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

Problems in designing and operating the functional safety solutions of higher integrity levels

Keywords

functional safety, control and protection systems, dependent failures, layer of protection, human factors

Abstract

The aim of this article is to identify and discuss some problems that have been encountered in designing and operating the functional safety solutions of higher safety integrity levels (SIL 3 and SIL 4) in the light of analyses outlined in a new version of the international standard IEC 61508:2010. Examples of such solutions are the *electric / electronic / programmable electronic systems* (E/E/PESs) and the *safety instrumented systems* (SISs) being designed and operated respectively according to IEC 61508 and IEC 61511 in the system safety life cycle. The role of *functional safety solutions* is effective reducing and controlling the individual and/or societal risk with regard to tolerable levels defined. Some aspects of potential influence of danger failures of the E/E/PESs or SISs on the plant safety are considered. The influence of common cause failures (CCFs) and dependent failures in the context of the layer of protection analysis is also discussed.

1. Introduction

The functional safety is to be considered as a part of general safety, which depends on the proper response of the control and/or protection systems. The concept of functional safety was formulated in international standard [11], [13] and is applied in the process of design and operation of safety-related *electric, electronic and programmable electronic* (E/E/PE) *systems* [11] or *safety instrumented systems* (SISs) [12] used in the process industry. These systems perform specified functions to ensure that risk is reduced and maintained at acceptable level.

Two different requirements are to be specified to ensure appropriate level of functional safety [11]:

- the requirements imposed on the performance of safety functions,
- the safety integrity requirements (the probability that the safety functions are performed in a satisfactory way within a specified time).

The requirements concerning performance of safety functions are determined with regard to hazards identified and potential accident scenarios, while the safety integrity level (SIL) requirements stem from the results of the risk analysis and assessment taking into accounted the risk criteria specified [11], [17].

Two categories of operation modes are usually considered in functional safety analysis: (1) *low*, and (2) *high* or *continuous* [11]. A low demand mode is usually found in the process industry systems [5, 12, 21, 23] but high or continuous ones appear in the machinery or transportation systems [17].

This article deals with current challenges and methodological issues of functional safety analysis. There are still methodological challenges concerning the functional safety analysis and management in the life cycle. They are related to the issues of potential hardware danger failures, software faults, common cause failures (CCFs), dependencies of equipment and barriers, human errors, organisational deficiencies, security aspects, etc. [2], [3], [15], [16], [19].

The primary objective of functional safety management is to reduce the risk associated with operation of hazardous installation to an acceptable level introducing a set of defined safety functions (SFs) that are implemented using mentioned programmable control and protection safety-related systems (S-RSs).

The human-operator contributes to realization of safety functions through relevant *human system interface* (HSI), which is to be designed to achieve safety goals during abnormal situations taking into

account functions of basic control system and S-RSs, such as E/E/PESs or SISs within protection layers. There is current issue how to design an independent *alarm system* (AS) [7], [18].
These issues are especially important for industrial installations and hazardous plants, such as chemical installations [21], [23] and nuclear reactors [8], [9].

2. Functional safety concept for risk reduction and control in hazardous plants

2.1. Safety functions and safety-related systems

Risk is defined as a combination of the probability of occurrence of harm and the severity of that harm. *Tolerable risk* is risk which is accepted in a given context based on the current values of society. *Residual risk* is understood as risk remaining after protective measures have been taken.
The electrical/electronic/programmable electronic system (E/E/PES) is a system for control, protection or monitoring based on one or more electrical / electronic / programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices [11].
Equipment under control (EUC) control system is a system that responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner.
EUC (*equipment under control*) *risk* is a category of risk arising from the EUC or its interaction with the EUC *control system*. *Target risk* is such risk that is intended to be reached for a specific hazard taking into account the EUC risk together with the E/E/PE S-RS and the other risk reduction measures [11].
Safety is defined as freedom from unacceptable risk. *Functional safety* is part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures.
An important term concerning the functional safety concept is the *safety integrity* [11], understood as the probability that given safety-related system (S-RS) will satisfactorily perform required safety function (SF) under all stated conditions within given period of time.
For the E/E/PES or SIS performing safety functions two probabilistic criteria are defined (*Table 1*) for consecutive SILs namely [11]:

- the average probability of failure PFD_{avg} to perform the safety-related function on demand for given system operating in a *low demand mode*, or
- the probability of a dangerous failure per hour *PFH* (the frequency) for given system operating in *high demand or continuous mode* of operation.

The *safety integrity level* (SIL) is a discrete level (from 1 to 4) for specifying the safety integrity requirements of given safety-related function to be allocated using the E/E/PE system [11] or the SISs [12]. The safety integrity of level 4 (SIL4) is a highest level, which requires a complex system architecture consisting of redundant subsystems [17].

Table 1. Safety integrity levels and probabilistic criteria to be assigned for safety functions operating in low demand mode or high/continuous mode

SIL	PFD_{avg}	*PFH* [h^{-1}]
4	[10^{-5}, 10^{-4})	[10^{-9}, 10^{-8})
3	[10^{-4}, 10^{-3})	[10^{-8}, 10^{-7})
2	[10^{-3}, 10^{-2})	[10^{-7}, 10^{-6})
1	[10^{-2}, 10^{-1})	[10^{-6}, 10^{-5})

Thus, the E/E/PE safety-related systems (S-RSs) operating in two modes of operation can be characterised as follows[11]:

– for a low demand mode of operation, the lower limit is set at an average probability of dangerous failure on demand on the level of 10^{-5},
– for a high demand or a continuous mode of operation, the lower limit is set at an average frequency of dangerous failure on the level of 10^{-9} [h^{-1}],
– requirements for the avoidance and control of systematic faults are given, which are based on experience and judgement gained from practical knowledge,
– a broad range of principles, techniques and measures to achieve functional safety for E/E/PE or SIS S-RSs are defined.

However, the concept of *"fail safe"* is not applied which may be of value only when the failure modes are well defined and the level of complexity is relatively low; the concept of *fail safe* was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard IEC 61508 [11].
The E/E/PE safety-related system shown in *Figure 1* consists of following subsystems: (A) input devices (sensors, transducers, converters *etc.*), (B) logic device, *e.g.* PLC (*Programmable Logic Controller*) and (C) output devices including the equipment under control (EUC).

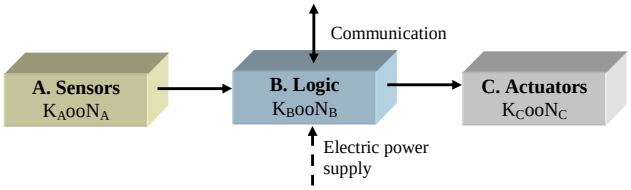

Figure 1. General architecture of E/E/PES or SIS for realization of safety functions

The *architecture* is a specific configuration of hardware and software elements in a system. The architecture of these subsystems is elaborated and determined during the design process of S-RS. Each logic controller comprises the central processor unit (CPU), input modules (digital or analog) and output modules (digital or analog). The E/E/PE subsystems have generally KooN architecture, *e.g.*, 1oo1, 1oo2, 1oo3 or 2oo3 [11], [17].
Fault tolerance is understood as ability of a functional unit to continue performing a required function in the presence of faults or errors [11].

2.2. Safe and danger failures of elements, subsystems and systems

Failure occurs at the moment of termination of the ability of a functional unit to provide a required function or operation [11].
Random hardware failure is a failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware.
Systematic failure is understood as a failure, related in a deterministic way to a certain cause that can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.
Safe failure is the failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that [11]:

a) results in the spurious operation of the safety function to put the EUC into a safe state or maintain a safe state; or
b) increases the probability of the spurious operation of the safety function to put the EUC into a safe state or maintain a safe state.

Dangerous failure is a failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that [11]:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,
b) decreases the probability that the safety function operates correctly when required.

The safe (S) or dangerous (D) failure can be detected (d) or undetected (u). *Figure 2* shows the elements of the failure intensity λ, which can be divided into safe (S) and danger (D) and further: safe detected (Sd), safe undetected (Su), danger detected (Dd), danger undetected (Du). In this figure FS is a safe failure fraction, and DC is diagnostic coverage of dangerous failures. The diagnostic coverage for safe failures is denoted DC_{SD}.
The failure intensity of interest can be easily calculated with regard to the tree presented in *Figure 2*. For example the danger undetected failure intensity can be calculated from the formula

$$\lambda_{Du} = \lambda(1-FS)(1-DC) \tag{1}$$

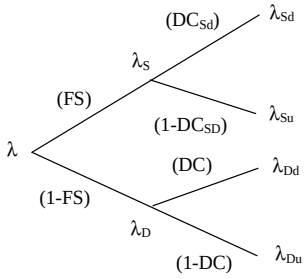

Figure 2. Elements of failure intensity in analysis of the protection system components and subsystems

For the redundant safety-related systems two probabilistic measures are often calculated, namely the average probability of failure on demand PFD_{avg} and the average probability of danger failure per hour *PFH*. The probabilistic models proposed should include parameters related to potential common cause failure.

2.3. Common cause failures

Common cause failure (CCF) is a failure, that is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure. The multiple failures may occur simultaneously or over a period of time. CCFs are a category of dependent failures [11].
Various analytic probabilistic models of E/E/PESs or SISs are proposed in the literature [11], [12], [17]. The CCF contribution in the average probability of failure on demand PFD_{avg} or the average probability of danger failure per hour PFH are usually incorporated using the β-factor method [11].
The scope of the methodology is usually limited to common cause failures within hardware. The reasons for this include the following [11]:

– the β-factor and shock models relate the probability of common cause failure to the probability of random hardware failure;
– reporting of common cause failures is generally limited to hardware failures, the area of most concern to the manufacturers of the hardware.

It is worth to mention that the probability of CCFs which involve the system as a whole depends on the complexity of the system (possibly dominated by the user software) and not on the hardware alone.

Because sensors, logic subsystems and final elements are subject to different environmental conditions and diagnostic tests with varying levels of capability, the analyses should be applied to each of these subsystems separately. For example, the logic subsystem is more likely to be in a controlled environment, whereas the sensors and final elements (e.g. actuators) may be mounted outside being exposed to various environmental stressors. On the other hand the programmable electronic channels have the potential for carrying out sophisticated diagnostic testing functions. These are characterized as follows [11]:

– have a high diagnostic coverage within the channels;
– monitor additional redundancy channels;
– have a high repetition rate; and
– in an increasing number of cases, also monitor sensors and/or final elements.

Thus, it is possible that a large fraction of common cause failures do not occur concurrently in all of the affected channels. Therefore, if the repetition frequency of the diagnostic tests is sufficiently high, a large fraction of common cause failures can be revealed and, hence, avoided before they affect all available channels [11].

Not all properties of a multi-channel system, that has a bearing on its immunity to common cause failures, can be evaluated by diagnostic tests. Those features related to diversity or independence are more effective. Any feature which is likely to increase the time between channel failures in a non-simultaneous common cause failure (or reduce the fraction of simultaneous common cause failures) increases the probability of the diagnostic tests detecting the failure or failures to make the plant more safe.

Therefore, the features relating to immunity to common cause failures are divided into: (1) X - those whose effect is thought to be increased by the use of diagnostic tests and (2) Y - those whose effect is not [11]. A method for scoring factors based on the expert opinions which influence the β-factor is described in the standard IEC 61508:2010.

Although, for a three-channel system, the probability of common cause failures which affect all three channels is likely to be slightly lower than the probability of failures which affect two channels, it is assumed, in order to simplify the β-factor method, that the probability is independent of the number of affected channels, i.e. it is assumed that if a CCF occurs it affects all channels.

Because there is no known data on hardware-related common cause failures available for the calibration of the method, the table 2 below was proposed that consists of β-factors evaluated by experts for some configurations KooM different than 1oo2 [11].

Table 2. Evaluation of β-factor for a E/E/PE system of different KooM configurations

KooM		M		
		2	3	4
K	1	β	0.5β	0.3β
	2	-	1.5β	0.6β
	3	-	-	1.75β

If we consider the effect of common cause failures on a multi-channel system without diagnostic tests running within each of its channels using the β-factor model, the probability of dangerous (D) common cause failures per time unit (hour) is

$$PFH_{CCF} = \lambda_D \beta \tag{2}$$

where

- λ_D is the probability of dangerous random hardware failures per unit time for each individual channel and
- β is the β-factor in the absence of diagnostic tests, i.e. the fraction of single-channel failures that affect all channels.

It was assumed that common cause failures affect all channels, and that the span of time between the first channel and all channels being affected is small compared to the time interval between successive common cause failures.

Suppose now that there are diagnostic tests running in each channel which detect and reveal a fraction of the failures. We can divide all failures into two categories [11]: (1) those that lie outside the coverage of the diagnostic tests (and so can never be detected) and (2) those that lie within the coverage (so they would be detected by the diagnostic tests).

The overall probability per time unit of the system failure due to dangerous common cause failures is then given by following formula:

$$PFH_{CCF}^{diag} = \lambda_{Du} \beta + \lambda_{Dd} \beta_D \tag{3}$$

where

– λ_{Du} is the probability of an undetected failure of a single channel, i.e. the probability of failures

which lie outside the coverage of the diagnostic tests; clearly, any reduction in the β-factor resulting from the repetition rate of the diagnostic tests cannot affect this fraction of the failures;
- β is the common cause failure factor for undetectable dangerous faults, which is equal to the overall β-factor that would be applicable in the absence of diagnostic testing;
- λ_{Dd} is the probability of a danger detected failure of a single channel, i.e. the probability of failures of a single channel that lie within the coverage of the diagnostic tests; here, if the repetition rate of the diagnostic tests is high, a fraction of the failures are revealed leading to a reduction in the value of β, i.e. β_D;
- β_D is the common cause failure factor for detectable dangerous faults; as the repetition rate of the diagnostic testing is increased, the value of β_D falls increasingly below β .
- β is obtained from a table D.4 in appendix D of the standard IEC 61508-6 for a score evaluated using relevant factors, $S = X + Y$ [11];
- β_D is obtained from the same table for a score evaluated using relevant factors, $S_D = X(Z+1)+Y$.

According to the score for assessed factors the values of β or β_D are lower for logic subsystems if compared with values for subsystems of sensors and final elements. For subsystems of sensors and final elements the values of β or β_D are selected for specified intervals of score as follows: 1%, 2%, 5%, and 10%. For subsystems of logic subsystems the values of β or β_D are selected for specified intervals of score as follows: 0.5%, 1%, 2%, and 5% [11].

2.4. Evaluation of system failure probabilities

An example of the reliability block diagram of a E/E/PE S-RS is presented in *Figure 3*. It consists of three subsystems: A (sensors), B (logic device) and C (final elements, e.g. actuators).

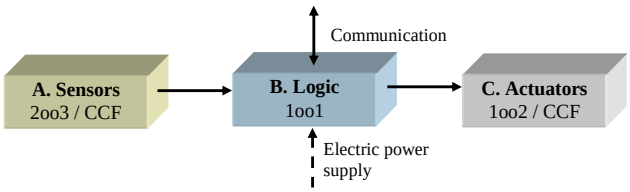

Figure 3. Configuration of a E/E/PE safety-related system

For the low demand mode E/E/PE S-RS the average probability of failure on demand of this S-RS can be calculated from following formula

$$PFD_{avg}(T) \cong PFD^{A}_{avg}(T) + PFD^{B}_{avg}(T) + PFD^{C}_{avg}(T) \quad (4)$$

where
T is the period considered for evaluation, e.g. highest value of the test periods T^j of subsystems A, B and C; PFD_{avg} for subsystems should include the influence of CCF.
For the continuous or high demand mode of E/E/PE S-RS the average probability of danger failure per hour over period T for consecutive subsystems can be evaluated from following formula

$$PFH^{j}_{D}(T) = \frac{1}{T}\int_0^T W^{j}_{D}(t)dt \quad (5)$$

where
$W^{j}_{D}(t)$ is a danger failure frequency [h^{-1}] of j-th subsystem; this frequency should include the influence of CCF.
Resulting probability of average danger failure per hour for the system can be calculated from following formula

$$PFH_{D}(T) = PFH^{A}_{D}(T) + PFH^{B}_{D}(T) + PFH^{C}_{D}(T) \quad (6)$$

The calculations made for some case studies indicate that the influence of CCF in redundant subsystems is usually significant, and can increase significantly the values of $PFD_{avg}(T)$ and $PFH_D(T)$, depending on parameters of the probabilistic models even more than an order of magnitude [17].
Thus, the SIL verified of a E/E/PE S-RS will be in fact lower than when assuming that failures of channels in a redundant system are independent.
In some industrial installations there can exist significant problem with potential spurious operation of the protection system due to safe failures in its subsystems.
For the continuous or high demand mode E/E/PE S-RS the average probability of safe failure per hour over period of interest T for consecutive subsystems can be evaluated from following formula

$$PFH^{j}_{S}(T) = \frac{1}{T}\int_0^T W^{j}_{S}(t)dt \quad (7)$$

where
$W^{j}_{S}(t)$ is a safe failure frequency [h^{-1}] of j-th subsystem; this frequency should include the influence of CCF.

Resulting probability of average safe failure per hour for the system can be evaluated from following formula

$$PFH_S(T) = PFH_S^A(T) + PFH_S^B(T) + PFH_S^C(T) \quad (8)$$

A spurious operation of the protection system will cause mainly the economic consequences because of the plant shutdown and resulting production losses. There is also risk involved due to potential transient event leading with a certain probability to unsafe state of the plant. In some cases of industrial plants the risk of such scenario is relatively high.

2.5. Basic requirements for the E/E/PE system during design and development

The design of the E/E/PE safety-related system (including the overall hardware and software architecture, sensors, actuators, programmable electronics, embedded and application software, software, data etc.) shall meet the requirements concerning [11]:

a) the hardware safety integrity comprising the architectural constraints on hardware safety integrity, and the requirements for quantifying the effect of random failures;
b) the special architecture for integrated circuits (ICs) with on-chip redundancy where relevant, unless justification can be given that the same level of independence between different channels is achieved by applying a different set of measures;
c) the systematic safety integrity, which can be met by achieving one of the following compliance routes:
   - *Route 1S* - compliance with the requirements for the avoidance of systematic faults and the requirements for the control of systematic faults, or
   - *Route 2S* - compliance with the requirements for evidence that the equipment is proven in use, or
   - *Route 3S* - compliance with the requirements for software according to of IEC 61508-3 [11];
d) the system behavior on detection of a fault;
e) the data communication processes.

In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be achieved by implementing one of two possible routes (to be implemented at system or subsystem level):

– *Route 1H* based on hardware fault tolerance and safe failure fraction concepts; or,
– *Route 2H* based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

In the case of *Route 2H* the minimum hardware fault tolerance for each subsystem of an E/E/PE safety-related system implementing a safety function of a specified safety integrity level is recommended to be as follows:

– a hardware fault tolerance (HFT) of 2 for a specified safety function of SIL 4;
– a hardware fault tolerance of 1 for a specified safety function of SIL 3.

For a specified safety function of SIL 1 or SIL 2 the HFT can be assumed 0 or 1.

The developer of the E/E/PE safety-related system should review the requirements for safety-related software and hardware to ensure that they are adequately specified. In particular, the E/E/PE system developer shall consider the following:

a) safety functions;
b) E/E/PE safety-related system safety integrity requirements;
c) equipment and operator interfaces.

The effect of random human error should be evaluated if a person is required to take action to achieve the safety function. The random nature of human error should be considered in cases where a person is alerted to an unsafe condition and is required to take action where it cannot be shown that operator inaction is prevented from affecting the safety function, by mechanisms or procedures, then the random nature of human error should be included in the overall calculation [11].

3. Risk assessment and reduction

3.1. Necessary risk reduction

The necessary risk reduction is such reduction of risk that has to be achieved to meet *the tolerable risk* for a specific situation considered. It may be stated either *qualitatively* or *quantitatively*. The concept of necessary risk reduction is of fundamental importance in the development of the safety requirements specification for the E/E/PE safety-related systems [11].

The tolerable risk depend on various factors (for example, severity of injury, the number of people exposed to danger, the frequency at which a person or people are exposed to danger and the duration of the exposure). In arriving at what constitutes a tolerable risk for a specific application, a number of inputs are considered, which include [11]:

– legal requirements, both general and those directly relevant to the specific application,
– guidelines from the appropriate safety regulatory authority,

– discussions and agreements with the different parties involved in the application,
– industry standards and guidelines,
– international discussions and agreements; the role of national and international standards is becoming increasingly important in arriving at tolerable risk criteria for specific applications,
– the best independent industrial, expert and scientific advice from advisory bodies.

There are reports and more widely accepted proposals concerning methodological issues and indications to elaborate criteria concerning individual and societal risk, including industrial workers and society, for supporting the safety-related decision making, e.g. [24].

3.2. Individual and societal risk assessment for decision making

Individual risk

Different targets are usually defined for employees and members of the public. The target for individual risk for employees is applied to the most exposed individual and may be expressed as the total risk per year arising from all work activities. The target is used to a hypothetical person and therefore needs to take into account the percentage of time that the individual spends at work [11].

The target of individual risk, e.g. 10^{-5} per year, applies to all risks to most exposed person. The maximal individual risk evaluated for given installation and location if is higher has to be reduced at least to a tolerable or target level using a number of ways. The risk reduction solutions selected for implementation should be technologically advanced and cost-effective in life-cycle [17]. One of such solutions cold be a safety function or safety functions to be implemented using E/E/PE safety-related system.

Let assume that the individual risk is dominated by an accident scenario and that a protection system of industrial hazardous installation reducing the frequency of this scenario operates in a low demand mode. Then required average probability of protection system failure on demand can be evaluated as follows

$$PFD_{avg} \leq \frac{R_{at}^{I}}{R_{a}^{I}} \tag{9}$$

where

R_a^I is the average annual individual risk of most exposed hypothetical person per year before designing a protection system, and R_{at}^I is tolerable/target individual risk per year after implementing protection system. Knowing the value of PFD_{avg} the SIL required of E/E/PE S-RS is determined from the second column of Table 1.

The target of risk reduction applied to an individual safety function should take into account possible conservatism of the risk analysis method applied. It is possible to use also a qualitative method for risk evaluation. Due to pessimistic assumptions and intrinsic conservatism in risk analyses using qualitative methods, e.g. a risk graph method, there is a high degree of confidence that the required risk reduction will be achieved as postulated [11].

If members of the public can be exposed to risk from a failure of E/E/PE operating in high or continuous mode of operation then such situation should be included in the evaluation of individual risk and appropriate improving of E/E/PE system with higher SIL should be considered.

There are methods developed for cost-benefit analysis (CBA) suitable for safety-related decision making in the context of individual risk assessment and ALARP (*as low reasonably practicable*) principle based on assumed level of VPF (Value of Protecting Fatality) that support decision making in designing of protection systems including E/E/PESs or SISs [17].

Societal Risk

In some hazardous plants multiple fatalities are likely to arise from single events. Such events are called societal because they are likely to provoke a socio-political response. There can be significant public and organisational aversion to high consequence events and this will need to be taken into consideration in designing of protection systems.

The societal risk associated with operation of given complex technical system is evaluated on the basis of a set of following triples [17]

$$\Re = \{< S_k, F_k, C_k >\} \tag{10}$$

where

S_k is *k*-th accident scenario (usually representing an accident category) defined with regard to results of deterministic modeling, F_k is the frequency of this scenario (evaluated as probability per time unit, usually one year), and C_k denotes the consequences of *k*-th scenario (e.g. environmental or economic losses); the number of injuries and fatalities denoted as N_k can be placed in (10) instead of C_k.

The criterion for societal risk is normally specified in the form of an F-N curve (CCDF – *complementary*

cumulative distribution function) where F is the cumulative frequency of hazards and N the number of fatalities arising from the hazards. The relationship is normally a straight line when plotted on logarithmic scales. The slope of the line will depend on the extent to which the organisation is risk averse to higher levels of consequence. It is necessary to ensure that the accumulated frequency for a specified number of fatalities is lower than the accumulated frequency expressed using the F-N curve [17, 24].

Risk control and continuous improvement

Thus, the criteria for individual and societal risk are to be proposed and defined in some counties. As it was mentioned the principle ALARP of reducing risk to a level *as low as reasonably practicable* is proposed to be used in practice. In deciding about the risk criteria to be applied for a specific hazard the risk profile over the life of the asset may need to be considered [17], [24].

In practice the residual risk in industrial installations will vary from low just after a proof test or a repair has been performed to a maximum just prior to proof testing. This may need to be taken into consideration by organisations that specify the risk criteria to be applied.

If proof test intervals are significant then it may be appropriate to specify the maximum hazard probability that can be accepted just prior to proof testing or that the PFD(t) or PFH(t) is lower than the upper SIL boundary more than a specified percentage of the time (e.g. 90%) [11]. It can cause some practical problems of risk assessment during operation. As it is proposed in this work the decision making concerning the risk reduction will be based on average probabilities calculated for given period of time T (e.g. one year): $PFD_{avg}(T)$ and/or $PFH(T)$.

4. Issues of safety integrity analysis

4.1. Safety integrity and the role of E/E/PE systems for various applications

Safety integrity is defined as the probability that a safety-related system is satisfactory performing the required safety functions under all the stated conditions within a stated period of time. Safety integrity relates to the performance of the safety-related systems in carrying out the safety functions. Safety integrity is usually considered to be composed of the following two elements [11]:

– *Hardware safety integrity* - that part of safety integrity relating to random hardware failures in a dangerous mode of failure. The achievement of the specified level of safety-related hardware safety integrity can be estimated to a reasonable level of accuracy, and the requirements can therefore be apportioned between subsystems using known rules for the combination of probabilities. It may be necessary to use redundant architectures to achieve adequate hardware safety integrity.
– *Systematic safety integrity* - that part of safety integrity relating to systematic failures in a dangerous mode of failure. Although the mean failure rate due to systematic failures may be capable of estimation, the failure data obtained from design faults and common cause failures means that the distribution of failures can be hard or impossible to predict. This has the effect of increasing the uncertainty in the failure probability calculations for a specific situation (for example the probability of failure of a safety-related protection system). Therefore a judgement has to be made on the selection of the best techniques to minimise this uncertainty.

It should be emphasised that measures to reduce the probability of random hardware failure will not have a corresponding effect on the probability of systematic failure. Techniques such as redundant channels of identical hardware, which can be effective at controlling random hardware failures, are of little use in reducing systematic failures such as software errors. The diverse solutions of channels in redundant systems contribute usually significantly to reducing common cause failures (CCFs) and improving safety integrity [11], [12].

The E/E/PE safety-related systems contribute in providing the necessary risk reduction in order to meet the tolerable risk. A safety-related system:

– implements the required safety functions necessary to achieve a safe state for the equipment under control or to maintain a safe state for the equipment under control, and
– is intended to achieve, on its own or with other E/E/PE safety-related systems the necessary safety integrity for the required safety functions, i.e. the safety functions must be performed by the safety-related systems with the degree of confidence appropriate to the application, in order to achieve the tolerable risk.

A human can be an integral part of a safety function having influence on E/E/PE S-RS. For example, a person could receive information, on the state of the EUC, from a display screen and perform a safety action based on this information. As it was mentioned the E/E/PE safety-related systems can operate in: (1) a low demand mode of operation or (2) high demand or continuous mode of operation.

The mode of operation relates to the way in which a safety function is intended to be used with respect

to the frequency of demands made upon it which may be either:
- *low demand mode*: where frequency of demands for operation made on the safety function is no greater than one per year; or
- *high demand mode*: where frequency of demands for operation made on the safety function is greater than one per year.; or
- *continuous mode*: where demand for operation of the safety function is continuous.

4.2. Risk reduction for low demand mode applications

The required safety integrity of the E/E/PE S-RS and other risk reduction measures must be of such a level so as to ensure that:
- the average probability of failure on demand PFD_{avg} of the S-RSs is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk R_t, and/or
- the S-RSs influence the consequences of failure to the extent required to meet the tolerable risk.

Figure 4 illustrates a general concept of risk reduction. The general model assumes that [11]:
- there is a EUC and a control system;
- there are associated human factor issues;
- the safety protective features comprise the E/E/PE S-RSs, and other risk reduction measures.

The risk model for a specific application will need to be developed taking into account the specific manner in which the necessary risk reduction is actually being achieved by the E/E/PE S-RS and/or other risk reduction measures.
The risks indicated in *Figure 4* are as follows:
- *EUC risk – R_{np}*: the risk existing for the specified hazardous events for the EUC, the EUC control system and associated human factor issues: no designated safety protective features are considered in the determination of this risk;
- *tolerable risk*; the risk which is accepted in a given context based on the current values of society;
- *residual risk - R_t:* in the context of this standard, the residual risk is that remaining for the specified hazardous events for the EUC, the EUC control system, human factor issues but with the addition of, E/E/PE safety-related systems and other risk reduction measures.

The necessary risk reduction is achieved by a combination of all the safety protective features.

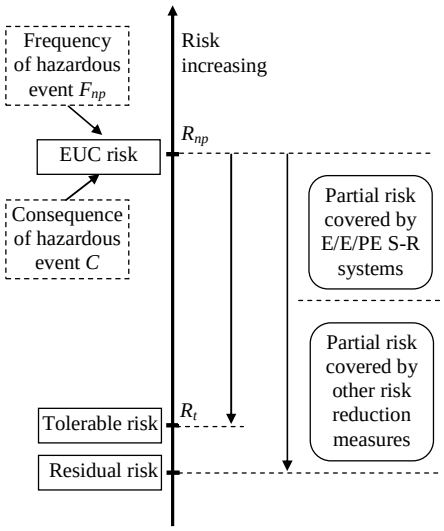

Figure 4. General concept of risk reduction for low demand mode of operation

The EUC risk R_{np} (*no protection*) can be evaluated from the following formula

$$R_{np} = F_{np} C \tag{11}$$

where
F_{np} is the frequency of hazardous event (no protection), i.e. the demand rate on the safety-related protection system when considered, a^{-1};
C is the consequence of hazardous event (in units of a consequence).
The tolerable risk is defined as follows

$$R_t = F_t C_x \tag{12}$$

where
F_t is the tolerable frequency of hazardous event (with protection), a^{-1};
C_x is the consequence of hazardous event (in units of consequences) possibly reduced, i.e. lower then C.
For low demand mode the protection system failure on demand can be evaluated from the formula as follows

$$PFD_{avg} \le \frac{R_t}{R_{np}} \tag{13}$$

If it will be pessimistically assumed that $C_x = C$ then the average probability of the protection system failure on demand can be calculated from the formula as follows

$$PFD_{avg} \le \frac{F_t}{F_{np}} \tag{14}$$

Thus, the SIL of E/E/PE S-RS (protection system) can be determined indicating relevant interval from the second column of Table 1. For instance if $PFD_{avg} = 3x10^{-4}$, then required SILx of the E/E/PE S-RS is SIL3, as regards random failure of hardware. It is necessary to design the configuration of this system consisting of appropriate subsystems and elements and to verify required level of SIL3 based on relevant probabilistic model of the E/E/PE S-RS and evaluation of $PFD_{avg}(T)$ according to formula (4) taking into account potential CCFs.

4.3. Risk reduction for high demand mode applications

The required safety integrity of the E/E/PE safety-related systems and other risk reduction measures must be of such a level to ensure that [11, 17]:
- the average probability of failure on demand of the safety-related systems is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk, and/or
- the average probability of danger failure per hour of the safety-related system is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk.

Figure 5 illustrates the general concepts of high demand applications. The general model assumes that:
- there is a EUC and a control system;
- there are associated human factor issues;
- the safety protective features comprise a E/E/PE safety-related system operating in high demand mode and other risk reduction measures.

Various demands on the E/E/PE safety related systems can occur as follows [11]:
- general demands from the EUC;
- demands arising from failures in the EUC control system;
- demands arising from human failures.

If the total demand rate arising from all the demands on the system exceeds one per year then the critical factor can be the dangerous failure rate of the E/E/PE S-RS. The value of $PFH_D(T)$ is evaluated according to the formula (6). Residual hazard frequency can never exceed the dangerous failure rate of the E/E/PE safety-related system. It can be lower if other risk reduction measures reduce the probability of harm.

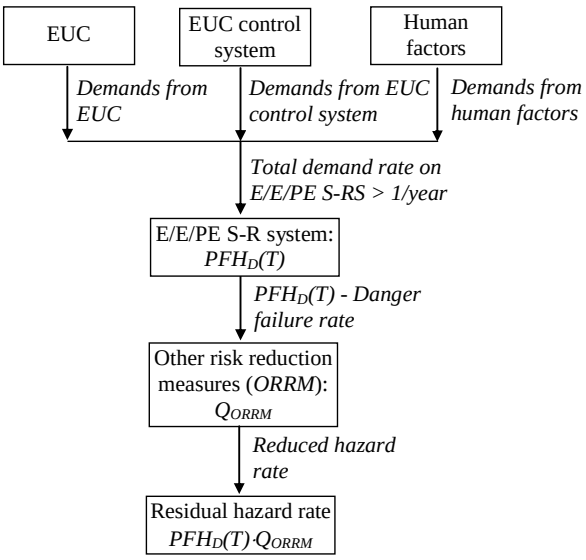

Figure 5. Risk reduction diagram for high demand applications

The risk for high demand mode R_{HDM} of operation can be evaluated from following formula

$$R_{HDM} = PFH_D(T) \cdot Q_{ORRM} \cdot C_x \le R_{HDMt} \qquad (15)$$

where
$PFH_D(T)$ is the average danger failure rate (6) in the period T of the system operating in a high demand mode;
Q_{ORRM} is the failure probability of relevant other risk reduction measures (ORRM).

4.4. Risk reduction for continuous mode applications

The required safety integrity of the E/E/PE S-RS and any other risk reduction measures must be of such a level to ensure that the average probability of a dangerous failure per hour of the safety-related system is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk. With an E/E/PE safety-related system operating in continuous mode other risk reduction measures can reduce the residual hazard frequency according to the risk reduction provided. The conceptual model is shown in *Figure 6*.
The risk for high demand mode R_{CM} of operation can be evaluated from following formula

$$R_{CM} = PFH_{DC}(T) \cdot Q_{ORRM} C_x \le R_{CMt} \qquad (16)$$

where
$PFH_{DC}(T)$ is the average danger failure rate in the period T of the system operating in a continuous mode;

Q_{ORRM} is the failure probability of relevant other risk reduction measures (ORRM).

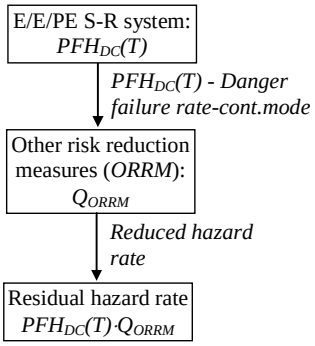

Figure 6. Risk reduction diagram for continuous operation mode

4.5. Risk reduction of protection system spurious operation

As it was mentioned in some industrial installations there can be a significant problem with potential spurious operation of protection system due to safe failures in its subsystems. The probability of average safe failure per hour for the system for the period T (e.g. one year) can be evaluated using formulas (7) and (8).

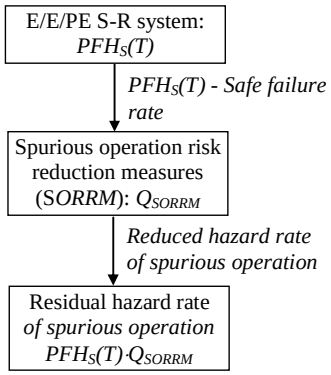

Figure 7. Risk reduction diagram for spurious operation of protection system

The risk concerning spurious operation of protection system R_S of operation can be evaluated from following formula

$$R_S = PFH_S(T) \cdot Q_{SORRM} \cdot C_x \leq R_{St} \qquad (17)$$

where
$PFH_S(T)$ is the average safe failure rate in the period T of the system operating in a continuous mode;
Q_{SORRM} is the failure probability of relevant spurious operation risk reduction measure (SORRM) if it was designed.

4.6. Allocation of safety requirements

Safety integrity applies solely to the E/E/PE safety-related systems and other risk reduction measures and is a measure of the likelihood of those systems/facilities satisfactorily achieving the necessary risk reduction in respect of the specified safety functions. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the safety-related systems can be allocated [11].
The allocation of safety requirements (both the safety functions and the safety integrity requirements) to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities is shown in *Figure 8*.
The methods used to allocate the safety integrity requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities depend, primarily, upon whether the necessary risk reduction is specified explicitly in a numerical manner or in a qualitative manner. As it was mentioned these approaches are termed quantitative and qualitative methods respectively.

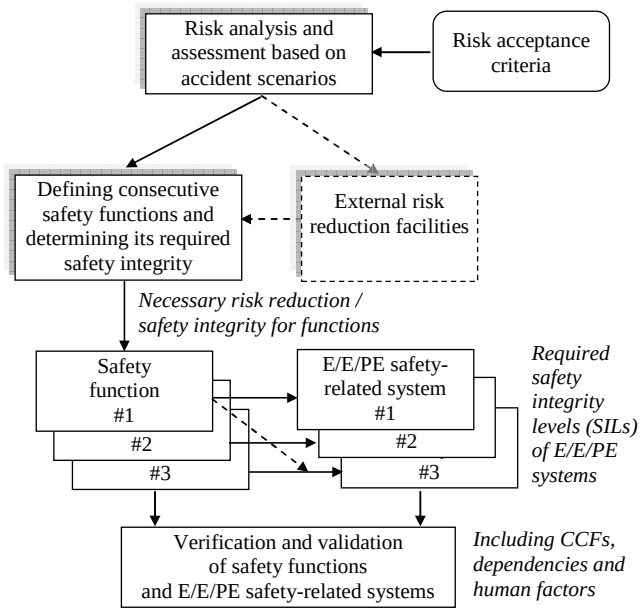

*Figure 8.*Allocation of safety requirements to the E/E/PE safety related-systems and other/external risk reduction facilities

4.7. Mitigation Systems

Mitigation systems take action in the event of full or partial failure of other safety-related systems including E/E/PE safety-systems. The objective is to reduce the consequences associated with a hazardous event rather than its frequency. Examples of mitigation systems include fire and gas systems

(detection of fire/gas and subsequent action to put the fire out, e.g. by water deluge) [11].
When determining the safety integrity requirements it should be recognised that when making judgements on the severity of the consequences with and without operation of the mitigation system. That is, determine the increase in the severity of the consequence if given function did not operate over that when it does operate as intended [11].
If the mitigation function is initiated by a E/E/PE SR-S, its probability of failure on demand can be evaluated from following formula

$$PFD_{avg} \leq \frac{F_{xM} C_{xM}}{F_x C_{xE}} \tag{18}$$

where
F_x is the frequency of the hazardous event with potentially escalating consequences C_{xE} (e.g. due to fire, greater than consequences C_x of given accident scenario);
F_{xM} is the reduced (tolerable) frequency of hazardous event with the mitigation system in operation making reduced consequences $C_{xM.}$; $F_{xM} = F_x \cdot Q_M$ (Q_M is overall unavailability of the mitigation system when required).
Thus, in such situation it is necessary carefully evaluate hazardous events and their consequences in the context of relevant protection and mitigation systems, safety functions and E/E/PE S-RSs.

5. Functional safety and layers of protection

5.1. Common cause and dependency failures

During verifying the safety integrity levels it is important to take account the common cause and dependency failures. In some existing methods (e.g. [LOPA]) and many safety analysis studies these kinds of failures are not considered assuming that each safety-related system relevant to given hazard is fully independent.
The consequence of such assumption can be insufficient risk reduction in spite of using two or more protection layers. There are many applications where some dependencies exist. Examples include the following [11]:

1. Where a dangerous failure of an element within the EUC control system can cause a demand on a safety-related system and the safety-related system uses an element subject to failure from the same cause. An example of this could be where the control and protection system sensors are separate but common cause could lead to failure of both.
2. Where more than one safety-related system is used and some of the same type of equipment is used within each safety-related system is subject to failure from the same common cause. An example would be where the same type of sensor is used in two separate protection systems both providing risk reduction for the same hazard.
3. Where more than one protection system is used, the protection systems are diverse but proof testing is carried out on all the systems on a synchronous basis. In such cases the actual PFD_{avg} achieved by the combination of multiple systems will be significantly higher than the PFD_{avg} suggested by the multiplication of the PFD_{avg} values of the individual systems.
4. Where the same individual element is used as part of the control system and the safety-related system. Where more than one protection system is used and where the same individual element is used as part of more than one system.

In such safety-related cases the effect of common cause/dependency will need to be considered. Consideration should be given as to whether the final arrangement is capable of meeting the necessary *systematic capability* and the necessary probability of dangerous random hardware failure rates in relation to the overall risk reduction required. The effect of common cause failures is difficult to determine and often requires the construction of special purpose models, e.g. fault trees or Markov models.
It is necessary to emphasise that the effect of common cause is likely to be more significant in applications involving high safety integrity levels. In some application it may be necessary to incorporate diversity so that common cause effects are minimised. It should be however noted that incorporation of diversity can lead to problems during design, maintenance and modification. Introducing diversity can lead to errors due to the unfamiliarity and lack of operation experience with the diverse devices [11].

5.2. Safety integrity when multiple layers of protection are used

When multiple layers of protection are used to achieve a tolerable risk frequency there may be interactions between systems themselves and also between systems and causes of demand. As discussed above there are always concerns about common cause and dependent failures since these can be significant factors when overall risk reduction requirements are high or where demand frequency is low [11, 17].
Evaluation of the interactions between safety layers and between safety layers and causes of demand can be complex and may need developing a holistic model and based, for example on a top down

approach with the top event specified as the tolerable hazard frequency.
The model may include all safety layers for calculating correct risk reduction and all causes of demand for calculating the resulting frequency of accident (*Figure 9*). This allows the identification of minimal cut sets for failure scenarios, reveals the weak points (i.e. the shortest minimal cut sets: single, double failures, etc.) in the arrangement of systems and facilitate system improvement through sensitivity analysis [11], [17].

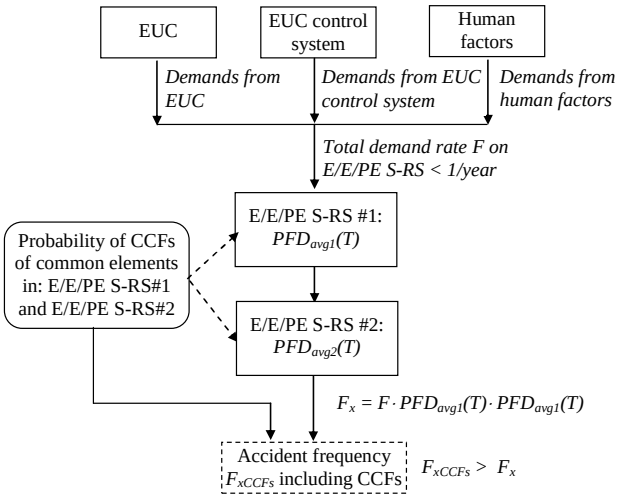

Figure 9. Including common cause and dependent failures in probabilistic modelling of two E/E/PE systems for low demand applications

The frequency of given accident scenario F_x is to be evaluated when causes and systems are assumed to be independent from the following formula

$$F_x = F \cdot PDF_{avg1}(T) \cdot PDF_{avg2}(T) < F_{xCCFs} \qquad (19)$$

where
F is the demand rate (frequency);
$PFD_{avg1}(T)$ is the average probability of system #1 failure on demand;
$PFD_{avg2}(T)$ is the average probability of system #2 failure on demand;
F_{xCCFs} is the accident scenario frequency when causes and systems are dependent.
Thus, when potential dependencies are included in the probabilistic model a relation between risk measures will be $R_{xCCFs} > R_x$ and in cases of higher safety integrity $R_{xCCFs} >> R_x$.

5.3. Software safety integrity levels

Due to wide range of necessary risk reductions that the safety-related systems have to achieve, it is useful to have available a number of safety integrity levels as a means of satisfying the safety integrity requirements of the safety functions allocated to the safety-related systems. The software safety integrity levels are used as the basis of specifying the safety integrity requirements of the safety functions implemented in part by safety-related software. Requirements for software in safety-related applications are given in part 3 of international standard IEC 61508 [11].
The specification of safety integrity requirements for software is in relation to the safety integrity levels determined for the E/E/PE safety-related systems. As it is known in mentioned standard, four safety integrity levels are specified, with safety integrity level 4 being the highest level and safety integrity level 1 being the lowest. The design of software for E/E/PE S-RS of SIL4 is a challenging task. In the process sector applications it was assumed that realistically highest achievable level is SIL3 [12].

5.4. Layers of protection and human factor induced dependency problem

Hazardous industrial plants are designed according to a concept of *defense in depths* using several barriers (protection layers). Designing of a safety-related system is based on the risk analysis and assessment to determine required safety-integrity level (SIL), which is then verified in the probabilistic modeling process. It is important to include in probabilistic models potential dependencies between events representing equipment failures and/or human errors [3], [4], [20], [23], [25], [26].
Figure 10 shows typical layers of protection of in a hazardous industrial plant. A simplified methodology for preliminary risk analysis and safety-related decision-making is the layer of protection analysis (LOPA) methodology [22].

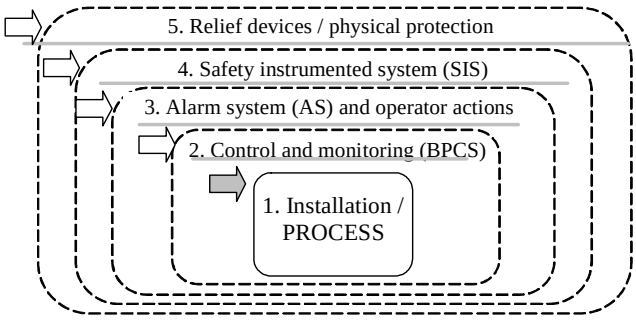

Figure 10. Typical protection layers in hazardous industrial installation

According to the LOPA guidance [22] the protection layer (PL) should be:
- *effective* in preventing the consequence when it functions as designed,

- *independent* of the initiating event and the components of any other PL already claimed for the same scenario,
- *auditable*, i.e. its effectiveness in terms of consequence prevention and probability of failure on demand (PFD) has to be capable of validation (by documentation, review, testing, etc.).

An active PL generally comprises: a sensor of some type (instrument, mechanical, or human), a decision-making element (logic solver, relay, spring, human, etc.), and an action element (automatic, mechanical, or human). As it was mentioned the analysis of potential CCFs within E/E/PE S-RS should be carried out in the designing process. The possibility of dependent failures between the protection layers should be also carefully considered.

Figure 11 illustrates potentially dependent three protection layers (PLs): 2, 3 and 4 shown in *Figure 10*. These layers include:

- PL1 – *basic process control system* (BPCS),
- PL2 – *human*-OPERATOR, who supervises the process and intervene in cases of abnormal situations or during emergencies that are indicated by an alarm system,
- PL3 – *safety instrumented system* (SIS), which can perform a function of *emergency shutdown* (ESD).

An important part of such complex system is the human-system interface (HSI).

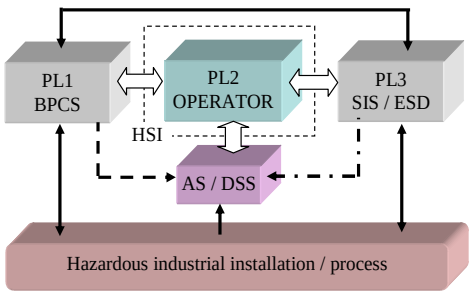

Figure 11. Operator and alarm system / decision support system (AS/DSS) as components of protection layers

Treating of dependent failure events in human reliability analysis (HRA) [4, 17, 26] has been outlined below.

The THERP technique [4, 23] offers a dependency model for potential human failure events to be considered in complex situations distinguishing: ZD - zero dependence, LD - low dependence, MD - moderate dependence, HD - high dependence, and CD - complete dependence.

In the monograph [17] this model was modified introducing the dependency β_H-factor equivalent to β-factor described above. The β_H-factor have values as follows: $\beta_H = 0$ for ZD, $\beta_H = 0.05$ for LD, $\beta_H = 0.14$ for MD, $\beta_H = 0.5$ for HD and $\beta_H = 1$ for CD.

This dependency model is explaied on an example of two dependent events of human errors: A (previous) and B (consecutive). The probability to make the error A and error B (potentially dependent) is evaluated as follows:

$$\begin{aligned} P(A \cap B) &= P(A)P(B \mid A) \\ &= P(A)[\beta_H + (1-\beta_H)P(B)] \\ &= (1-\beta_H)Q_A Q_B + \beta_H Q_A \end{aligned} \tag{20}$$

where:

$P(A) = Q_A$ and $P(B) = Q_B$ are probabilities of relevant failure events. For $\beta_H = 0$ (independence of events/errors) the result is $P(A \cap B) = Q_A Q_B$, but for $\beta_H = 1$ (complete dependence of failures) $P(A \cap B) = Q_A$.

Determining the dependency type, e.g. HD, is based on the task analysis of human operators in the control room [26] including diagnosing and acting with time constrains according to procedures (*Figure 11*).

The human error probability $P(A)$ or $P(B)$ above are named in THERP [4] and SPAR-H [24] methods the human error probability (HEP). The HEP depend on various factors.

The HEP is evaluated when the human failure event is placed into the probabilistic model structure of the system. In the HRA performed within PSA only more important human failure events are considered [17]. Then, the abnormal situation context and related performance shaping factors (*PSFs*) are identified and evaluated according to rules of given HRA method. As the result a particular value of HEP is evaluated.

Different approaches are used for evaluating HEP with regard to PSFs, e.g. assuming a linear relationship for each identified PSF_k and its weight w_k, with constant x for the model calibration

$$HEP = NHEP \sum_k w_k PSF_k + x \tag{21}$$

or nonlinear relationship used in the SPAR-H method for higher values of more important *PSFs*

$$HEP = \frac{NHEP \cdot PSF_{composite}}{NHEP(PSF_{composite} - 1) + 1} \tag{22}$$

where

NHEP is the nominal HEP; the *NHEP* equals 0.01 for diagnosis, and *NHEP* equals 0.001 for action [26].

In the method SPAR-H eight factors are evaluated: *1. Available time; 2. Stress/Stressors; 3. Complexity; 4. Experience/Training; 5. Procedures; 6. Ergonomics/HMI; 7. Fitness for Duty and 8. Work Processes.*

If all PSF ratings are nominal, then the *Diagnosis Failure Probability* = 10^{-2}, otherwise, the Diagnosis Failure Probability is: 1.0E-2 x (M_{D1} for Available Time) x (M_{D2} for Stress/Stressors) x (M_{D3} for Complexity) x (M_{D4} for Experience/Training) x (M_{D5} for Procedures) x (M_{D6} for Ergonomics/HMI) x (M_{D7} for Fitness for Duty) x (M_{D8} for Work Processes), where M_{Di} is multiplier of *i*-th factor for diagnosis.

If all PSF ratings are nominal, then the *Action Failure Probability* = 10^{-3}, Otherwise, the Action Failure Probability is: 1.0E-3 x (M_{A1} for Available Time) x (M_{A2} for Stress/Stressors) x (M_{A3} for Complexity) x (M_{A4} for Experience/Training) x (M_{A5} for Procedures) x (M_{A6} for Ergonomics/HMI) x (M_{A7} for Fitness for Duty) x (M_{A8} for Processes), where M_{Ai} is multiplier of *i*-th factor for action.

The values of M_{Di} and M_{Ai} have been evaluated by experts taking into account own experience and comparative assessment of results obtained from other HRA methods [4], [26].

It is worth to mentioned that the highest values of M_{Di} and M_{Ai} on the level of 50 can be assigned to factors: 5. Procedures (*Not available*) and 6. Ergonomics/HMI (*Missing/Misleading*). In such cases to calculate relevant HEP the formula (22) must be used instead of multiplying of M_{Di} or M_{Ai} as it was explained above.

The evaluations of factors: 5. Procedures and 6. Ergonomics/HMI, are based on careful analysis of solutions proposed with regard to hierarchy of goals, functions, tasks and human operator activities including functions (F), sub-functions (SF) and tasks (T) in a HSI design model with relevant levels of display/control (D/C) pages (*Figure 12*). The HRA is performed in designing process of Instrumentation and Control (I&C) systems and HSI of particular hazardous plant [8], [9].

Depending on the complexity of the tasks or function, there can be many levels. The high level function is broken into sub-functions. The sub-functions can be broken into tasks. The tasks can be broken into task steps. The steps can be further broken into activities. Activities are the lowest level of analysis and describe behaviors such as monitoring the temperature or pressure [8], [9].

Tasks in a sequence tend to cycle through relevant categories, although well-designed and skillfully performed tasks do not necessarily show distinct categories. The benefit of this framework is that it directs the analyst's attention to the necessary components of deliberate, rule based (i.e. procedural) behavior [4], [17], [23]. The task steps level of this analysis specifies critical details that may be associated with each task activities.

To achieve consecutive goals the operators use a procedure from a set of predefined procedures developed for some categories of transients, abnormalities and emergency situations. The structure of a function based display using task analysis results and function decomposition is shown in *Figure 12*.

A few goals can be extracted from the procedure, and these goals can be broken into more detail functions. These functions can be then decomposed into tasks. Thus this figure shows the display design model of a function based display distinguishing three levels of pages: I - for function (a page with concise information), II - for sub-functions and III – for tasks consisting of more detailed information.

The task requirements and sequence information are significant inputs in procedure development. In fact, draft procedures can be written directly from the task analysis, especially when new tasks are issued from function allocation [8], [9].

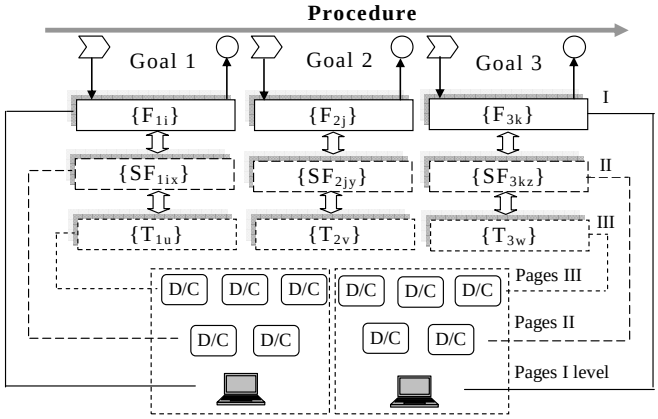

Figure 12. Functions (F), sub-functions (SF) and tasks (T) based HSI design model with three levels of display/control (D/C) pages

Due to importance of the problem of assessing HEP for emergency situations considered in the safety analysis and evaluating correctly the frequency of accident scenarios and related risk levels the research works have been undertaken to include issues of human factors in the context of functional safety analysis [1], [15], [17], [18], [19], [20].

They are aimed at the development of a methodology and software tool consisting of probabilistic models and relevant data/knowledge bases (KBs) with regard to computer supported assessments of human factors in performing HRA (human reliability analysis) and evaluating HEPs with regard to potential dependencies. The methodology includes a framework for uncertainty assessment in risk

informed decision making [6], [14], [20] and quality aspects in developing safety-related advisory software [10].

6. Conclusion

The functional safety is a part of general safety, which depends on the proper response of the control and/or protection systems. The concept of functional safety was formulated in international standard and is applied in the process of design and operation of safety-related *electric, electronic and programmable electronic* (E/E/PE) *systems* or *safety instrumented systems* (SISs) used in the process industry. These systems perform specified functions to ensure that risk is reduced and maintained at acceptable level.

The article was devoted to current challenges and methodological issues of functional safety analysis. There are still methodological challenges concerning the functional safety analysis, assessment and management in the life cycle. They are related to the issues of potential hardware danger failures, software faults, common cause failures (CCFs), dependencies within equipment and barriers as well as human errors, and organizational deficiencies.

The primary objective of functional safety management is to reduce the risk associated with operation of hazardous installation to an acceptable level introducing a set of defined safety functions (SFs) that are implemented using mentioned programmable control and protection safety-related systems (S-RSs). The article presents in a systematic way how to analyse and assess the influence of danger failures of protection system as well as potential spurious operation of this system.

The human-operator contributes to realization of safety functions according to a set of procedures through relevant *human system interface* (HSI), which has to be designed to achieve safety goals during abnormal situations and emergencies taking into account functions of basic control system and S-RSs, such as E/E/PESs or SISs within protection layers. There is current issue how to design an independent *alarm system* (AS). These issues are especially important for industrial installations and hazardous plants, such as chemical installations and nuclear reactors.

Acknowledgments

The research outlined in this work has been carried out as a part of research works aimed at developing methods and prototype software tools for functional safety management in life cycle. They are supported by the Ministry for Science and Higher Education – Center for Research in Warsaw: a research project VI.B.10 for 2011-13 concerning the functional safety management of programmable control and protection systems in industrial hazardous installations.

References

[1] Barnert, T., Kosmowski, K.T. & Sliwiński, M. (2009). A knowledge-based approach for functional safety management. Taylor & Francis Group, *Proc. European Safety & Reliability Conference ESREL*, Prague.

[2] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2010). Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issues. *Proc. PSAM 10*, Seattle,

[3] Carey, M. (2001). *Proposed Framework for Addressing Human Factors in IEC 61508*. A Study prepared by Amey VECTRA Ltd. for Health and Safety Executive (HSE), U.K., Research Report 373.

[4] Gertman, I.D. & Blackman, H.S. (1994). *Human Reliability and Safety Analysis Data Handbook*. New York: A Wiley-Interscience Publication.

[5] Gruhn, P. & Cheddie, H. (2006). *Instrumented Systems: Design, Analysis and Justification*. ISA – The Instrumentation, Systems and Automation Society.

[6] Guidance (2009). Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making, Office of Nuclear Regulatory Research, NUREG-1855, Vol. 1, US NRC.

[7] EEMUA (2007). Publication 191: Alarm Systems, A Guide to Design, Management and Procurement (Edition 2). London: The Engineering Equipment and Materials Users' Association.

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

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

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

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

[12] IEC 61511 (2003). Functional safety: Safety Instrumented Systems for the Process Industry

Sector. Parts 1-3. International Electrotechnical Commission, Geneva.

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

[14] Kosmowski, K.T. (2004). Modelling and uncertainty in system analysis for safety assessment. *Proc. of the International Conference on Probabilistic Safety Assessment and Management, PSAM 7 - ESREL '04*, Berlin, Springer.

[15] Kosmowski, K.T. (2006). Functional Safety Concept for Hazardous System and New Challenges. *Journal of Loss Prevention in the Process Industries* 19(1), 298-305.

[16] Kosmowski, K.T., Śliwiński, M. & Barnert, T. (2006). Functional safety and security assessment of the control and protection systems. Taylor & Francis Group, *Proc. European Safety & Reliability Conference, ESREL 2006*, Estoril. London.

[17] Kosmowski, K.T. (Ed.) (2007). *Functional Safety Management in Critical Systems.* Gdansk University of Technology. Publishing House OF Gdansk University (Wydawnictwo Fundacji Rozwoju Uniwersytetu Gdańskiego).

[18] Kosmowski, K.T. (2011). Functional Safety Analysis including Human Factors. International *Journal of Performability Engineering* 7 (1), 61-76.

[19] 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*, Vol. 3 (1), 39-51.

[20] Kosmowski, K.T., Barnert, T., Śliwiński, M. & Porzeziński, M. (2012). Functional Safety Assessment within the Risk Informed Decision Making Process. PSAM 11 – ESREL 2012, Helsinki.

[21] SINTEF (2007). The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems. SINTEF A1626.

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

[23] OECD Report (1998): Critical Operator Actions – Human Reliability Modeling and Data Issues. Nuclear Safety, NEA/CSNI/R; OECD Nuclear Energy Agency.

[24] R2P2 (2001). Reducing Risk, Protecting People. HSE's Decision Making Process, Norwich.

[25] Reason, J. (1990). *Human Error*. Cambridge University Press.

[26] SPAR-H (2005): Human Reliability Analysis Method, NUREG/CR-6883, INL/EXT-05-00509, US NRC.