Barnert Tomasz

Kosmowski Kazimierz T.

Śliwiński Marcin

Gdańsk University of Technology, Gdańsk, Poland

Framework for RIDM within functional safety management process

Keywords

functional safety, functional safety management (FSM), safety integrity level (SIL), risk informed decision making (RIDM), safety, security, uncertainty

Abstract

The functional safety management in life cycle is a complex process starting with identifying hazards and defining *safety-related functions* (SRFs) with regard to the results of risk assessment oriented at determining the safety integrity level of consecutive functions. Another element of such process is a verification of required SIL for considered architectures of safety-related system that implements given safety function. Due to complexity of the problem, to overcome difficulties in safety-related decision making often under considerable uncertainties, usually without taking into account security aspects, we propose to apply the RIDM methodology oriented on functional safety management of programmable control and protection systems in life cycle taking into some more important risk-related factors identified.

1. Introduction

The functional safety that is a part of overall safety, play nowadays an increasing role in reducing the risk related to operation of hazardous industrial plants. It introduces a set of safety-related functions (SRFs) to be implemented by the safety-related systems that include programmable control and protection systems, as the risk reducing tools. A proper recognition, description and design of such SRFs require careful identification of hazards and detailed analysis of risks.

There are frameworks for functional safety management in life cycle described in IEC 61508 [11] and some sector standards, e.g. IEC 61511 [12], IEC 62061 (machinery) and IEC 61513 (nuclear plants). A main scope of such frameworks is determining safety integrity level (SIL) for defined safety-related functions (SRFs) and verifying SIL for considered architectures of E/E/PES (*Electric / Electronic / Programmable Electronic System*) [11] or SIS (Safety Instrumented System) [12] using appropriate probabilistic models for relevant modes of operation, i.e. low demand mode or high/continuous mode. In addition these analyses should include such issues and factors as: the architectural constraints, possibility of systematic failures and software faults, *common mode failures* (CCFs) [22], as well as the human factors and errors [15], [16], [17], [23].

There is considerable uncertainty involved in the risk analysis and assessment to determine SIL for consecutive safety-related functions [20] and its verifying [1], [2], [3]. The qualitative and/or quantitative methods are used in practice for that purpose.

The programmable control and protection systems usually operate in an environment of computer networks using the wire and/or wireless communication technologies. In functional safety analyses the security aspects are often neglected, but they can significantly influence the results of safety analyses. So, those aspects should be taken into account during a process of functional safety analysis, however the standard IEC 61508 does not indicate directly how to consider them. Some proposals are given in [5], [6], [18].

Due to complexity of described above problem, to overcome difficulties in decision making we propose to apply the methodology of the *Risk Informed*

Decision Making (RIDM) [9], [19]. The methodology proposed is compatible with the functional safety management methodology described in IEC 61508 [11]. It enables the decision making in a more transparent and systematic way. In this methodology the overall *functional safety management* (FSM) includes the RIDM and periodic risk reassessment based on performance monitoring of the installation and subsystems of the programmable control and protection systems.

2. Framework for RIDM within functional safety management process

2.1. Safety-related lifecycle

The term *safety-related* (SR) applies to the systems, which perform a specified functions (SRFs) to ensure that the risk is maintained at an acceptable or tolerable level. Two different requirements should be satisfied to ensure the functional safety [11]:

- requirements imposed on the performance of safety-related functions,
- requirements for the safety integrity expressed by the probability that given safety function is performed in satisfactory way within a specified time.

The requirements for safety functions are determined taking into account the results of hazards identification, while the safety integrity requirements result from risk assessment. The higher the safety integrity level (SIL) is, for given SRF, the lower *probability of failure on demand* (PFD_{avg}) or *probability of danger failure per hour* (PFH) is required to reduce the risk to required level. Higher safety integrity levels impose more strict requirements on the design of a safety-related system. Most often, the safety function is performed using the *electric, electronic and programmable electronic system* (E/E/PES) [11] or the *safety instrumented system* (SIS) [12].

The safety-related E/E/EPS comprises all the elements that are necessary for the safety function performance, i.e., from sensors, via logic control systems and interfaces to controllers, including any safety critical operations undertaken by a human-operator. Standard IEC 61508 defines 4 performance levels for the safety functions. The safety integrity level 1 (SIL1) is the lowest one, while the safety integrity level 4 is the highest level. The standard formulates in details the requirements to be fulfilled for each safety integrity level to be achieved.

Table 1. Safety integrity levels and interval probabilistic criteria for safety-related systems

Safety integrity level (SIL)	PFD_{avg} (a system operating in a low demand mode)	*PFH* (a system operating in a high demand or continuous mode)
SIL4	$[\,10^{-5}, 10^{-4}\,)$	$[\,10^{-9}, 10^{-8}\,)$
SIL3	$[\,10^{-4}, 10^{-3}\,)$	$[\,10^{-8}, 10^{-7}\,)$
SIL2	$[\,10^{-3}, 10^{-2}\,)$	$[\,10^{-7}, 10^{-6}\,)$
SIL1	$[\,10^{-2}, 10^{-1}\,)$	$[\,10^{-6}, 10^{-5}\,)$

In order to deal - in a systematic manner - with all activities necessary to achieve the required safety integrity for the safety functions to be carried out by the E/E/PES, the standard [11] adopts an overall safety lifecycle scheme as shown in *Figure 1* that is proposed as a technical framework. All activities related to the *functional safety management* including the determination of SIL and its verification are not shown on this scheme for reasons of simplicity. They are specified for the E/E/PE system (hardware), software and human factors. The requirements for the functional safety management shall run in parallel with the overall safety lifecycle phases [11].

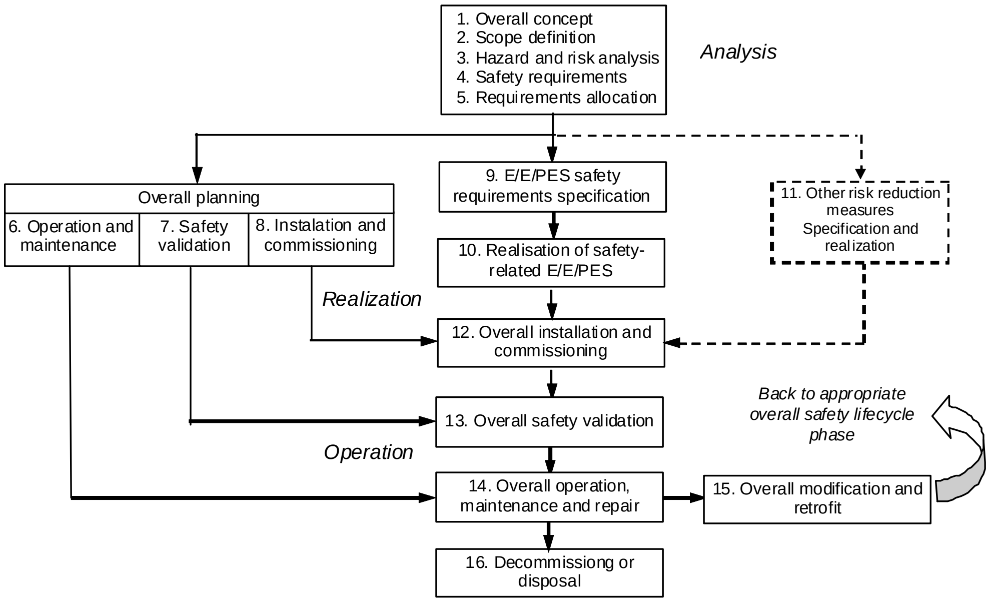

1. Overall concept
2. Scope definition
3. Hazard and risk analysis
4. Safety requirements
5. Requirements allocation
Analysis
Overall planning
6. Operation and maintenance
7. Safety validation
8. Instalation and commissioning
9. E/E/PES safety requirements specification
10. Realisation of safety-related E/E/PES
11. Other risk reduction measures Specification and realization
Realization
12. Overall installation and commissioning
13. Overall safety validation
Back to appropriate overall safety lifecycle phase
Operation
14. Overall operation, maintenance and repair
15. Overall modification and retrofit
16. Decommissiong or disposal

Figure 1. Overall functional safety-related lifecycle proposed in IEC 61508

For each safety-related E/E/PES fulfilling defined safety-related function of given SIL, two probabilistic criteria are defined in the standard [11]. The first is the average probability of failure (PFD_{avg}) to perform the design function on demand for the system operating in a low demand mode of operation. And second - the probability of a dangerous failure per hour (PFH), i.e. the frequency for the system operating in a high demand or continuous mode of operation.

These numeric probabilistic criteria expressed as intervals for consecutive SILs and two modes of operation are presented in *Table 1*.

2.2. Concept and principles of risk-informed decision making

A concept of risk-informed decision making has been developed at some regulatory and research institutions of nuclear industry in USA [9]. In the safety philosophy created the importance of addressing uncertainties as an integral part of decision-making with regard to the results of *probabilistic risk assessment* (PRA) has been emphasized. It was necessary to understand the potential impact of these uncertainties on the conclusions arrived at when the comparisons of PRA results with acceptance guidelines and some defined quantitative criteria have been made. When dealing with uncertainties, it should be clarified the use and meaning of other supporting analyses addressing some potential risk contributors not included fully transparently in the PRA [9].

Regulatory Guide (RG) 1.200 [9] states that a full understanding of the uncertainties and their impact is needed (i.e., sources of uncertainty should be identified and analyzed). Specifically an important aspect in understanding the base PRA results is knowing what are the sources of uncertainty and assumptions to understand their potential impact. Uncertainties can be either parameter or model uncertainties, and assumptions can be related either to PRA scope and level of detail or to the model uncertainties. The impact of parameter uncertainties is gained through the actual quantification process.

The assumptions related to PRA scope and level of detail are inherent in the structure of the PRA model. The requirements of the applications will determine whether they are acceptable. The impact of model uncertainties and related assumptions can be evaluated qualitatively or quantitatively. The sources of model uncertainty and related assumptions are characterized in terms of how they affect the base PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, introduction of a new initiating event etc.) [9].

In a white paper, *Risk-Informed and Performance-Based Regulation* (NRC, 1999), the Commission defined a *risk-informed* approach to regulatory decision-making that represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety [9].

In developing this process, NRC defined in 2002 a set of key principles in RG 1.174 to be followed for decisions regarding plant-specific changes to the licensing basis. Following principles are global in nature and have been generalized to all activities that are important subjects of risk-informed decision-making [9], [19]:

Principle 1: Current Regulations Met.
Principle 2: Consistency with Defense-in-Depth Philosophy.
Principle 3: Maintenance of Safety Margins.
Principle 4: Acceptable Risk Impact.
Principle 5: Monitor Performance.

Taking into account these principles some main areas of functional safety-related decision making were identified, which are shown in *Figure 2*. As it was mentioned, nowadays the programmable control and protection systems operating in networks play an important role in maintaining high performance and safety of many technical systems, in particularly in complex hazardous plants. Therefore, the relevant risk-informed analyses performed for identification of more important factors influencing performance and risk should be of a considerable interest for operators and regulators.

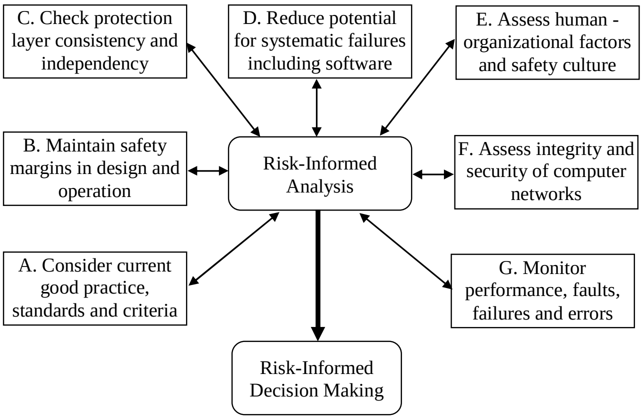

C. Check protection layer consistency and independency
D. Reduce potential for systematic failures including software
E. Assess human - organizational factors and safety culture
B. Maintain safety margins in design and operation
Risk-Informed Analysis
F. Assess integrity and security of computer networks
A. Consider current good practice, standards and criteria
G. Monitor performance, faults, failures and errors
Risk-Informed Decision Making

Figure 2. Main areas of functional safety analyses for decision making

2.3. Determining and verifying the safety integrity level for identified safety-related functions

Determining of safety integrity level (SIL) for the specific safety-related functions is one of the main stages in the functional safety analysis. The safety integrity level is directly associated with risk reduction factor associated with some analyzed automated system/process and safety-related function designed. To identify and determine overall safety requirements for this function, several analyses like hazard identification, risk assessment, risk allocation, etc. have to be executed.

Talking about technical system's risk reduction and its allocation with safety integrity levels, there are several methods to determine SIL for given safety function. These methods are qualitative, semi-quantitative or quantitative, which means how they use information about the risk parameters (descriptive or quantified). Some of more popular methodologies used in industrial practice are [3], [16]:

- risk matrix (qualitative, semi-quantitative),
- risk graph (qualitative, semi-quantitative),
- layers of protection analysis (semi-quantitative),
- strictly quantitative method.

The process of safety integrity level determination is associated with proper execution of the risk assessment for analysed safety-related function. An idea of risk can be explained as a combination of probability or frequency of some dangerous event occurrence and its consequences [11]. A value of risk is determined usually on the basis of three vector parameters function, which are [13]:

- accident scenarios,
- probability or frequency of scenarios' occurrences,
- hazardous accidents' consequences.

A measure of technical system's risk is determined by a combination of a set of accident scenarios, a set of frequencies and a set of consequences. A description of this functions can be complex and the values describing its parameters may refer to different risk parameters and measures [3]. For each accident scenario S_k two associated parameters exist: f_k – the frequency of accident scenario and n_k – its consequences leading to some losses. A formula presented below describe the risk:

$$\boldsymbol{R} = \{ < S_k, f_k, n_k > \} \quad (1)$$

If some safety-related system implementing defined safety-related function is introduced to the accident scenario then frequency of its occurrence f_k will be reduced to the value f_k^*. This concept is valid in case of n_k=*const* assumption, which means that the consequences of the accident are constant regardless of safety-related systems existence.

$$\boldsymbol{R}^* = \{ < S_k, f_k^*, n_k > \} \qquad (2)$$

The accident scenario is usually illustrated by event tree [13] (see *Figure 3*).

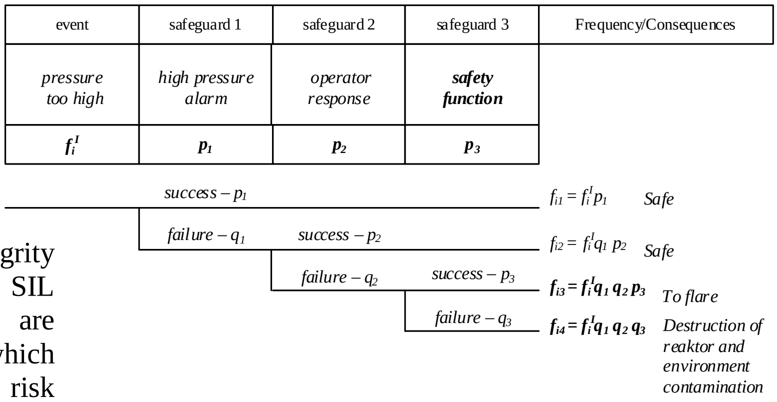


Figure 3. An example of event tree for some accident scenario

It describes some accident cases associated with the sequences of some events and their consequences as an output of the tree. Simultaneously, the existence of safety-related functions (reducing frequency from f_k to f_k^*) can be included in the tree and then can be used in the analysis process.

According to IEC 61508 the safety validation should be performed in terms of overall safety function requirements and overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related system in designing. Thus, in particular the PFD$_{\text{avg}}$ value must be verified in the probabilistic modelling process for architectures considered of given E/E/PE safety-related system taking into account the probabilistic criteria specified in Table 1 for given SIL. Some main phases within overall functional safety management process are shown with related tasks and information sources in *Figure 4* [19].

There are several sources of uncertainties to be considered in the functional safety management. In next item it is proposed to include them within a framework of *Risk-Informed Decision Making* [9].

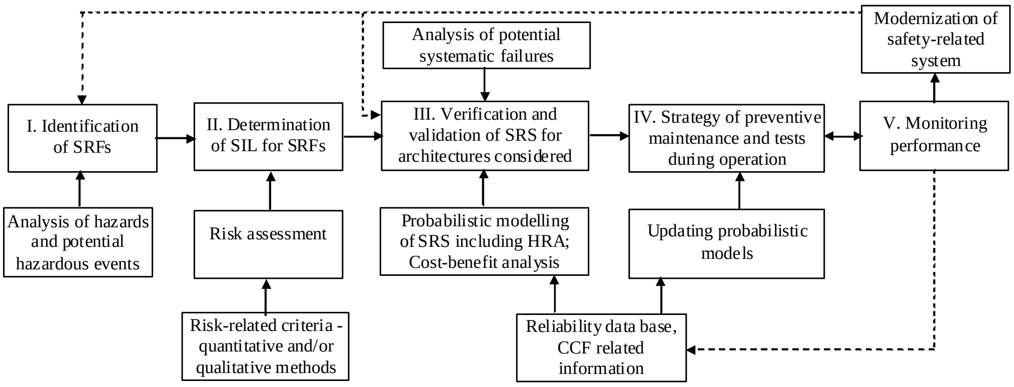

Modernization of safety-related system
Analysis of potential systematic failures
I. Identification of SRFs
II. Determination of SIL for SRFs
III. Verification and validation of SRS for architectures considered
IV. Strategy of preventive maintenance and tests during operation
V. Monitoring performance
Analysis of hazards and potential hazardous events
Risk assessment
Probabilistic modelling of SRS including HRA; Cost-benefit analysis
Updating probabilistic models
Risk-related criteria - quantitative and/or qualitative methods
Reliability data base, CCF related information

Figure 4. Main phases within overall functional safety management process

3. Uncertainty in functional safety analyses

3.1. Sources of uncertainty

Representing and assessing uncertainty is an important issue in probabilistic assessments and safety management to reach meaningful conclusions [14, 16]. The problem is to understand the relationship between a part of reality and its model. Potential sources of uncertainty are perceived at general level in relation to the abstraction and conceptualisation of reality. These issues are also relevant to representation and quantification of uncertainty in risk analysis and then risk assessment.

The idea of inherently random phenomena in nature can be refuted, especially when two kinds of the risk models are distinguished, namely generic and plant specific [13], [14]. In this context there are difficulties to acquire data as parameters of probabilistic and risk models. Often, due to lack of plant specific data it is necessity to use generic data with subjective corrections with regard to relevant influencing factors. Some failure events, especially those related to human errors, rooted organisational deficiencies, are modelled with regard to qualitative and more or less fuzzy quantitative information. In such a case using only a Bayesian framework for quantitative probability evaluations and uncertainty assessment is a subject of discussions between researchers.

In recent years efforts of the scientific community have focused on distinguishing between different types of uncertainty, leading to some controversy about the validity of such *uncertainty types* categorisations. Uncertainty has been generally classified as being basically of two types: *epistemic uncertainty* (reducible), arising from a limited knowledge about the system, and *aleatory uncertainty* (irreducible), arising from a property of the system, which can behave in different ways, being inherently or to some extent stochastic [9], [19].

Uncertainty is induced also in terms of the model uncertainty due to our inability to validate with certainty the set of assumptions in the system conceptualisation. Views are also presented that the apparent randomness of nature is not an inherent characteristic, but rather is the result of limitations to carry out observations and measurements to acquire relevant knowledge. Randomness of nature is also being treated as a way of our limited understanding of the reality slice under investigation. Thus, it is rather a source of uncertainty stemming from inherent vagueness.

In the functional safety analyses and management two main problems of uncertainties characterization have been identified, namely uncertainties related to the determination of required safety integrity level (SIL) for given SRF (see block I and II in *Figure 4*), and uncertainties related to the verification of safety integrity level for SRS performing consecutive safety-related function (see block III and IV in *Figure 4*). They are shown respectively on *Figure 5* and *Figure 6*. The identification and characterization of epistemic and aleatory uncertainties are related to:

- model selected or developed and assumptions;
- model uncertainties; completeness uncertainties; parametric uncertainties.

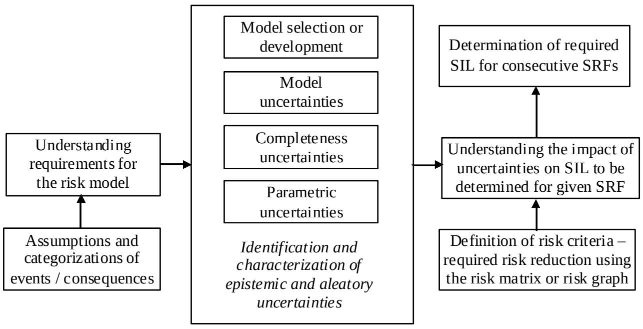

Model selection or development
Model uncertainties
Completeness uncertainties
Parametric uncertainties
Identification and characterization of epistemic and aleatory uncertainties
Understanding requirements for the risk model
Assumptions and categorizations of events / consequences
Determination of required SIL for consecutive SRFs
Understanding the impact of uncertainties on SIL to be determined for given SRF
Definition of risk criteria – required risk reduction using the risk matrix or risk graph

Figure 5. Uncertainties related to the determination of required safety integrity level

Obviously in both cases to be considered the nature of uncertainty is different. In first case it is related to the risk analysis and assessment for the risk criteria defined. In second case uncertainty is associated with probabilistic modeling of systems and interval probabilistic criteria for relevant operating modes as specified in *Table 1*.

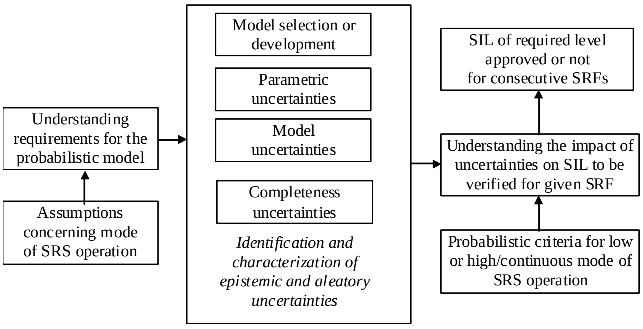
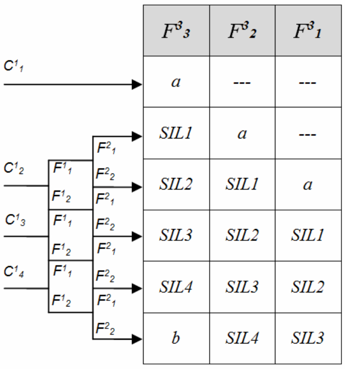

Understanding requirements for the probabilistic model
Assumptions concerning mode of SRS operation
Model selection or development
Parametric uncertainties
Model uncertainties
Completeness uncertainties
Identification and characterization of epistemic and aleatory uncertainties
SIL of required level approved or not for consecutive SRFs
Understanding the impact of uncertainties on SIL to be verified for given SRF
Probabilistic criteria for low or high/continuous mode of SRS operation

Figure 6. Uncertainties related to the verification of safety integrity level

3.2. Factors and uncertainties related to determining required safety integrity levels

The functional safety analysis basically relies on some information taken from the process of hazard identification as well as further risk assessment of designed or existing control systems in a technical installation. The level of risk associated with those systems is assessed on the basis of some risk factors which influence the frequency in some way as well as the consequences. The frequency parameter is basically associated with reliability of the control or protection system (which consists of hardware and software), human factors and some security issues [1], [2], [3]. It can be determined using relevant methods. If a reliability data of risk factors is provided and well known, the risk assessment process can be done quantitatively [7]. Otherwise, it should be performed using one of the qualitative or semi-quantitative methods. A basic and simple method used in the functional safety analysis is the risk graph, which should be appropriately calibrated.

An example of standard risk graph with already assigned SILs is presented on *Figure 7*.



F^3_3	F^3_2	F^3_1
a	---	---
SIL1	*a*	---
SIL2	*SIL1*	*a*
SIL3	*SIL2*	*SIL1*
SIL4	*SIL3*	*SIL2*
b	*SIL4*	*SIL3*

Figure 7. Example of standard risk graph [12]

A conventional set of four risk parameters in risk graph method is: the consequence (C^1), the frequency and exposure time (F^1), the possibility of failing to avoid hazard (F^2) and the probability of unwanted occurrence of potential events that demand the operation of given E/E/PE safety-related system (F^3). Each risk parameter owns some features and characteristics which help better estimating quantitative values or descriptive ranges are ascribed to them [1].

Talking about risk graphs, the characteristics of risk parameters associated with this method can be suggested. For example, the F^3 parameter may be considered using some features like:

- presence of other independent layers of protection,
- historical data about presence of similar accidents in the past,
- reliability of equipment installed,
- human factors,
- security issues, etc.

The probability of avoiding hazard F^2 can be estimated with some other factors like:

- process dynamics,
- time needed to create hazard after the incident occurs,
- local access to the process main indicators by operators,
- process staff and operators training, etc.

The frequency or exposure time F^1 may be associated with some other parameters, e.g.:

- density of population in hazardous area,
- shift work presence,
- work organization and management,
- temporary operations (like repairs or inspections) in hazardous area, etc.

The consequences *C* parameter may depend on:

- category of object or system,
- substances and materials using in the process,
- weather related factors,
- high-level plant administration, etc.

Each risk parameter (C^1, F^1, F^2 and F^3) gives a portion of information about the presence of risk in the technical object and leads to assess the proper required risk reduction level, which is associated directly with required safety-related function SIL. The process of such risk assessment is usually preceded by a detailed hazard identification, accident scenario determination and preliminary risk categorization for each most representative scenarios. During those stages some important information about analyzed installations and systems are gathered and used later in the risk assessment method, eg. risk graph by team of experts and different fields specialists. Their knowledge and correctness of gathered data is one of the most important (after appropriate choose of assessment method and its calibration [3]) condition to ensure proper and best quality results of functional safety analysis and SIL determining process. The expert knowledge is needed during all steps of risk assessment.

It is better to make accessible more risk parameter criteria ranges, which covers narrower intervals of values or more detailed description of them. But this should be done in the first stage associated with defining risk parameters and building appropriate method [7], eg. modifiable risk graph [3], [4]. Other approach is related to representation of fuzzy perception of the risk parameters and experts knowledge. This approach requires well defined framework to ensure that experts' opinions will be collected and used appropriately. This kind of approaches and frameworks are described precisely in the articles [20] and [21].

The RIDM approach is justified in functional safety management, because it will help in understanding more important factors influencing risk.

3.3. Verifying SIL of safety-related functions with regard to contribution of common cause failures

For verifying SIL of the E/E/PE system or SIS the quantitative method based on the reliability block diagram (RBD) is often used. There is also known problem to determine the value of β-factor representing potential CCF (*common cause failure*) for given redundant system [1], [10], [22]. For practical reasons a knowledge-based approach can be applied, similarly as in IEC 61508, based on scoring of factors influencing potential dependent failures. There are proposals in some references to evaluate β factor depending on architecture of redundant systems considered, for instance in [10] as follows

$$\beta_{k\ oo\ n} = \beta \cdot c_{k\ oo\ n} \qquad (3)$$

where: β is the base factor for a simple architecture 1oo2 and the $C_{k\ oo\ n}$ is a coefficient for actual architecture of the system. The values of C_{koon} have been proposed as follows: $C_{1oo2}=1$; $C_{1oo3}=0.5$; $C_{2oo3}=1.5$ [1], [10]. The value of basic β factor is assumed with regard to properties of the (sub)system considered and other factors related to the site of system installation.

The safety instrumented system in designing (Fig. 8) consists of: the pressure sensors PS (subsystem ssPS) - 2oo3, the temperature sensors TS (subsystem ssTS) - 2oo3, the programmable logic controller PLC 1oo2 and the actuator subsystem (redundant valves SVA) 1oo2.

The value of PFD_{avg} for given SIS was calculated using the reliability data from *Table 2*. The component reliability data and parameters of a probabilistic model are given in *Table 3*.

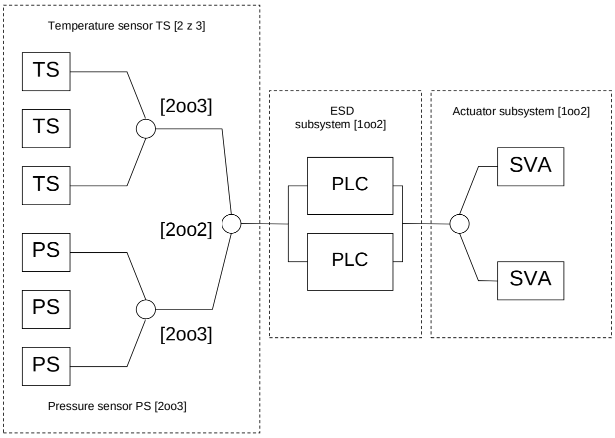

Temperature sensor TS [2 z 3]
TS
TS
TS
[2oo3]
[2oo2]
PS
PS
PS
[2oo3]
Pressure sensor PS [2oo3]
ESD
subsystem [1oo2]
PLC
PLC
Actuator subsystem [1oo2]
SVA
SVA

Figure 8. An example of SIS hardware architecture

The analysis of results obtained indicates that for SIS presented in *Figure 8* the PFD_{avg} value is equal $9.75 \cdot 10^{-4}$, fulfilling the requirement of SIL3 (for PLC $\beta = 1\%$). For β factor 2% the resulting value for this SIS is $1.02 \cdot 10^{-3}$, fulfilling the requirement of SIL2. In PFD_{avgSYS} calculation for this SIS the point value for slightly different β factor can be near the upper or lower limits of relevant criteria ranges resulting in different SIL. For instance, for the PLC $\beta = 1\%$ PFD_{avgSYS} is equal $9.75 \cdot 10^{-4}$, fulfilling formally requirement of SIL3 but for higher value of β the PFD_{avgSYS} is much higher, in the interval of probabilistic criterion for SIL2.

Table 2. The SIL verification report for SIS including CCF data

System /subsystems /elements		**KooN**	**β [%]**	**PFD_{avg}**	**SIL**	**x_i [%] PFD_{avgS}**
SIS	**0**	**-**	**-**	**$9.75 \cdot 10^{-4}$**	**3**	100
ssTS	**.1**	**2oo3**	**2**	**$4.52 \cdot 10^{-4}$**	**3**	**46.4**
TS	..2	-	-	$1.31 \cdot 10^{-2}$	1	-
TS	..2	-	-	$1.31 \cdot 10^{-2}$	1	-
TS	..2	-	-	$1.31 \cdot 10^{-2}$	1	-
ssPS	**.1**	**2oo3**	**2**	**$2.74 \cdot 10^{-5}$**	**4**	**2.9**
PS	..2	-	-	$1.31 \cdot 10^{-3}$	2	-
PS	..2	-	-	$1.31 \cdot 10^{-3}$	2	-
PS	..2	-	-	$1.31 \cdot 10^{-3}$	2	-
ESD	**.1**	**1oo2**	**1**	**$3.97 \cdot 10^{-4}$**	**3**	**40.7**
PLC	..2	-	-	$2.19 \cdot 10^{-2}$	1	-
PLC	..2	-	-	$2.19 \cdot 10^{-2}$	1	-
asSV	**.1**	**1oo2**	**2**	**$9{,}78 \cdot 10^{-5}$**	**4**	**10.0**
SVA	..2	-	-	$3.52 \cdot 10^{-3}$	2	-
SVA	..2	-	-	$3.52 \cdot 10^{-3}$	2	-

Table 3. Component reliability data and parameters of a SIS probabilistic model

	SVA	**PLC**	**PS**	**TS**
DC [%]	24	66	54	66
λ_{DU} [1/h]	$8\cdot10^{-7}$	$5\cdot10^{-6}$	$3\cdot10^{-7}$	$3\cdot10^{-6}$
MTTR [h]	8	8	8	8
T_I [h]	8760	8760	8760	8760
β	0.02	0.01	0.02	0.02

Presented above case is rather a simple one. It is known that the probability measure of E/E/PE (or SIS) failure is generally a function of some variables, e.g. $PFD_{avgi} = f(\lambda_i, \beta_i, MTTR_i, DC_i, T_{Ii})$. Each parameter of probabilistic model influences to some extent the system failure probability. Final values of PFD_{avg} (or PFH) depend on respective parameters, and are very sensitive to β factor representing potential dependent failures.

4. Conclusion

Due to complexity of the functional safety management in industrial hazardous plants, to overcome difficulties in decision making under significant uncertainties, we propose to apply the methodology of risk informed decision making (RIDM). The methodology proposed and outlined in this paper is compatible with the functional safety management methodology described in IEC 61508. It enables to carry out the decision making in a more transparent and systematic way. In the methodology proposed the overall functional safety management (FSM) in life cycle includes the RIDM and periodical risk reassessment based on performance monitoring of the installation as well as faults and failures of programmable control and protection systems. In the future, the proposed framework should integrate the functional safety and security issues. During the process of SIL determining, the security aspect should be considered as a risk parameter affecting also uncertainty of results obtained from analyses. On the other hand, in the SIL verification stage, the result of security analysis can affect uncertainty of probabilistic model parameters.

Acknowledgments

The research outlined in this paper 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. & Śliwiński, M. (2007). *Methods for verification safety integrity level in control and protection systems, Functional Safety Management in Critical Systems*. Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk, pp. 171-185.

[2] Barnert, T., Kosmowski, K.T. & Śliwinski, M. (2008). Security aspects in verification of the safety integrity level of distributed control and protection systems. *Journal of KONBIN*. Air Force Institute of Technology, Warsaw.

[3] 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.

[4] Barnert, T., Kosmowski, K.T. & Sliwinski, M. (2008). Determining and verifying the safety integrity level of the control and protection systems under uncertainty. Taylor & Francis Group, *European Safety & Reliability Conference ESREL 2008*, Valencia. London.

[5] 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. *PSAM, Seattle*.

[6] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2010). A method for including the security aspects in the functional safety analysis of distributed control and protection systems. *ESREL*, Rhodes, Greece.

[7] Baybutt, P. (2007). An improved risk graph approach for determination of safety integrity level (SILs). *Process Safety Progress*, Vol. 26.

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

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

[10] Hokstad, P. (2004). A generalisation of the beta factor model. *Proceedings of the European Safety & Reliability Conference*, Berlin.

[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] Kosmowski, K.T. (2002). *Methodology for the risk analysis in reliability and safety management of nuclear power plants* (*in Polish*). Gdansk University of Technology, Gdansk.

[14] Kosmowski, K.T. (2004). Incorporation of human and organizational factors into qualitative and quantitative risk analyses. *Proceedings of the International Conference on Probabilistic Safety Assessment and Management*, PSAM 7 - ESREL '04, 2048-2053.

[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. (2007). *Functional Safety Management in Critical Systems*. Gdansk University of Technology. Wydawnictwo Fundacji Rozwoju Uniwersytetu Gdańskiego. Gdańsk.

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

[18] Kosmowski, K.T., Sliwinski, 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.

[19] 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.

[20] Nait-Said, R., Zidani, F. & Ouzraoui, N. (2008). Fuzzy Risk Graph Model for Determining Safety Integrity Level. *International Journal of Quality, Statistics, and Reliability*.

[21] Simon, C., Sallak, M. & Aubry, J. (2007). SIL allocation of SIS by aggregation of experts' opinions. *Proceedings of the Safety and Reliability Conference* (ESREL '07), Stavanger.

[22] SINTEF (2010). Reliability Data for Safety Instrumented Systems - PDS Data Handbook. Edition, SINTEF A13502.

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