Journal of Polish Safety and Reliability Association
Summer Safety and Reliability Seminars, Volume 6, Number 2, 2015

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

Methodological issues of functional safety and reliability assessment of critical systems in industrial hazardous plants

Keywords

hazardous plants, control systems, functional safety, security, human factors, human reliability

Abstract

The aim of this article is to identify and discuss some methodological issues that are of interest among functional safety specialists and experts after publication of the second edition of international standards IEC 61508 and IEC 61511, including the design and implementing the safety-related functions of higher safety integrity levels and protection layers. The basic role of safety-related systems is to reduce effectively and to control in time the individual and/or societal risk with regard to its tolerable levels. These issues include: risk criteria, reliability data, probabilistic models of systems operating in high and/or low mode, dependent failures, human reliability analysis, security of programmable safety-related systems, and reducing uncertainty issues in decision making process applying the cost-benefit analysis. Selected aspects of these issues are discussed and some challenges requiring further research are indicated.

1. Introduction

The functional safety a part of general safety, which depends on the proper functioning in time of the programmable control and/or protection systems. The general concept of functional safety was formulated in the international standard IEC 61508 [10]. It includes defining for given hazardous installation a set of *safety-related functions* (SrF) that are implemented using properly designed the *electric, electronic and programmable electronic* (E/E/PE) *systems*, or so called *safety instrumented systems* (SIS) [11] when used in the process industry sector.

Two different requirements have to be specified to ensure appropriate level of functional safety:

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

The requirements concerning performance of safety functions are determined with regard to hazards identified and potential accident scenarios distinguished, while the *safety integrity level* (SIL) requirements stem from the results of the risk analysis and assessment taking into accounted the risk criteria specified [10]-[11].

Two categories of operation modes cab be considered in functional safety analysis: (1) *low*, and (2) *high* or *continuous* [10]. A low demand mode is often found in the process industry protection systems, e.g. within protection layers, but high or continuous ones appear in the machinery or transportation systems [17].

The E/E/PE systems or SIS have to be appropriately designed to perform specified functions to ensure that relevant risks are reduced to fulfill specified criteria (defined or assumed) at the plant design stage and then verified periodically during operation. The risk related criteria are not explicitly specified in standards [10]-[12], in which only some examples are given with some remarks that specific criteria should be defined for installations of the hazardous plant under consideration.

Therefore, the *risk graphs* presented in standards [10]-[11] for determining the SIL of safety-related functions should be treated only as examples. Therefore, a risk graph for particular hazardous installation should be verified, at least properly adapted or redefined for particular case based on a *risk matrix* defined for a set of accident scenarios obtained in a process of deterministic and probabilistic modelling of this installation [15]. In defining accident scenarios and their probabilistic modelling the event tree (ET) method combined with the *fault trees* (FT) are to be often employed.

This article deals with methodological issues and current challenges of functional safety and reliability analysis and management in the light of modifications introduced in second editions of the international standards IEC 61508 [10] and IEC 61511 [11].

These issues include: determining required SIL for considered safety functions based in individual risk and/or societal risk criteria, and verifying required SIL with regard to the architectures of E/E/PE or SIS systems designed for implementing these functions.

Additionally such aspects as reliability data used in probabilistic models of the control and protection systems, and human factors and human reliability [6]-[7], [13], [22], [24]-[25], [28]-[29] are of interest in safety analysis and management [14], [17], [23], [25].

The functional safety and security of programmable systems and uncertainty treating aspects are becoming nowadays important issues [16], [26] for rational safety-related decision making within *functional safety and security management system* (FS&S MS) [5], [16], [18], [21].

Nowadays new challenges emerge concerning modernisations of the instrumentation and control systems in the industry [8]-[9]. It is proposed to support such decisions applying relevant cost-benefit analysis methods [15], [23].

In final part of this article some more important problems requiring further research are indicated and shortly discussed.

2. Determining required safety integrity level of safety-related functions

2.1. An approach based on risk matrix

The safety integrity requirements apply to the safety-related functions (SrF) implemented in the E/E/PE systems or SIS. The SIL of given SrF is expressed by a natural number from 1 to 4 and is related to the necessary risk reduction when the SrF is implemented. The allocation of safety requirements to the safety functions using the E/E/PE safety-related systems, and other technology safety-related systems or external risk reduction facilities is shown in *Figure 1*.

For the *safety functions* implemented using the E/E/PE system or SIS two types of interval probabilistic criteria are defined in IEC 61508 given in *Table1* for two modes of operation:

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

The E/E/PE system or SIS has a typical configuration shown in *Figure 2* that consists of three subsystems, generally of KooN configuration: (A) input devices (sensors, transducers, converters *etc.*), (B) logic device, e.g. safety PLC (*Programmable Logic Controller*) and (C) output devices, e.g. indicators or the *equipment under control* (EUC), such as actuators.

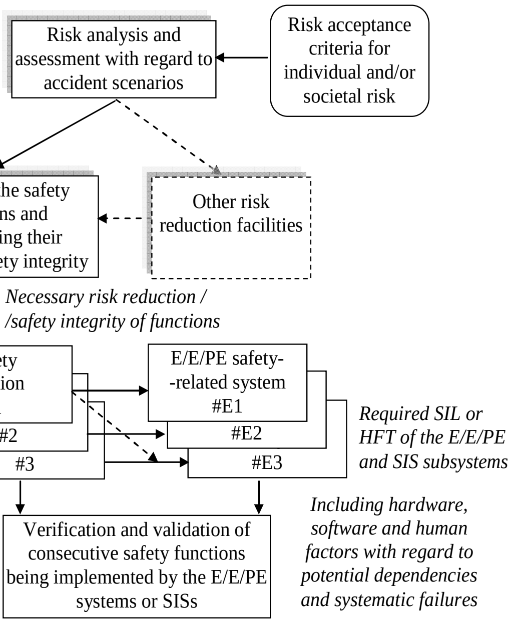
Risk analysis and assessment with regard to accident scenarios
Risk acceptance criteria for individual and/or societal risk
Defining the safety functions and determining their required safety integrity
Other risk reduction facilities
Necessary risk reduction / /safety integrity of functions
Safety function #1
#2
#3
E/E/PE safety- -related system #E1
#E2
#E3
Required SIL or HFT of the E/E/PE and SIS subsystems
Verification and validation of consecutive safety functions being implemented by the E/E/PE systems or SISs
Including hardware, software and human factors with regard to potential dependencies and systematic failures

Figure 1. Allocation of requirements to the E/E/PE safety-related systems

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})

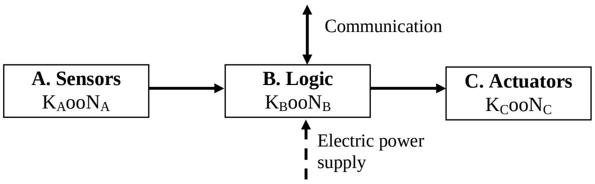

Figure 2. Typical configuration of E/E/PE system or SIS for implementing safety functions

The risk of potential hazardous events can be rationally reduced in the context of evaluated categories of: the *frequency of unwanted occurrence* (*W*) and *consequences* (*N*) as shown in *Table 2*. The total probability of safety system failure for the cases considered has to be reduced to the value shown in right site of arrow ↓ (to obtain reduced frequency *F* of given category from *a* to *e*). As it is shown the required SIL level of given safety function to be implemented depend on possibility of failing to avoid hazardous event using other safety measures (^{x}, ^{y}, or ^{z} as described below *Table 2*). In cases denoted as *b* single E/E/PE system or SIS is not sufficient, and additional protection layer has to be designed.

Table 2. Example of extended risk matrix for determining SIL of the E/E/PE system or SIS

Categories: Fatality → Frequency ↓	N_A (10^{-3}, 10^{-2}] Injury	N_B (10^{-2}, 10^{-1}] More injuries	N_C (10^{-1},1] Single fatality	N_D (1, 10] Several fatalit.	N_E (10, 10^2] Many fatal.
W_3 [a^{-1}], F^e (1 , 10] Frequent	*a*	↓10^{-3} SIL3^z SIL2^y; SIL1^x	↓10^{-4} SIL4^z SIL3^y; SIL2^x	↓10^{-5} b^z SIL4^y; SIL3^x	*b*^{z} *b*^{y} *b*^{x}
W_2 [a^{-1}], F^d (10^{-1} , 1] Probable		↓10^{-2} SIL2^z SIL1^y; a ^{x}	↓10^{--3} SIL3^z SIL2^y; SIL1^x	↓10^{-4} SIL4^z SIL3^y; SIL2^x	↓10^{-5}*b*^{z} *SIL4*^{y} *SIL3*^{x}
W_1 [a^{-1}], F^c (10^{-2} , 10^{-1}] Occasional		↓10^{-1} SIL1^z a^y;	↓10^{-2} SIL2^z SIL1^y; a^x	↓10^{-3} SIL3^z SIL2^y; SIL1^x	↓10^{-4}*SI* *L4*^{z} *SIL3*^{y} *SIL2*^{x}
W_0 [a^{-1}], F^b (10^{-3} , 10^{-2}] Seldom			↓10^{-1} *SIL1*^{z} *a*^{y}*;*	↓10^{-2} *SIL2*^{z} *SIL1*^{y}*;* *a*^{x}	↓10^{-3}*SI* *L3*^{z} *SIL2*^{y} *SIL1*^{x}
W_{-1} [a^{-1}], F^a (10^{-4} , 10^{-3}] Remote				↓10^{-1} *SIL1*^{z} *a*^{y}	↓10^{-2}*SI* *L2*^{z} *SIL1*^{y} *a*^{x}

W - frequency of unwanted occurrence, *F* - reduced frequency of hazardous event, *N* - its consequences
Possibility of failing to avoid hazardous event using other safety measures: ^{x} ($Q^x = 10^{-2}$); ^{y} ($Q^y = 10^{-1}$); ^{z} ($Q^z = 1$)
a - no special safety requirements, *b* - single E/E/PE system or SIS is not sufficient

The risk matrix defined in *Table 2* can be modified, e.g. to take into account some societal values or an aversion to major accidents with serious consequences [17]. It would change SIL requirements to be assigned to the E/E/PE system or SIS (increased SIL for higher consequences), or necessity to design additional safety layer.

To fulfill requirements of a higher SIL (3 or 4) assigned to the safety-related function an appropriate architecture of the E/E/EP system or SIS is to be designed, e.g. 1oo2, 2oo3 or 2oo4. The highest safety integrity level that can be claimed when designing a safety function is limited by the *hardware safety integrity constraints*. According to IEC 61508 it can be achieved by implementing one of two possible routes at a system or subsystem level [10]:

- Route 1H based on *hardware fault tolerance* (HFT) and *safe failure fraction* (S_{FF}) concepts; or
- Route 2H based on component reliability data obtained from end users increasing confidence levels and HFT for required and specified safety integrity levels.

In the case of Route *2H* the minimum HFT 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:

- HFT of 2 for a specified safety function of SIL4;
- HFT of 1 for a specified safety function of SIL3.

For a specified safety function of SIL1 or SIL2 the HFT can be assumed 0 or 1.

Thus, there are indications in the standard [10] how to design the E/E/PE system or SIS architecture based on some HFT-related rules to achieve required safety integrity level, determined from a risk matrix as in *Table 1* or modified risk matrix, obtained with an assumption of the risk aversion for higher consequences. This will make higher required safety integrity levels (SIL) in cells situated in upper right side of this matrix or it will be necessary to design additional protection layer (cells marked with *b*^{z}, *b*^{y} or *b*^{x}). However, formally the SIL for an architecture considered should be verified using selected probabilistic modelling method of E/E/PE system or SIS considered [4].

2.2. Risk reduction and evaluation of safety integrity level for low demand mode application

The required safety integrity of the E/E/PE implementing safety-related function SrF 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 SrF is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk R_t, and/or
- the SrF influences the consequences of hazardous event to the extent required to meet tolerable risk.

Figure 3 illustrates a general concept of risk reduction. The general model assumes that [10]:

- there is the *equipment under control* (EUC) and its control/protection system;
- there are associated human factor issues;
- the safety protective features comprise the E/E/PE implementing SrF, 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 being achieved by the E/E/PE implementing SrF and other risk reduction measures.

The risks indicated in *Figure 3* are as follows:

- the *EUC risk R_{np}* - the risk existing for specified hazardous event (no designated safety protective features are considered in the determination of this risk);
- the *tolerable risk R_t* - the risk which can be accepted in a given context based on the current societal values;
- the *residual risk R_r* - remaining risk for the specified hazardous events including the EUC, the EUC control system, and human factor issues with the addition of SrF implemented using E/E/PE safety-related system, human factors and other risk reduction measures.

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

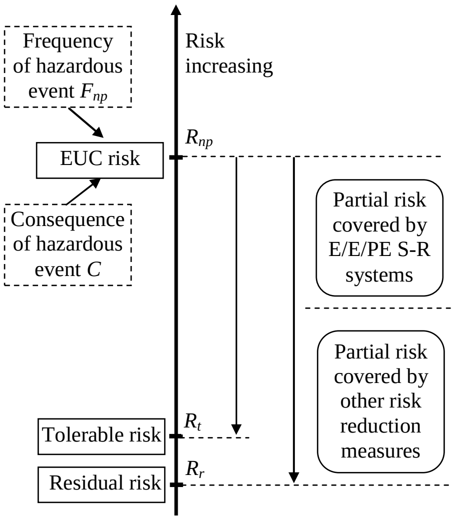
Frequency of hazardous event F_{np}
Risk increasing
R_{np}
EUC risk
Consequence of hazardous event C
Partial risk covered by E/E/PE S-R systems
Partial risk covered by other risk reduction measures
Tolerable risk
R_t
Residual risk
R_r

Figure 3. General concept of risk reduction for low demand mode of operation

The EUC risk R_{np} is to be evaluated from the following formula

$$R_{np} = F_{np} C \tag{1}$$

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 denotes the consequence of hazardous event (in units of a consequence).

The tolerable risk is defined as follows

$$R_t = F_t C_x \tag{2}$$

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) presumably reduced, i.e. lower then C.

For a low demand mode of operation, the average probability of protection system failure on demand (PFD_{avg}) can be evaluated, assuming that $C_x = C$, from the formula as follows

$$PFD_{avg} \le \frac{F_t}{F_{np}} \tag{3}$$

Knowing the value of PFD_{avg} the SIL of given SrF implemented using the E/E/PE protection system can be determined indicating relevant interval in the second column of *Table 1*. For instance if PFD_{avg} = 3x10^{-4}, then from this table SIL3 will be obtained as regards random failure of hardware. Requirements concerning the safety integrity level of software for implementing given function are specified in part 3 of IEC 61508.

3. Verifying the safety integrity level of system implementing safety-related function

3.1. Verifying the safety integrity level of a single protection system

Having the SIL the design the architecture of E/E/PE system is to be designed consisting of appropriate subsystems of specified configuration (see *Figure 2*) with appropriate subsystems and channels/ elements. Then the SIL this system can be verified using appropriate probabilistic model of random failures with regard to reliability data of hardware, potential common cause failures (CCF), and human reliability.

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 the manufacturing processes and quality management system, operational procedures, and other relevant factors.

For the low demand mode of the E/E/PE system implementing given SrF the average probability of failure on demand is often calculated from following formula

$$PFD_{avg}(T) \cong PFD^{A}_{avg}(T_A) + PFD^{B}_{avg}(T_B) + PFD^{C}_{avg}(T_C) \tag{4}$$

where: T is the testing period evaluated for the E/E/PE system, e.g. highest value of the test periods T_j of the subsystems A, B, and C.

The probabilistic models developed for these subsystems should include the influence of CCF and the human factors introduced applying selected method of human reliability analysis (HRA) [15].

If verified SIL is lower than required, the E/E/PE system architecture must be redesigned to achieve higher SIL. Another issue is verifying of software for designed SrF of determined SIL according to part 3 of IEC 61508 [10].

3.2. Layer of protection analysis and dependency issue

Protection systems of 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 human failure events that depend on various factors [1]-[3], [12], [15].

Figure 4 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 [20].

According to the LOPA guidance 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.).

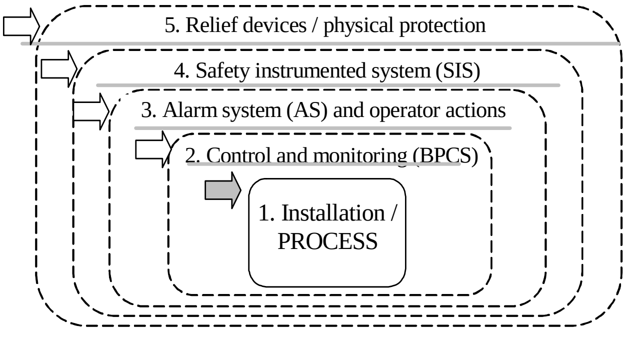
5. Relief devices / physical protection
4. Safety instrumented system (SIS)
3. Alarm system (AS) and operator actions
2. Control and monitoring (BPCS)
1. Installation / PROCESS

Figure 4. Typical protection layers in hazardous industrial installation

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. 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 [10], [15], [19].

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 to be based, for example, on a top down approach with the top event specified as the tolerable hazard frequency.

The model may include selected safety layers for calculating correct risk reduction and all causes of demand for calculating the resulting frequency of accident (*Figure 5*). 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.

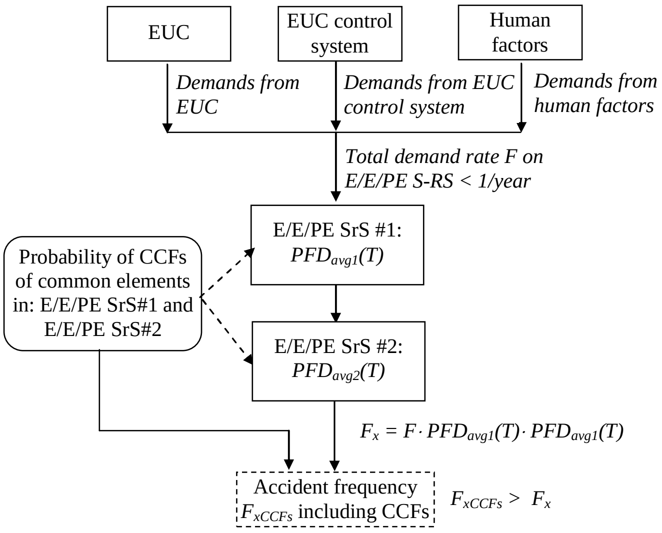
EUC
EUC control system
Human factors
Demands from EUC
Demands from EUC control system
Demands from human factors
Total demand rate F on E/E/PE S-RS < 1/year
E/E/PE SrS #1: PFDavg1(T)
Probability of CCFs of common elements in: E/E/PE SrS#1 and E/E/PE SrS#2
E/E/PE SrS #2: PFDavg2(T)
Fx = F· PFDavg1(T)· PFDavg1(T)
Accident frequency FxCCFs including CCFs
FxCCFs > Fx

Figure 5. Including common cause and dependent failures in probabilistic modelling of two E/E/PE systems for low demand applications

If the frequency of given accident scenario F_x is calculated when causes and systems are assumed to be independent, then following relation is fulfilled

$$F_x = F \cdot PDF_{avg1}(T) \cdot PDF_{avg2}(T) < F_{xCCFs} \qquad (5)$$

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 assumed to be dependent.

Thus, when potential dependencies are included in the probabilistic model a relation between risk measures will be $R_{xCCFs} > R_x$.

4. Issues raised in second edition of functional safety standards: generic and process sector

4.1. Reliability data

In second edition of IEC 61511 [11] there is new clearly formulated requirement that the reliability data used for quantifying the effect of random hardware failures shall be *credible, traceable, documented and justified*. The reliability data should be based on the *field feedback* existing on similar devices used in a similar operating environment. This includes *user collected data*, vendor/provider/user data derived from data collected on devices, data from general field feedback reliability databases, etc.

In some cases, engineering judgement can be used to assess missing reliability data or evaluate the impact on reliability data collected in a different operating environment. The lack of reliability data reflective of the operating environment is a recurrent shortcoming of probabilistic calculations. End-users should organize relevant device reliability data collections to improve the implementation of the IEC61511 standard. The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.

The following techniques can be used for calculating the failure measures [11]:

- using the confidence upper bound (i.e., 70%) of each input reliability parameter instead of its mean in order to obtain *conservative point estimations* of the failure measures.
- using the probabilistic distributions functions of input reliability parameters or performing Monte Carlo simulations to obtain an histogram representing the distribution of the failure measure and assess a conservative value from this distribution.

On a pure statistical basis, the average of a reliability parameter can be estimated by using the *maximum likelihood estimate* and the confidence bounds [$\lambda_{10\%}$, $\lambda_{90\%}$] calculated for the χ^2 (Chi-square) function which is tabulated in statistical books.

There is no clear indication in mentioned above standard [10] about of the *failure mode, effect and criticality analysis* (FMECA) methods, especially for new components in design, useful for evaluation of typical parameters as diagnostic coverage (DC) and other shown in *Figure 6*, necessary for probabilistic modeling of components used in functional safety systems.

As it is known the safe (S) or dangerous (D) failure can be detected (d) or undetected (u). *Figure 6* 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 6*. For example the danger undetected failure intensity can be calculated from the formula

$$\lambda_{Du} = \lambda(1 - FS)(1 - DC) \tag{6}$$

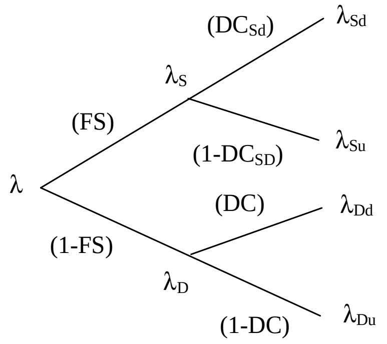

Figure 6. Elements of failure intensity in analysis of the protection system components and subsystems

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.

The reliability data and their uncertainly issues useful for probabilistic modeling in functional safety analysis are discussed in monograph [15]. More details are given in the report [27].

4.2. Human factors and human reliability

In part 1 of 2nd edition of IEC 61511 [11] there is requirement concerning the specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors.

The design of the SIS shall take into account human capabilities and limitations and be suitable for the task assigned to operators and maintenance staff. The design of operator interfaces shall follow good human factors practice and shall accommodate the likely level of training or awareness that operators should receive.

Interfaces to the SIS can include, but are not limited to the operator interface(s), maintenance/engineering interface(s), and communication interface(s). There is requirement concerning the operator interface when the SIS operator interface is via the BPCS operator interface. In such design should be taken into account all credible failures that may occur in the BPCS operator interface.

In part 2 of IEC 61511 there is a remark that human factors do not need to be considered when determining hardware fault tolerance. However, addressing human factors (e.g., configuration, calibration, testing) is required by the use of different personnel for checking and approval.

There are also remarks concerning human system interfaces (HSIs). The logic solver (the SIS) interface capability should be designed to allow for a functionally safe interface to the BPCS for shadowing, operator interface, alarming, diagnostics and interchange of specific values. The following was implemented in the SIS interfaces to the BPCS:

- using of redundant HMI consoles,
- using of redundant communication links,
- using of an internal communication watch-dog timer for interfaces handling critical data (e.g., all data to the BPCS operator console).

The shutdown pushbutton should be mounted on one of the HMI consoles, and equipped with a plastic safety cover to avoid inadvertent shutdowns.

Factors to be considered in the design of the operator interface include:

A. Alarm management requirements,
B. Operator response needs,
C. Good ergonomics.

Changes to the application program (including trip settings) of the SIS can only be made through the SIS engineering consoles with appropriate security measures.

Alarm management should ensure that problems and potential hazards are presented to the operator in a manner that is timely and easily identified and understood by using alarm prioritization. Alarm prioritization reflects the site’s alarm management philosophy. Features implemented include [11]:

A) Alarms for which risk reduction credit is taken in the LOPA have the highest priority. These alarm should be checked at the same twice-per-year frequency as the SIS.
B) Pre-trip alarms that initiate operator action prior to SIS action have the highest priority.
C) Use of BPCS operator interface features to distinguish the different priority level alarms.
D) Use of pre-trip and trip alarms to help define operator response requirements
E) SIS diagnostic alarms are displayed on a separate graphic in the HMI.

There are also requirements concerning the operator response, i.e. the ability of the operator to respond to HSI initiated alarms requires the implementations as follows:

a) Use of sequence of events (SOE) recording (the normal scanning time of the BPCS provides true first-out alarm functionality),
b) Use of pre-trip alarms (the operator may take corrective action before a trip occurs (e.g., adding shortstop to prevent runaway reaction).

Thus, in these cases pre-trip alarms are provided. Pre-trip alarm and trip settings should take into account process dynamics and sensor response.

In part 2 of IEC 61511 there are also suggestions how to perform human reliability analysis (HRA) to identify conditions that cause people to err and provides estimates of error rates based on past statistics and behavioural studies. Some examples of human error contributing to chemical process safety risk include [11]:

- undetected errors in design;
- errors in operations (e.g., wrong set point);
- improper maintenance (e.g., replacing a valve with one having the incorrect failure action);
- errors in calibrating, testing or interpreting output from control systems;
- failure to respond properly to an emergency.

In this standard there are suggested references concerning HRA, but some of them seem to be not fully up-to date.

4.3. Security related issues

A security risk assessment should highlight the threats that could potentially exploit vulnerabilities and result in security events. The threat scenarios may cover the following ones [11]:

- External persons (spying, influence, targeted attacks, denial of service, unauthorized access/control, and malware infection, etc.);
- Personnel, organizations and knowledge (dissipation of the organization or a person);
- Degradation of security mechanisms (firewalls, weak passwords, insufficient authentication mechanisms);

- Hardware (improper use of an equipment, spying on equipment, overuse of equipment, deterioration of equipment, modification of equipment, loss of equipment, etc.);
- Software, application programming, and data (Improper use, analysis without modification, overuse by exploiting security bugs, deletion by mistake or intentionally, modification unauthorized/ erroneous modification of software, disappearance if the software is not maintained, license has not been renewed);
- Networks (passive interception of data, man in the middle – the network is being snooped, data are intercepted and modified, saturation, degradation, modification, etc.).

In part 1 of 2nd edition of IEC 61511 [11] there are also new requirements concerning security-related aspects to be included in functional safety analysis. It includes a security risk assessment that shall be carried out on the SIS and its associated elements. It shall result in [11]:

a) a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);
b) a description of identified threats that could potentially exploit vulnerabilities and result in security events (including intentional attacks on the hardware and related software, as well as unintentional attacks resulting from human error);
c) a description of the potential consequences resulting from the security events and the likelihood of these events occurring;
d) consideration of various phases such as design, operation, and maintenance;
e) the determination of requirements for additional risk reduction;
f) a description of, or references to information on, the measures taken to reduce or remove the threats.

The design of the SIS should be such that it provides the necessary resilience against the identified security risks.

The maintenance/engineering interface shall provide the following functions with *access security protection* to each [11]:

- SIS mode of operation, program, data, means of disabling alarm communication, test, bypass, maintenance;
- SIS diagnostic, voting and fault handling services;
- add, delete, or modify application program;
- data necessary to troubleshoot the SIS;
- where bypasses are required they should be installed such that alarms and manual
- shutdown facilities are not disabled.

Enabling and disabling the read-write access shall be carried out only by a *configuration management* process using the maintenance/engineering interface with appropriate documentation and security measures.

Supporting the access security and enhance cyber security for the SIS should be provided, such that revision to BPCS functions or data do not impact the SIS, and also the means by which communications are made secure (e.g. cyber security measures). The SIS logic solver embedded software provides file security by computing and checking the cyclic redundancy checks on all data streams stored in the compound file structure of the application.

For those devices (e.g., interface devices) where it is more difficult to control physical access, the use of administrative procedures should be implemented. Some basic security approaches implemented were:

- written approval with reasons for access with persons requiring access to be identified,
- definition of required training and/or familiarity with the system before access is permitted,
- Definition of who is to have access to the system, under what circumstances, and to perform what work; this includes the procedures needed to control the use of maintenance bypasses.
- SIS features that facilitate access control.

The use of programmable SIS introduced additional security concerns because of the relative ease of making changes in the application logic. For these systems, additional features should be implemented including:

- restricting access to the maintenance/engineering interface;
- establishing administrative policies/procedures that define the conditions under which the maintenance interface may be connected to the system during normal operation;
- use of virus checking software and appropriate program and file handling procedures in the engineering console to help avoid corruption of the embedded and/or application logic;
- the use of SIS utility software that tracks revisions in the application logic and allows the determination (after the fact) of when a change was made, who made the change, and what the change consisted of;
- no external connections of the SIS or BPCS to the internet or phone lines.

Smart sensors shall be write-protected to prevent inadvertent modification from a remote location, unless appropriate safety review allows the use of read/write. The review should take into account human factors such as failure to follow procedures.

5. Cost-benefit analysis of functional safety improvement options

Taking into account the definition of risk and the equation (2) following formulas can be written for the safety-related risk

$$R_k^{Sa} = F_k^I PFD_k^x C_k^x \tag{7}$$

where: F_k^I is *k*-th annual frequency of a safety-related initiating event *I*, PFD_k^x is a conditional probability of failure on demand for given initiating event *I* causing a consequence of category *x*, i.e. C_k^x, expressed in units of consequence *x*, e.g. a number of harmed individuals, or aggregated economic losses in monetary units [15];
and security-related risk

$$R_l^{Se} = F_l^A PFA_l^y C_l^y \tag{8}$$

where: F_l^A is *l*-th annual frequency of a security-related event of an adversary (intentional) attacking *A*, PFA_k^y is a conditional probability of failure mode on attack (vulnerability) for given event *A* causing a consequence of category *y*, i.e. C_l^y, expressed in units of consequence *y*, e.g. a number of harmed individuals, or aggregated economic losses in monetary units.

In the monograph [15] a cost-benefit analysis (CBA) approach is proposed for supporting the safety related decision making as regards the SIL of safety-related functions to be implemented using the E/E/PE system or SIS of configurations considered depending on specified SIL, with their relevant investment and operation costs discounted in time. In this approach the consequences can be expressed as the scope of potential fatalities in relation to the *value of protecting fatality* (VPF) or as aggregated losses evaluated in monetary units for identified accident scenarios.

For the frequency of j^{th} accident evaluated without protection F_j and two variants of protections: 1 and 2 considered characterised by the average probability of failure on demand PFD_{avg} for two variants of protection system for increasing SIL (lowering PFD_{avg}): $PFD^1_{\text{avg},j}$ and $PFD^2_{\text{avg},j}$ $\left(PFD^2_{\text{avg},j} < PFD^1_{\text{avg},j}\right)$, following relation is obtained for justified investment costs of the protection system improvement:

$$\begin{aligned}\Delta K^{\text{ju}}_{\text{In},j} &< L_d K_{\text{Lo},j}(F_{j,1} - F_{j,2}) = \\ &L_d K_{\text{Lo},j} F_j (PFD^1_{\text{avg},j} - PFD^2_{\text{avg},j})\end{aligned} \tag{9}$$

where: L_d is the coefficient of annual capital costs [a], calculated for the period *L* of the system lifetime and the discounting rate *d;* $K_{Lo,j}$ represent aggregated losses due to *j*-th accident scenario; F_j is the frequency *j*-th scenario without protections considered.

The aggregated justified investments costs for the improving of the protection system can be evaluated as follows:

$$\Delta K^{\text{ju}}_{\text{In}} = \sum_j \Delta K^{\text{ju}}_{\text{In},j} \tag{10}$$

For the frequency of j^{th} accident evaluated without protection F_j and two variants of protections: 1 and 2 considered characterized by the average probability of failure on demand PFD_{avg} for two variants of protection system for increasing SIL (lowering PFD_{avg}): $PFD^1_{\text{avg},j}$ and $PFD^2_{\text{avg},j}$ ($PFD^2_{\text{avg},j} < PFD^1_{\text{avg},j}$), following relation is obtained for justified costs of the protection system improvement for preventing putative fatalities:

$$\Delta K_j^{\text{ju}} = k_{\text{f}} \cdot VPF \cdot F_j \cdot [PFD^1_{\text{avg},j} - PFD^2_{\text{avg},j}] \cdot N_j \cdot L_d \tag{11}$$

where: *VPF* is a value of protecting fatality, e.g. 2 millions EUR [15]; k_f is a coefficient (k_f >1) for evaluating the cost of preventing fatality (*CPF*); N_j is number of fatalities in *j*-th hazardous event.

Example. Let *VPF* = EUR 2 000 000, k_{f} = 1.5, F_j = 0.1 [a^{-1}], N_j = 1, L_d = 15.4 (for *L = 30* [a] and discounting rate *d = 0.05* [a], $PFD^1_{\text{avg},j}$ = 0.01 (pessimistic value from *Table 1* for SIL2), $PFD^2_{\text{avg},j}$ = 0.001 (SIL3).

The result from (11) is: ΔK_j^{ju} = EUR 41 600. It is rather questionable to improve the system from SIL2 to SIL3 for this amount. *Remark:* For N_j = 1 in (11), the relevant frequencies F_j are equivalent to the individual risk R_j^{I}.

If the value of fatalities for the accident considered would be N_j = 10, then according to the result is ΔK_j^{ju} = EUR 416 000. For such amount it is undoubtedly possible to improve the protection system considered (higher HFT or higher SIL for components of designed E/E/PE system).

Similar formulas to those of (9) and (10) can be derived for security related risks, although the data are based in such cases much more on expert opinions with higher biases and uncertainty ranges.

6. Conclusions

There are several issues and new methodological challenges concerning functional safety as a part of general safety, which depends on reliable functioning of programmable control and/or protection systems. These systems perform nowadays crucial safety functions ensuring that relevant risks are reduced in designing process and maintained at acceptable level during operation of hazardous installation.

These issues and challenges include: defining the risk criteria, using reliability data in probabilistic modelling based on the *field feedback* existing on similar devices used in a similar operating environment, applying verified probabilistic models for systems operating in high and/or low mode with appropriate treating of dependent failures, in particular common cause failures (CCFs).

The human factors analysis methods for designing human system interfaces (HSI) and human reliability analysis methods including cognitive aspects require further research effort. A relatively new issue that require additional research is security of programmable control and protection systems.

Due to uncertainty involved applying the cost-benefit analysis in safety and security-related decision making for representative parameters in relevant models with sensitivity evaluations is proposed.

References

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

[2] 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.

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

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

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

[6] HSE-HRA (2009). Review of human reliability assessment methods. Research Report RR679 prepared for Health and Safety Executive.

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

[11] IEC 61511 (2014). Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.

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

[13] Kirwan, B. (1994). A Guide to Practical Human Reliability Assessment. CRC Press, London.

[14] 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.

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

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

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

[18] 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.

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

[20] LOPA (2001): Layer of Protection Analysis, Simplified Process Risk Assessment. Center for

Chemical Process Safety. American Institute of Chemical Engineers, New York.

[21] NASA (2010). Risk-informed Decision Making Handbook. Office of Safety and Mission Assurance. NASA Headquarters.

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

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

[24] Rasmussen, J. & Svedung, I. (2000). *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, Karlstad.

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

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

[27] SINTEF RD (2010): Reliability Data for Safety Instrumented Systems – PDS Data Handbook. Edition, SINTEF A13502.

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

[29] Swain, A. D. & Guttmann, H. E. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. NUREG/CR-1278. Washington: US Nuclear Regulatory Commission.