result in excessive negative design impacts, such as increased complexity in the overall I&C architecture or reductions in safety-related functionality such as the extent of self test coverage. In particular it concerns the reliability of the application functions.

In the standard IEC 61513 there are not given quantitative reliability criteria, although there is requirement of the reliability assessment (see item 6.2.4.2 – Required analysis, in the standard [14], p. 56). There is only a general statement that the reliability of the application functions performed by the system "shall be justified as adequate", and that the "rigour of the demonstration should be higher for the functions of the highest category".

It is suggested also that the reliability-related demonstration would be based on deterministic criteria completed (based on modelling of the system and/or expert judgement) when appropriate, and by quantitative reliability analysis with the estimation of the contribution of potential hardware failures to the reliability of the function that is determined by probabilistic quantitative analysis with regard to the failure rates of components.

The reliability analysis shall take into account the effects of single failures, CCFs, and potential propagation of failures within systems contributing to the safety group considered. It is required that a quality assurance plant will be established and implemented to cover each of the activities of the system safety life cycle. The requirements for the system quality assurance shall be delivered from ISES GS-G-3.1 and ISO 9001 [7], [14].

It is possible to take credit from evidence of qualification of the hardware and software components, established outside the framework of a plant design or specific application context, e.g. pre-qualification or generic qualification of COTS (*Commercial Off-The-Shelf*) products or of an equipment family, so as to split essential parts of the qualification effort over several projects. Generic qualification may be performed as a joint effort for several NPP projects, or by a vendor of an equipment platform for safety-related applications.

Certification of COTS products to the safety integrity level of SIL 1, 2 or 3 according to the IEC 61508 series [12] by an independent and accredited safety assessor is an example of a form of pre-quantification. Since the IEC 61508 is a generic functional safety standard, such certification provides a good starting point for application-specific qualification of COTS products, and for demonstrating the compliance with the requirements of IEC 61513 and its daughter standards [9]-[11]. The safety requirements concerning software are described also in standards [15]-[16].

3.2. Requirements for the safety systems in the context of systems' classes

A general safety objective for existing nuclear power plants (NPPs), expressed by a target likelihood for the occurrence of severe core damage, is to be below 10^{-4} per plant operating year [a^{-1}]. Implementation of all safety principles for future NPPs may lead to the achievements of an improved goal of no more than 10^{-5} [a^{-1}]. Severe accident management and mitigation measures should reduce the probability of a large off-site release requiring an off-site response by a factor of at least 10 (see IAEA 75-INSAG-3). A major contribution to the safety philosophy is provided by the defence in depth concept [3].

A complementary application of this concept is multiple backup of I&C systems [14]. To minimize the magnitude of a disturbance and to achieve defence in depth, more than one I&C systems may be used, which act progressively as the controlled variable deviates from the desired value. At first, as the variable deviates from normal conditions, non classified control systems take action. Following the action of these control systems, one or more levels of additional control systems important to safety may take action, prior to the actuation of the protection system. If the event grows from a minor operational disturbance to a transient or to a significant transient. At each stage, the purpose is to terminate the event and return the system to normal operation for minor events and to shut down safely for events which become more serious.

The number of I&C systems and their functionality is plant specific. Typical examples of the I&C systems important to safety are as follows:

A. automation and control systems;
B. HMI systems;
C. protection and safety actuation systems;
D. emergency electrical power actuation systems.

As it was mentioned the I&C systems implementing functions important to safety are assigned to one of three classes that conform to defined design, manufacturing and qualification requirements, which make these systems suitable for implementing functions of one or more of the categories A, B or C or unclassified.

Typical classification of these systems based on IEC 61513 is presented in *Table 2*. The HMI system may be assigned to one of class 1, 2, 3 or not classified system. The HMI of class 1 may be restricted to

a few critical indicators and push-buttons in the control room or emergency control room [14].
The requirements for the function with highest category determine the class of the system. In *Table 3* some examples are presented that illustrate assigning the *hardware fault tolerance* (HFT) and the *safety integrity level* (SIL), concerning hardware and software requirements, to categories of functions and classes of safety systems.

Table 2. Typical classification of I&C systems [14]

I&C systems	Class 1	Class 2	Class 3	Not classified
Automation and control systems		x	x	x
HMI systems	x[a]	x	x	x
Protection and safety actuation systems	x			
Emergency electrical power actuation systems	x			

[a] May be restricted to a few critical indicators and push-buttons

Table 3 . Examples of requirements for I&C systems

I&C function category	I&C system class	Hardware fault tolerance (HFT)	Safety integrity level (SIL) of hardware and software
A (B, C)	1	2 (1[a])	4[c,d] (3)[d]
B (C)	2	1[a] (0[b])	3 (2)
C	3	1[a] (0[b])	2 (1)

[a] Fulfilling requirement of single failure criterion (SFC) that is necessary only for category A
[b] Justified when functional redundancy using another system is available
[c] IEC 61226 sets a limit on the reliability that may be claimed for systems which incorporate software to 10^{-4} (this value is on the border of intervals for SIL 4 and 3)
[d] Vital protection systems, e.g. the reactor protection system, designed as hardwired

When the safety integrity level (SIL) of I&C function would be determined based on the risk analysis and assessment then this level is to be verified in the probabilistic modelling process. It includes the I&C systems and human reliability analysis to evaluate the *human error probability* (HEP) in a similar way how it was proposed for the LOPA methodology [23]. Potential dependencies within safety systems including CCFs and required human actions should be taken into account.

For some systems the reliability targets may not be reached for given architecture of I&C systems. In such case it is necessary to ensure greater functional reliability by using additional safety systems that are capable of performing the assigned safety function. Diversity and physical separation of safety systems reduce the possibility of common cause failures. The standard IEC 61513 does not include methodology to deal with such problems. Therefore, adapting of the methodology similar to the layer of protection analysis (LOPA) is of interest for this purpose [23].

4. Basic design issues of protection systems in nuclear power plants

4.1. Classification of safety functions, structures and safety systems

The safety systems that implements various safety functions are named the protection systems. It was explained how to improve the reliability or availability of these systems designing them as redundant, e.g. using configuration of KooN and in some cases using diverse channels when required. Generally, the protection systems are classified as *preventive* and *mitigatory* safeguards that implement relevant safety functions [2], [6].
The preventive safety functions are aimed at preventing failures and abnormal operation. *The mitigatory safety functions* are designed to control abnormalities due to postulated initiating events and to mitigate consequences of potential hazardous events. The role of preventive and mitigatory safeguards in the context of a hazardous situation and then hazardous event is presented in *Figure 3*.

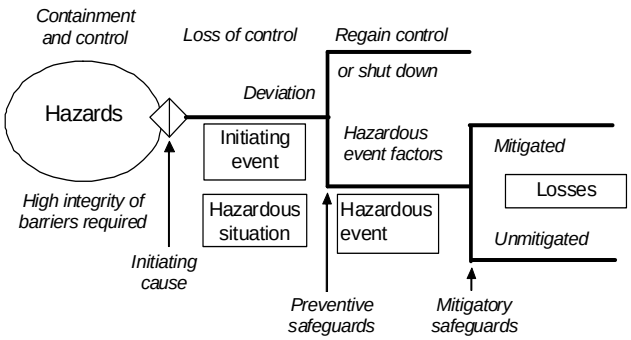

Figure 3. The role of preventive and mitigatory safeguards after an initiating cause (based on [2])

Due to an initiating cause and potential initiating event and a hazardous situation can occur. If preventive safeguards operate as designed the control is regained or the installation has to be shut down to a safe state. If the preventive safeguards do not operate as required, a hazardous event occur that causes some consequences. The level of losses

depend on operation of the mitigative safeguards that implement relevant safety functions. If they operate as required the losses will be mitigated, if not, the losses can be major.

Examples of generic safety functions for the light water reactors (PWR, BWR) are presented in *Table 4*. Three fundamental categories of the safety functions are distinguished as follows [6]:

F1: control of reactivity;
F2: removal of heat from the core; and
F3: confinement of radioactive material.

As it can be seen in *Table 4*, some safety functions can play role of both preventive and mitigatory with assigning them relevant category or categories (F1, F2 and/or F3).

The need to classify equipment in nuclear power plants according to its importance to safety has been recognized since the early days of the reactor design and operation. The existing methods for safety classification of *structures, systems and components* (SSCs) have evolved thanks to lessons learnt during the design and operation of existing nuclear power plants, equipped mainly with *light water reactors*. The purpose of safety classification in a nuclear power plant is to identify and categorize the safety functions and to identify and classify the related SSCs items on the basis of their safety significance [6], [22].

This will ensure that appropriate engineering design rules are determined for each safety class, so that SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected according to standards appropriate to their safety significance. The identification and categorization of safety functions enable classification of related SSCs to ensure required level of safety by meeting associated *quality and reliability targets* or other specified requirements accordingly [6], [22].

It was assumed in the analysis that there are features of all nuclear power plants that are common to all reactor types. For example, that all plants have a series of physical barriers or other barriers for the retention of the inventory of radioactive material and that all such barriers have to meet a set of requirements that govern the safe operation of the plant [6].

Furthermore, all plants are assumed to require certain physical processes to operate, including cooling of the fuel, limitation of chemical degradation and mechanical processes to prevent failures of the barriers retaining radioactive material, although in different designs, each of these aspects may be of different relative importance [6]. Some examples of engineering design rules for SSCs is discussed further.

Table 4. Examples of generic safety functions considered for light water reactors (based on [6])

Safety functions*	Preven-tive	Mitiga-tory
(1) to prevent unacceptable reactivity transients	F1	
(2) to maintain the reactor in a safe shutdown condition after all shutdown actions	F1	F1
(3) to shut down the reactor as necessary to prevent anticipated operational occurrences from leading to design basis accidents and to shut down the reactor to mitigate the consequences of design basis accidents	F1	F1
(4) to maintain sufficient reactor coolant inventory for core cooling in and after accident conditions not involving the failure of the reactor coolant pressure boundary		F2
(5) to maintain sufficient reactor coolant inventory for core cooling in and after all postulated initiating events considered in the design basis		F2
(6) to remove heat from the core after a failure of the reactor coolant pressure boundary in order to limit fuel damage		F2
(7) to remove residual heat in appropriate operational states and accident conditions with the reactor coolant pressure boundary intact	F2	F2
(8) to transfer heat from other safety systems to the ultimate heat sink		F2
(9) to ensure necessary services (such as electrical, pneumatic, hydraulic power supplies, lubrication) as a support function for a safety system	F1, F2, F3 Suppor-ting	F1, F2, F3 Suppor-ting
(10) to maintain acceptable integrity of the cladding of the fuel in the reactor core	F3	F3
(11) to maintain the integrity of the reactor coolant pressure boundary	F2, F3	F2, F3

*) Three fundamental categories of safety functions of the light water reactors (PWR, BWR): F1: control of reactivity; F2: removal of heat from the core; F3: confinement of radioactive material

Examples of engineering design rules and requirements imposed on the SSCs are presented in *Table 5* for preventive safety functions and *Table 6* for mitigatory safety functions.

It is postulated that the method for classifying the safety significance of items important to safety shall be based primarily on deterministic methodologies complemented where appropriate by probabilistic methods, with account taken of following factors [6]:

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

(2) the consequences of failure to perform the safety function;
(3) the frequency at which the item will be called upon to perform a safety function;
(4) the time following a *postulated initiating event* (PIE) at which, or the period for which, it will be called upon to operate.

The design should be such as to ensure that any interference between items important to safety shall be prevented. In particular any failure of items important to safety in a system classified in a lower class will not propagate to a system classified in a higher safety class. Main steps in classifying SSCs are illustrated in *Figure 4*.

For a specific plant, prerequisites for classifying all SSCs according to their safety significance should be based upon [6]:

- a list of all postulated initiating events (PIEs) considered in the plant design basis;
- the identification of the safety functions needed to achieve the fundamental safety goals for the different plant states.

The safety functions that prevent and mitigate these postulated initiating events should be derived at an adequate level of detail in order later to identify SSCs to perform these safety functions. These safety functions will be specific to each plant. Some plant specific safety functions can be defined to cover more than one postulated initiating event [6].

The plant specific safety functions which are required in order to fulfil the fundamental safety functions during *normal operation* should be also identified. These *preventive plant specific safety functions* are aimed at avoiding failures of SSCs that may cause initiating events and abnormal operations, and to maintain *the integrity of main confinement barriers*.

The primary *causes of postulated initiating events* may be credible *equipment failures* and *operator errors* or *human induced or natural events*. Grouping or bounding of postulated initiating events should be performed and assessed during the design prior to the safety classification process using deterministic safety analysis and where appropriate, probabilistic safety assessments [6], [8].

The plant specific safety functions are to be categorized into a limited number of categories on the basis of their safety significance, with account taken of aspects such as [6]:

- the consequences of a potential failure of the safety function;
- the frequency of occurrence of the postulated initiating events they prevent or mitigate;
- the time following a postulated initiating event at which they will be required to perform;
- the period following a postulated initiating event they will be required to perform (e.g. the time for achieving a controlled state or safe shutdown state).

The identification of SSCs or groups of SSCs that work together to perform the plant specific safety functions is also required.

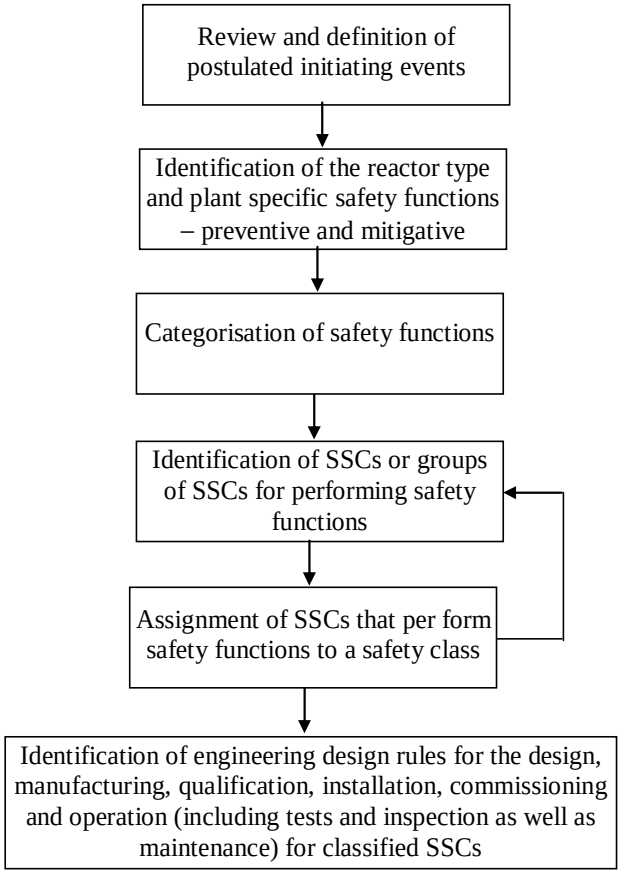

Figure 4. Main steps in classifying SSCs [6]

The nature of the steps taken at each stage can vary according to regulatory requirements and the plant design process. Different methods for the safety classification of SSCs have been used for different types of reactors and in different countries for operating nuclear power plants and for new designs [6]. The differences in approaches have, for instance, led to a different number of classes or different grouping of safety functions [5].

In this work the classification was assumed to be consistent with the functional safety concept for applying to nuclear power plants according to the international standards IEC 61226 [11] and IEC 61513 [14].

Table 5. Examples of engineering design rules and requirements imposed on SSCs for implementing preventive safety functions (based on [6])

	Implementing preventive safety functions		
Engineering design rules and codes (requirements)	Safety class 1	Safety class 2	Safety class 3
Quality assurance	nuclear grade	nuclear grade	commercial grade[1] or specific
Environmental qualification	harsh or mild[2]	harsh or mild	harsh or mild
Pressure retaining components (example codes)[3]	high pressure: C1 low pressure: C2	high pressure: C2 low pressure: C3	high pressure: C3 low pressure: C4
Electrical components (IEEE)	1E	1E	non 1E
Instrumentation and control (I&C) – category (IEC 61226)[4]	A or B	B or C	C
I&C – safety integrity level SIL (IEC 61508)	SIL 4 or 3	SIL 3 or 2	SIL 1
I&C – software quality (IEC 61508 and ISO/IEC 15504 models)	for SIL 4 or 3 SAFE+	for SIL 3 or 2 SAFE+	for SIL 1 SAFE
Seismic qualification	seismic category 1	seismic category 1	specific

Table 6. Examples of engineering design rules and requirements imposed on SSCs for implementing mitigatory safety functions (based on [6])

	Implementing mitigatory safety functions		
Engineering design rules and codes (requirements)	Safety class 1	Safety class 2	Safety class 3
Quality assurance	nuclear grade	nuclear grade	commercial grade[1] or specific
Environmental qualification	harsh or mild[2]	harsh or mild	harsh or mild
Pressure retaining components (example codes)[3]	high pressure: C2 low pressure: C3	C3	C4
Electrical components (IEEE)	1E	1E	non 1E
Instrumentation and control (I&C) – category (IEC 61226)[4]	A	B	C
I&C – safety integrity level SIL (IEC 61508)	SIL 3	SIL 2	SIL 1
I&C – software quality (IEC 61508 and ISO/IEC 15504 models)	for SIL 3 SAFE+	for SIL 2 SAFE+	for SIL 1 SAFE
Seismic qualification	seismic category 1	seismic category 1	specific

[1] Commercial grade practices need to demonstrate that the SSC is capable of performing its safety function consistent with its categorization

[2] Harsh or mild environmental conditions; SSCs need to be qualified for normal operation and for postulated initiating events, depending on the environmental conditions at their location in the plant

[3] C1 indicates quality level 1, for example level 1 of ASME III or RCC-M (e.g. reactor pressure boundary); C2 indicates quality level 2. for example level 2 of ASME III or RCC-M (e.g. emergency core cooling system); C3 indicates quality level 3, for example level 3 of ASME III or RCC-M (e.g. component cooling water system, essential service water system); C4 is a quality class comprising non nuclear grade pressure retaining components with special requirements (for example seismic design, quality requirements): components in class C4 can be designed in accordance with any pressure retaining component design code, with account taken of special requirements (e.g. for the fire system)

[4] Category A denotes functions that play a principal role in the achievement or maintenance of plant safety to prevent design basis accidents from leading to unacceptable consequences. Category B denotes functions that play a complementary role to the category A functions in the achievement or maintenance of plant safety, particularly functions

4.2. Application of engineering rules for SSCs including I&C

Engineering design rules are related mainly to the three characteristics of *capability*, *dependability* (*reliability*) and *robustness* [6]:

- *capability* is the ability of an SSC to perform its designated safety function as required, with account taken of uncertainties;
- *dependability* (reliability) is the ability of an SSC to perform the required plant specific safety function with a sufficiently low failure rate consistent with the safety analysis;
- *robustness* understood as the ability of an SSC to ensure that no operational loads or loads caused by postulated initiating events will adversely affect the ability of the safety functional group to perform a designated safety function.

Quality assurance or management system requirements for the design, qualification, procurement, construction, inspection, installation, commissioning, operation, testing, surveillance and modification of SSCs should be assigned on the basis of their safety class, in accordance with specified requirements [6]-[7]. Examples of engineering design rules and requirements imposed on SSCs are presented in *Table 5* for preventive safety functions and *Table 6* for mitigatory safety functions.

The environmental qualification of SSCs should be determined in accordance with the conditions associated with normal operation and for postulated initiating events where the SSCs may be called on to operate. At a minimum, environmental qualification should include consideration of humidity, temperature, pressure, vibration, chemical effects, radiation, operating time, ageing, submergence, electromagnetic interference, radio frequency interference and voltage surges, as applicable [6].

The instrumentation and control (I&C) categories are taken according to IEC 61226. It is proposed that the software quality in programmable control and protection systems will be achieved for developing models with regard to requirements given in international standards IEC 61508 and ISO/IEC 15504.

It is proposed, that safety integrity level (SIL) verification for the I&C system of given class that implements defined safety function will be carried out according to requirements given in IEC 61508.

4.3. Design measures to achieve a high reliability of safety functions

Appropriate design measures shall be used [17], [19], [22], if necessary in combination, to achieve and maintain the required reliability commensurate with the importance of the safety functions to be performed.

Redundancy, understood as the use of more than the minimum number of sets of equipment to accomplish a given safety function, shall be employed for improving the reliability and to meet the single-failure criterion in systems performing F1 functions and certain F2 functions. Redundancy enables failure or unavailability of one set of equipment to be tolerated without loss of the function. For the purposes of redundancy, identical or diverse components may be used. The assessment of the degree of redundancy required should take account of the requirements of the SFC, and of the requirements resulting from the PSA results. The redundancy requirements for *passive systems* may be less than those for active systems. However, many passive systems rely on the correct functioning of components such as check valves or batteries. The reliability of such components needs to be assessed in determining redundancy requirements.

Prevention of common-cause failures (CCFs), i.e. *f*ailure of a number of devices or components to perform their functions may occur as a result of a single specific event or cause. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a man-induced event, saturation of signals, a change in ambient conditions, or an unintended cascading effect from any other operation or failure within the plant. Appropriate measures should be taken as far as reasonably practicable in the design to minimise such effects.

While no formal lower reliability limit is provided for CCF of non-diverse systems, the reliability required of a particular function will be an important aspect of the overall assessment of the requirement for diversity for probabilistic treatment of CCF. The examination for potential CCFs shall include passive features that may be sensitive to less predictable behaviour. The potential causes of CCFs shall be examined to determine where *independence, physical separation* and *diversity* are required.

*Physical separation in the s*ystem layout and design utilising the principles of physical separation shall be used as far as reasonably practicable to increase assurance that independence will be achieved, particularly in relation to certain CCF. These principles include:

- separation by distance, arrangement, orientation etc.;
- separation by barriers;
- separation by a combination of these.

The choice of means of physical separation will depend on the events to be considered in the design basis, e.g. the effects of fires, chemical explosions, aircraft crashes, missiles, flooding, temperature, humidity etc.

Autonomy in respect of electric power supply of the control systems

The period of independence of the installation in relation to external electrical power supplies shall be at least 72 hours; this applies to *normal operation* as well as *incident conditions*, *accident conditions* and *design extension conditions* (DEC). The period of 72 hours is defined as the longest period after which it is considered that at least one external high-power source should have been re-established, irrespective of the cause of the loss. This period applies both to loss of external supplies in normal operation and to fault sequences with loss of external supplies.

Where the plant relies on the safety category I AC supplies, if the *station black out* cannot be shown to be of sufficiently low frequency (i.e. $<10^{-7}$ per year), then the independence of the installation to such a loss should be such that *criteria for limited impact* (CLI) are not exceeded with a probability of $>10^{-7}$ per year, making reasonable assumptions about the timescale for the recovery of at least one AC power source. The reliability and restoration time for grid supplies will be supplied by the utility for a given site. The batteries which are required to perform F1 functions shall be sized so that their expected autonomy is at least 2 hours following any *design basis condition* (DBC), without recharging.

It is evident that most of specified above safety related criteria and requirements for nuclear power plants based on the European Utility Requirements (EURs) are directly or indirectly related to the protection systems that can be designed with regard to functional safety principles given in international standards [9]-[11], [14]-[15]. From the functional safety point of view the SIL level of the I&C control and protection systems implementing the preventive or mitigatory safety functions is of interest (see *Tables 5-6* and requirements concerning the hardware and software). The analyses have shown that for category A the I&C systems initiating defined safety functions should be designed in most cases as the configuration of 2oo4.

5. Conclusion

The primary means of preventing and mitigating the consequences of accidents is *defence in depth* (D-in-D) that is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. These issues have been discussed in the context of functional safety concept presented in the generic standard IEC 61508, sector standard IEC 61513 concerning nuclear power plants and other related standards.

The *instrumentation and control* (I&C) systems support each of the above levels of defence in depth and each of the barriers identified above. In traditional I&C designs, different systems often supported each of the lines of defence. Strong independence should be provided between safety systems and safety-related systems. The *engineered safety features* (ESF) actuation systems and reactor trip systems use different actuation logics. In addition, signal and functional diversity are to be provided so that shared data and environment would not jeopardize multiple lines of defence.

The design of computer-based I&C systems faces now new problems which, if not properly dealt with, may jeopardize independence between lines of defence or independence between redundant elements within a line of defence. The architecture of most computer-based I&C systems is fundamentally different from that of traditional I&C.

Considering the safety of nuclear power plants (NPPs) at the design stage requires understanding the relations between the safety objectives of the NPP and the requirements for the overall architecture of the I&C systems important to safety as well as the requirements concerning the individual systems.

Some general issues and analyses to be undertaken include: categorisation of functions and classification of systems, separation of systems to become more independent, hardware reliability and software quality aspects of computer-based systems, defence against common cause and dependent failures, and the control room design including relevant interfaces.

Generally, the protection systems are classified as *preventive* and *mitigatory* safeguards that implement relevant safety functions. Some examples of generic safety functions have been presented. The appropriate design of the I&C architecture enables structuring the *human machine interface* (HMI) and the main control room, supplementary control points, local control panels and the emergency control centre, with defined degree of redundancy and the user friendliness necessary to accommodate the constraints from plant operation and maintenance.

The aim of this article was to identify and discuss only selected issues of the safety systems' design, mainly instrumentation and control systems (I&C) for nuclear power plants equipped with the light water reactors. These are relatively new issues, but very important, because the technology of programmable control and protection systems are

becoming of increasing interest in the design of nuclear power plants. There are, however, still some problems that require dealing with systematically in further research.

An important problem, which requires further research, is related to the necessity of integration of the safety and security analyses in the design and operation of the programmable control and protection systems of hazardous plants. The research works have been undertaken and some proposals developed for understanding and solving these issues [18]-[20]. New research efforts are also needed aimed at developing the methods for verifying the software quality and information security in industrial computer systems and networks, in particular those performing safety functions in nuclear power plants.

References

[1] Froome, P. & Jones, C. (2002). *Developing Advisory Software to comply with IEC 61508. Contract Research Report 419,* Series: HSE Books.

[2] Guidelines for Hazard Evaluation Procedures. (2008). New York: Center for Chemical Process Safety, Wiley-Interscience, A John Wiley & Sons.

[3] IAEA INSAG-10 (1996*).* Defense in Depth in Nuclear Safety. A report by the International Nuclear Safety Group. International Atomic Energy Agency, Vienna.

[4] IAEA Nuclear Energy Series No NP-T-3.10 (2010). Integration of Analog and Digital Instrumentation and Control Systems in Hybrid Control Rooms. International Atomic Energy Agency, Vienna.

[5] IAEA Nuclear Energy Series No NP-T-3.12 (2011). Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants. Vienna: International Atomic Energy Agency.

[6] IAEA Safety Guide (draft) (2011). Safety classification of structures, systems and components in nuclear power plants. International Atomic Energy Agency, Vienna. Draft safety guide DS367, ver. 6.2.

[7] IAEA Safety Reports Series No 22 (2002). Quality Standards: Comparison between IAEA 50-C/SG-Q and ISO 9001:2000. International Atomic Energy Agency, Vienna.

[8] IAEA-TECDOC-719 (1993). Defining initiating events for purposes of probabilistic safety assessment. International Atomic Energy Agency, Vienna.

[9] IEC 60880 (2006). Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions. International Electrotechnical Commission, Geneva.

[10] IEC 60987 (2007). Nuclear power plants, Instrumentation and control important to safety, Hardware design requirements for computer-based systems. International Electrotechnical Commission, Geneva.

[11] IEC 61226 (2009). Nuclear power plants, Instrumentation and control important to safety – Classification of instrumentation and control functions. International Electrotech-nical Commission, Geneva.

[12] IEC 61508 (2010). Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems. *Parts 1–7,* International Electrotechnical Commission, Geneva.

[13] IEC 61511 (2005). Functional safety: Safety Instrumented Systems for the process industry sector. Parts 1–3, International Electrotechnical Commission, Geneva.

[14] IEC 61513 (2011). Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems. International Electrotechnical Commission, Geneva.

[15] IEC 62138 (2004). Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions. International Electrotechnical Commission, Geneva.

[16] IEC 62280 (2002). Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in closed transmission systems. International Electrotechnical Commission, Geneva.

[17] Kosmowski, K.T. (2003). *Risk analysis methodology for reliability and safety management of nuclear power plants* (in Polish). Monografie 33. Gdańsk University of Technology Publishers.

[18] Kosmowski, K.T. (2012). Current challenges and methodological issues of functional safety and security management in hazardous technical systems. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars*, 3, 1, 39–51.

[19] Kosmowski, K.T. (2013). *Functional safety and reliability analysis methodology for hazardous industrial plants*. Gdańsk University of Technology Publishers.

[20] Kosmowski, K.T. (2013). Problems in designing and operating the functional safety solutions of higher integrity levels. Journal of Polish Safety

and Reliability Association, Summer Safety and Reliability Seminars, 4, 1, 83–99.

[21] Kosmowski, K.T. (2014). *Human factors and functional safety analysis in designing the control rooms of industrial hazardous plants*. Springer-Verlag Book/Volume of Advances in Intelligent Systems and Computing, Berlin.

[22] Kosmowski, K.T. (Ed.) (2007*). Functional Safety Management in Critical Systems*. Publishing House of Gdansk University of Technology.

[23] LOPA (2001): Layer of Protection Analysis, Simplified Process Risk Assessment. Center for Chemical Process Safety. American Institute of Chemical Engineers, New York.