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

Current challenges and methodological issues of functional safety and security management in hazardous technical systems

Keywords

functional safety, safety integrity level (SIL), information security, evaluation assurance level (EAL)

Abstract

The aim of this article is to identify problems of the risk assessment of the *electric / electronic / programmable electronic* (E/E/PE) *systems* concentrating on the *functional safety* and *security* aspects. These aspects should be considered in an integrated way in the system life cycle. The role of *functional safety solutions* is effective reducing the risk from unacceptable level. The risk is defined as a combination of the probability of occurrence of harm and the severity of that harm. *Security* is concerned with the protection of assets including the E/E/PE systems or *safety instrumented systems* (SISs) from potential threats including *cyber attacks*. This article deals with current challenges and methodological issues of integrating the functional safety and security aspects of the programmable systems' operation for the control and protection of hazardous industrial systems.

1. Introduction

A main difficulty in integrating the safety and security analyses and assessments is the fact that they consist of two different kinds of requirements. In case of programmable control and protection systems the security management is aimed at the protection of assets such as: information, data, computer and peripherals, communication equipment and installations, power supplies, system and application programs, etc. [1], [2], [15], [19]. In this case, the risk is associated with some categories of generally understood objects (including data and software modules) that have to be protected with regard to required levels of such attributes as [12], [23]:

- confidentiality: ensuring that information is accessible only to authorized users,
- integrity: safeguarding the accuracy and completeness of data and processing methods,
- availability: ensuring that authorized users have access to the system and associated assets when required.

The potential causes of losses are threats, which may be natural, technical or human and they should be included in the security oriented risk analyses [12]. The role of protecting the assets of interest, including information, is especially important when the control and protection systems are decentralized and use different data communication channels [22].

On the other hand, the functional safety can 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 standards [9, 11] and is applied in the process of design and operation of safety-related *electric, electronic and programmable electronic* (E/E/PE) *systems* [9] or *safety instrumented systems* (SISs) [10] in case of process industry. These systems perform specified functions to ensure that risk is maintained at acceptable level.

Two different requirements are to be specified to ensure appropriate level of functional safety [9]:

- 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 [3], [7], [14].

Two types of operation modes are usually considered in functional safety analysis: (1) *low*, and (2) *high* or *continuous*. A low demand mode is usually found in the process industry systems, but high or continuous one appears in machinery or transportation systems.
The SISs are especially important for the safety of industrial distributed installations. They contribute often in integrated operations and there is a need for remote access to such systems from vendors external to the operating company. This kind of access will go through a number of networks used for other purposes, including the open Internet [20]. This raises a number of security issues, ultimately threatening the safety integrity of SISs.
This article deals with current challenges and methodological issues of integrating the functional safety and security analyses of the programmable systems' operation for the control and protection of industrial hazardous systems.

2. Functional safety management of the control and protection systems

2.1. Designing the safety-related functions and systems

Modern industrial plants are equipped with complex programmable control and protection systems operating usually witin a computer network. For designing such systems a functional safety concept [9] is more and more widely of interest, to be implemented in various industrial sectors, including the process industry [10].
However, 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 failures and software faults, common cause failures (CCFs), functional dependencies of equipment and barriers, human errors, organisational factors, security, etc. [14].
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-related functions (SRFs) that are to be implemented using programmable control and protection systems.
The human-operator contributes to realization of given SRF through relevant *human machine interface* (HMI) to be designed in relation to the functions of SCADA (*supervisory control and data acquisition*) system or DCS (*digital control system*) and in some cases an independent *alarm system* (AS) is required.
The standard IEC 61511 [10] distinguishes two kinds of programmable systems, namely the *basic process control system* (BPCS) and the *safety instrumented systems* (SISs). They are designed according to the technical specifications and procedures developed for normal, transient and abnormal situations, but their functions are especially important in situations of emergency conditions.
An important term related to the functional safety concept is the *safety integrity* [9], understood as the probability that given safety-related system will satisfactorily perform required SRF under all stated conditions within given period of time.
The *safety integrity level* (SIL) is a discrete level (from 1 to 4) for specifying the safety integrity requirements of given safety-related functions to be allocated using the E/E/PE system [9] or the SISs [10]. The safety integrity of level 4 (SIL4) is a highest level, which requires - when required in given SRF solution – a complex system architecture consisting of redundant subsystems [3], [16], [18].
For the E/E/PES or SIS performing a SRF two probabilistic criteria are defined (*Table 1*) for consecutive SILs namely [9]:

- 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 a high demand or continuous mode of operation.

Table 1. Probabilistic criteria to be assigned for safety-related functions

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})

The SIL for given SRF is determined e.g. in the qualitative risk assessment process using a defined risk matrix, which includes areas of several risk classes, *e.g.* unacceptable, moderate and acceptable, or a risk graph [9].

The E/E/PE safety-related system shown in *Figure 1* consists of following subsystems: (A) input devices (sensors, transducers, converters, *etc.*), (B) programmable logic controllers, *e.g.* PLC and (C) output devices including the equipment under control (EUC). The architecture of these subsystems is determined during the design process. Each logic controller comprises the central 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 [9], [16].

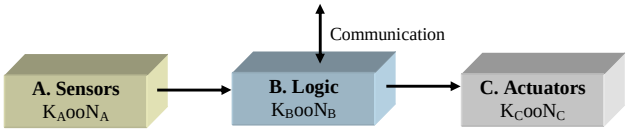


Figure 1. General architecture of E/E/PES or SIS consisting of redundant subsystems for realization of safety-related function

2.2. Layers of protection and dependency problems

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 [16], [21].

Figure 2 shows typical layers of protection of in a hazardous industrial plant. An interesting methodology for preliminary risk analysis and safety-related decision-making is the layer of protection analysis (LOPA) methodology [10].

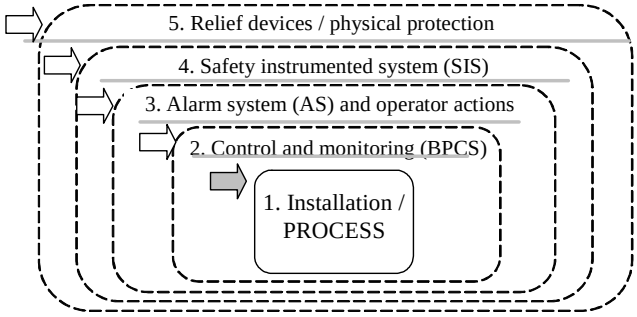


Figure 2. Typical protection layers in hazardous industrial installation

The protection layer (PL) should be [16]:

- *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).

Figure 3 illustrates the protection layers that include *Basic Process Control System* (BPCS), *human operators* and *Safety Instrumented System* (SIS). These systems should be functionally and structurally independent; however, it is not always possible in industrial practice.

Fig. 4. illustrates potential structural and functional dependencies of three protection layers (PLs): 2, 3 and 4 shown in *Figure 2*. These layers include:

- PL1 – *basic process control system* (BPCS),
- PL2 – *human-operator* (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).

Thus, an important part of such complex system is the human-machine interface (HMI).

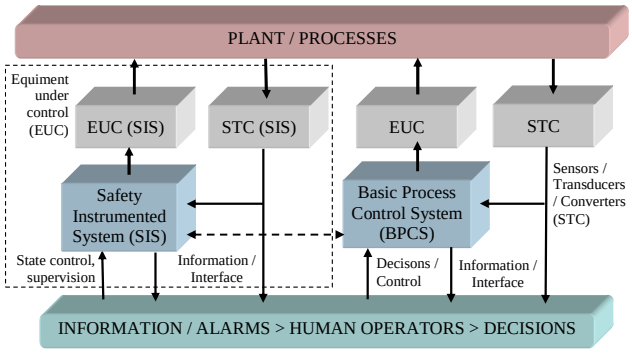


Figure 3. Components of safety-related systems for monitoring, control and protection

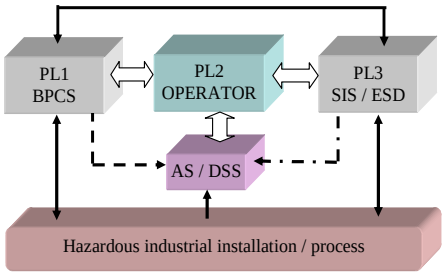


Figure 4. Operator and alarm system / decision support system (AS/DSS) as components of protection layers

The design process of the control and protection systems in a hazardous plant is presented in *Figure 5*. It includes preliminary risk analysis and defining safety-related functions, determining the risk mitigation and control strategy, designing BPCS with regard to decision support system (DSS), human-machine interface (HMI) and alarm system (AS).

Selected issues of the alarm system designing were outlined in publications [13], [17]. The research challenges in this area includes man-machine interaction and contextual human reliability analysis (HRA) with regard to cognitive aspects of operators' behavior who undertake coordinated team actions when abnormality occur [16].
The safety-related functions to be implemented using SIS are designed for given SIL determined during the risk analysis and assessment. The final solution proposed, including algorithms of actions and related software, has to be verified and validated according to requirements and procedures given in IEC 61508 [9] and IEC 61511 [10].

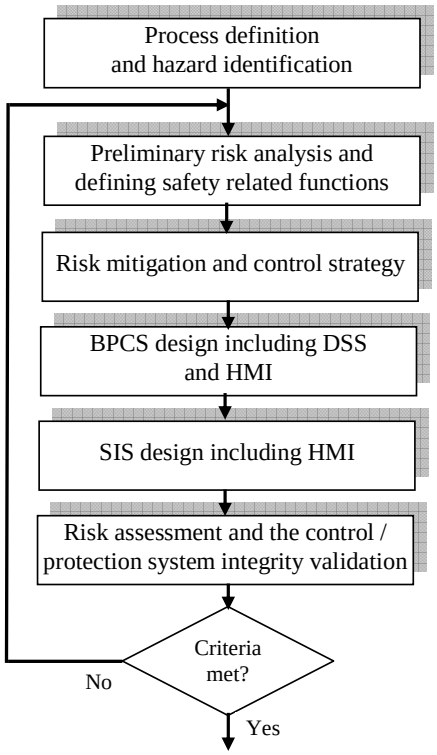


Figure 5. The design process of programmable control and protection systems

2.3. Some trends in development of safety instrumented solutions and dependency issue

As the industrial users are becoming more knowledgeable about safety issues, they perform more accurately extensive hazard identification and risk analysis to determine needs for the installation protection. To reduce the cost of configuration, training, and technical support, some users consider the possibility of closer integration of the control and protection systems. It includes such aspects as field wiring and gathering diagnostic data from the devices. Thus, the users are looking to employ high-integrity fieldbusses in safety-related applications. Finally, they are interested to have better tools for safety lifecycle management and flexible architectures that enable increased scalability [1].
In the past, most manufacturers required the process control systems to be completely independent from their emergency shutdown systems. Some have even assumed that the BPCS and the SIS have to be supplied from different manufacturers to reduce the possibility of common cause failures (CCF). Thus, there were and still are some good reasons to put the safety and control functions in different controllers. These precautions are justified form the point of view [1]:

- Avoiding dependent failures to minimize the risk of simultaneous failures within the control systems and protection systems (e.g. BPCS and SIS);
- Increasing security to prevent danger changes in programmable control and protection systems from causing any change or fault in BPCS and SIS;
- Different requirements for the BPCS and SIS; BPCS is usually designed for maximum availability, but a SIS is normally designed to fail in a safe way and has special features like extended diagnostics, software error checking, protected data storage, fault tolerance, etc.

Such advanced solutions as regards the safety attributes are in use for instance in the nuclear power industry applications, as described in an international standard IEC 61513.
Some new integrated solutions with particular functional characteristics and relations between BPCS and SIS are also proposed as shown in *Figure 6.*

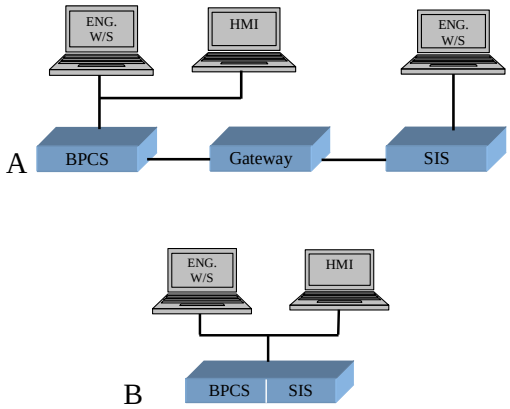


Figure 6. Integrating of SIS with BPCS [1]:
A. Interfaced, and B. Common

Some suppliers of the control and protection systems offer now similar systems for either functionality, which incorporate similar HMI, configuration procedures, programming languages, and

maintenance procedures. The key issue is to ensure that such two systems are separate as regards different hardware and software solutions, even though they have a common configuration, operations and maintenance interface [1].
The benefits of such integrated solutions as regards the safety and security characteristics are not clear and there are still more challenges concerning such integration to be solved before implementation in industrial practice [17].

2.4. Additional requirements for data communications

When data communication is used in the implementation of a safety function then the failure measure, such as the probability of undetected failure, of the communication process shall be estimated taking into account transmission errors, repetitions, deletion, insertion, re-sequencing, corruption, delay and masquerade (the term masquerade means that the true contents of a message are not correctly identified [9]. For example, a message from a non-safety element is incorrectly identified as a message from a safety element. This failure measure shall be taken into account when estimating the failure measure of the safety function due to random failures.
The techniques and measures necessary to ensure the required failure measure (e.g. the probability of undetected failure) of the communication process shall be implemented according to the requirements of this standard and IEC 61508-3. This allows two possible approaches:
– the entire communication channel shall be designed, implemented and validated according to IEC 61508 (a so-called 'white channel' - see Figure 7a), or
– parts of the communication channel are not designed or validated according to IEC 61508 (a so-called 'black channel' see Figure 7b); in this case, the measures necessary to ensure the performance of the communication process shall be implemented in the E/E/PE safety-related elements that interface with the communication channel in accordance with IEC 62280 [9].

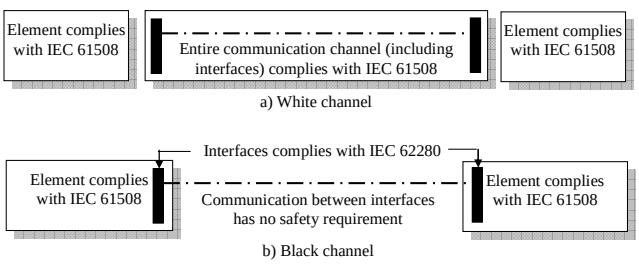


Figure 7. Architectures for data communication [9]

The E/E/PE safety-related system shall be integrated according to the specified E/E/PE system design and shall be tested according to the specified E/E/PE system integration tests. As part of the integration of all modules into the E/E/PE safety-related system, the E/E/PE safety-related system shall be tested as specified. These tests shall show that all modules interact correctly to perform their intended function and are designed not to perform unintended functions [9].
The integration of safety-related software into the E/E/PE safety-related system shall be carried out according to item 7.5 of IEC 61508-3. Appropriate documentation of the integration testing of the E/E/PE safety-related system shall be produced, stating the test results and whether the objectives and criteria specified during the design and development phase have been met. If there is a failure, the reasons for the failure and its correction shall be documented. During the integration and testing, any modifications or change to the E/E/PE safety related system shall be subject to an impact analysis which shall identify all subsystems and elements affected and the necessary re-verification activities.
The E/E/PE system integration testing shall document the following information [9]:
a) the version of the test specification used;
b) the criteria for acceptance of the integration tests;
c) the version of the E/E/PE safety-related system being tested;
d) the tools and equipment used along with calibration data;
e) the results of each test;
f) any discrepancy between expected and actual results;
g) the analysis made and the decisions taken on whether to continue the test or issue a change request, in the case when discrepancies occur.

3. Problems of information security management in industrial distributed systems

3.1. Security related concepts and challenges

The SISs are especially important for the safety of industrial distributed installations. They contribute often in integrated operation and there is a need for remote access to such systems from vendors external to the operating company. This kind of access will go through a number of networks used for other purposes, including the open Internet. This raises a number of security issues, ultimately threatening the safety integrity of SIS [20].
The international standards [9] define respectively the safety and security follows:

- *safety* is a freedom from unacceptable risk, where risk is a combination of the probability of occurrence of harm and the severity of that harm;
- *security* is concerned with the protection of assets from threats, where threats are categorised as the potential for abuse of assets.

The multipart standard ISO/IEC 15408 [11] defines criteria referred to as the *Common Criteria* (CC), to be used as the basis for evaluation of security properties of IT products and systems. The CC permits comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.

The CC is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. For evaluation an IT product or system is known as a *Target of Evaluation* (TOE). Such TOEs include, for instance, operating systems, computer networks, distributed systems, and applications.

The CC addresses protection of information from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called *confidentiality*, *integrity*, and *availability*, respectively. The CC may also be applicable to aspects of IT security outside of these three. The CC concentrates on threats to that information arising from human activities, whether malicious or otherwise, but may be applicable to some nonhuman threats as well. In addition, the CC may be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.

The CC is applicable to IT security measures implemented in *hardware*, *firmware* or *software*. Where particular aspects of evaluation are intended only to apply to certain methods of implementation, this will be indicated within the relevant criteria statements.

Security Function (SF) is a part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TOE *Security Policy* (TSP). *TOE Security Functions (TSF)* is defined as a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP. *TOE Security Policy (TSP***)** is considered as a set of rules that regulate how assets are managed, protected and distributed within a TOE.

The security concept proposed in the standard ISO/IEC 15408 is shown in Fig. 8. Security is considered with the protection from threats, where threats are categorized as the potential for abuse of assets. All categories of threats should be considered, but in the domain of security greater attention is given to those threats that are related to malicious or other human activities.

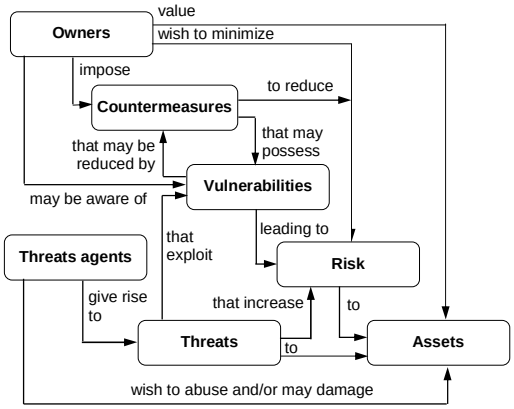


Figure 8. Security concepts and relationships [11]

The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable [5], [6].

3.2. Vulnerability assessment and evaluation assurance levels

The *Security Assurance Requirements* are grouped into classes. There are 8 assurance classes of the CC described in Part 3 of ISO/IEC 15408 [11]:

- Configuration management,
- Guidance documents,
- Vulnerability assessment,
- Delivery and operation,
- Life cycle support,
- Assurance maintenance,
- Development, and
- Test.

Each of these classes contains some members named families, which are grouping the sets of security requirements (*Figure 9*). The members of given family are components that describe a specific set of security requirements and are the smallest selectable set of security. The set of components in a family may be ordered to represent increasing strength or capability of security requirements. The Evaluation assurance levels (EALs) for selected vulnerability assessment class are presented in *Table 2*.

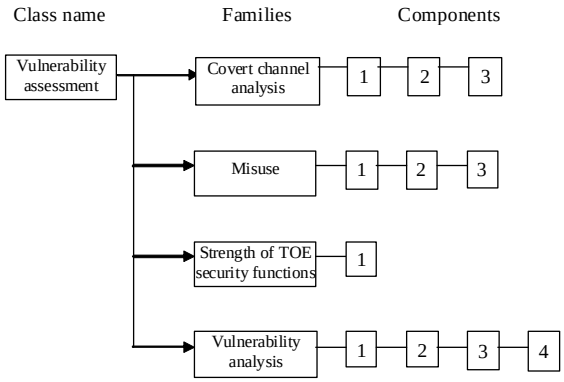


Figure 9. Decomposition diagram of selected vulnerability assessment class [11]

Table 2. Evaluation assurance levels for selected vulnerability assessment class [11]

Assurance Family	Assurance components by EAL						
	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Covert channel analysis					1	2	2
Misuse			1	2	2	3	3
Strength of TOE security functions		1	1	1	1	1	1
Vulnerability analysis		1	1	2	3	4	4

Consecutive EAL can be described as follows:
EAL1 – functionally tested,
EAL2 – structurally tested,
EAL3 – methodically tested and checked,
EAL4 – methodically tested, designed and reviewed,
EAL5 – semi-formally designed and tested,
EAL6 – semi-formally verified design and tested,
EAL7 – formally verified design and tested.
The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.
Determination of assets' *sensitivity* and *criticality*, especially information and data, is needed to protect them from unauthorized disclosure, fraud, abuse or waste [3], [4], [5].
Sensitivity is determined depending on the type of information. Level 1 applies to information that requires a minimal amount of protection. Level 2 (moderate sensitivity) can include information that must be protected. Level 3 consists of the most sensitivity information that requires the greatest security protection.
Criticality refers to processing capabilities. Level 1 applies to automated information system including software and hardware that have minimal influence on the protected object in case of failure. Level 2 identifies important automated information systems. Level 3 (high criticality) refers to the system which failure, even for short period of time, lead to loss important assets.
Thus, IT product or system should have appropriate protection. This safeguard is strictly connected with estimated levels of sensitivity and criticality. The strength of security level may be determined by rings of protection (*Figure 10*). Depending on the EALs the amount of the rings of protection is increasing. Outer ring of protection is connected with the highest EAL levels.

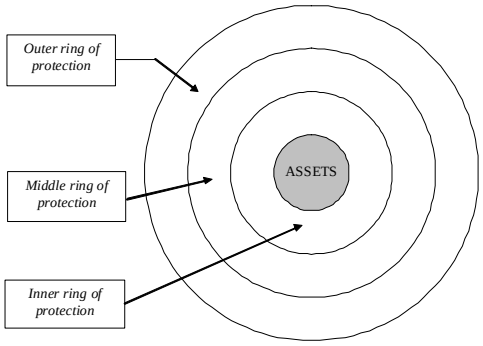


Figure 10. Rings of protection

Both sensitivity and criticality are related to the security risk analysis. Main aspects of this analysis are threat assessment and vulnerability assessment. *Threat assessment* is a process which identifies specific classes of adversaries that may perpetrate the security-related events. It consists of adversary identification process and adversary characterization, which can be helpful in determining the adversary's capabilities and motivation. *Vulnerability assessment* is useful to find existence of exploitable covert channels, the possibility of misuse or incorrect configuration of the TOE [11].

4. Proposal for integrating the safety and security aspects

4.1. Designing critical systems with regard to the safety and security aspects

As it was emphasised in the process of system development and its operation both safety and security aspects should be exhaustively considered and implemented as integrated solution in a rational way. In *Figure 11* a conception is proposed for integrated safety and security management in life cycle of critical systems.

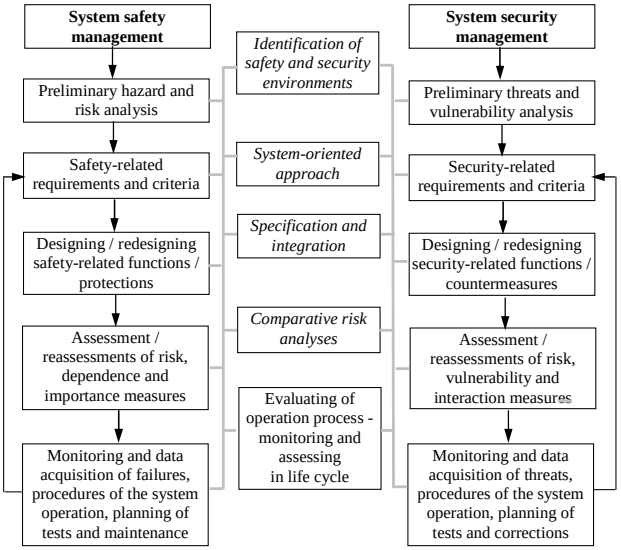


Figure 11. The development and operation of critical systems including safety and security aspects

Although the conceptions of the safety and security of programmable systems (in general IT) are generally outlined in standards [9] and [11, 12], respectively, additional research effort should be undertaken to develop integrated, systemic oriented methodology. Following problems require special attention to be successfully solved:

- identifying relevant hazards and threats for distinguished categories of systems and their environment,
- modeling the system performance with regard to safety and security aspects,
- identifying more important technical and organizational factors influencing risk,
- integrated risk assessment with regard to quantitative and qualitative information,
- designing adequate countermeasures including technical and organizational solutions for effective risk reducing,
- development of integrated safety and security policy.

4.2. A method for integrated safety and security analysis

The classification of computerized systems is useful for the integrated design and operation requirements with reference to general safety and security aspects. A critical object can be classified into three main categories [2], [3], [4], [5]:

I. Concentrated critical objects/plants (e.g. refinery, chemical plant, military plant, etc.),
II. Distributed critical objects/installations, where protection and monitoring system data can be send by outside communication channels (e.g. gas pipeline, energy system),
III. Distributed critical systems, where protection and monitoring system data is to be sending by outside communication channels (e.g. transportation systems like railway, aviation, road protection and monitoring, etc.).

Proposed classification is related to a data transfer methods and means between subsystems. Important data can be transmitted by: (I) an internal network system – a first category system, (II) using external communication channels (e.g. stationary networks, gsm, satellite communication) – a second category system, or (III) both – a third category system.

Taking into consideration outlined above classification of computerized critical systems the method of integration safety and security is proposed. Concentrated critical systems (e.g. chemical plant) using the internal network (e.g. cable, Ethernet, optical fiber, etc.) require independent safety and security analyses, which integration is at present also advisable for some solutions, especially for hazardous systems.

When a critical system data transfer network consists of external communication channel (II or III category) the problem with integration safety and security aspects occurs. It is especially important in cases of designing and operating SCADA systems in hazardous distributed plants systems which belong to the critical infrastructure.

The idea for evaluating, respectively SIL for safety analysis and EAL for security analysis, is illustrated in *Figure 12*.

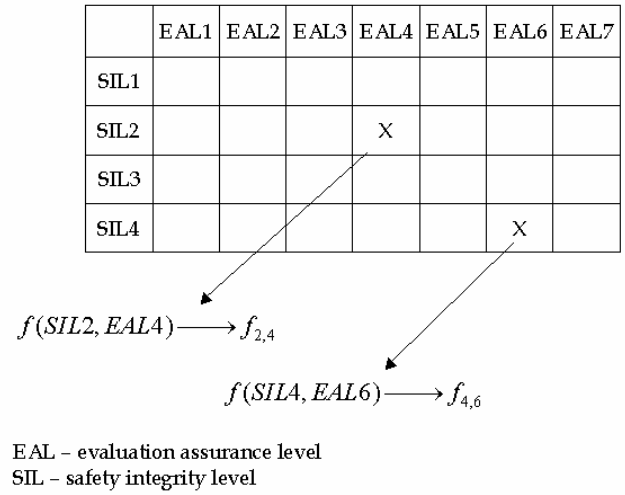


Figure 12. Proposal for integrated safety and security evaluations for systems of II and III category

For integrating relevant levels of SIL and EAL a two parametrical function, which characterizes given system, is defined. Thus, in case of distributed

plant/system of second or third category, relevant SIL and EAL has to be characterized, and represented as a function $f_{i,j}$ (*i*– stands for level of SIL and *j* – level of EAL). Some case studies for systems of category II and III are described in the paper [15].
For reaching determined level of EAL some protection rings have to be designed that include the technical and organizational solutions relevant to the architecture of distributed IT system considered and its environment.

4.3. Distributed computer networks and designing rings of protection

Several cyber security measures for secure operation of programmable control and protection systems (e.g. designed as *distributed control system* - DCS) in distributed industrial installation can be proposed. They include following solutions [22]:
1 – Malware detection and prevention (including antivirus and whitelisting),
2 – Patch management,
3 – *User account management* (UAM) – administration of operator and user rights (for role based access control),
4 – System hardening – adapting system from default to secure,
5 – Firewalls and *Virtual Private Network* (VPN),
6 – Security cells (secure architecture based on network segmentation) including *DeMilitarized Zone*: DMZ (*perimeter network*), i.e. additional layer of security in an organization within LAN (*Local Area Network*),
7 – Politics and procedures (including the security management process, operational guidelines as well as business continuity management and disaster recovery),
and are represented as rings of protection in *Figure. 13.*
An additional ring can be also drawn for representing measure of physical security, i.e. a protection for preventing physical access of intrude to the control and/or protection equipment.
Very important in high risk installations/systems are countermeasures protecting their SIS against intentional actions of hackers from *Internet* or *Wide Area Network* (WAN) [20], [22], [23] existing for communication of contractors. Relevant protection rings are illustrated in *Figure 14*.

4.4. Defining the risk matrix for security related analysis

An example of the risk ranking matrix for the security vulnerability analysis shown in *Figure 15*. Each category of severity and likelihood is too be defined with regard to qualitative or preferable quantitative information available for given case of hazardous system considered. It is worth to mention that such matrix can be defined to be compatible with risk matrix for functional safety analysis based on qualitative information [9].

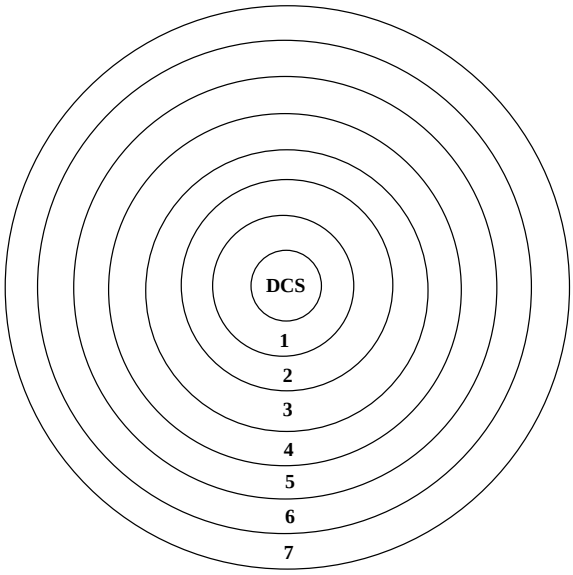
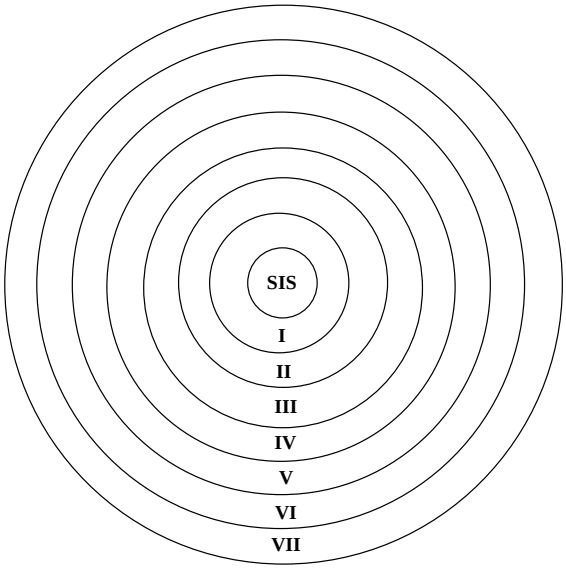


Figure 13. Examples of protection rings within distributed control system (DCS)



I - BPCS and AS, II – Process, III – DMZ, IV – Network, V – Outer DMZ, VI – Wide Area Network (WAN), and VII – Internet

Figure 14. Examples of protection rings of Safety Instrumented System (SIS)

S → L ↑	S_1	S_2	S_3	S_4	S_5
L_5	R_2	R_3	R_4	R_5	R_5
L_4	R_2	R_2	R_3	R_4	R_5
L_3	R_1	R_2	R_2	R_3	R_4
L_2	R_1	R_1	R_2	R_2	R_3
L_1	R_1	R_1	R_1	R_2	R_2

Figure 15. An example of risk ranking matrix for five levels of severity (S) and likelihood (L)

For risk analysis the qualitative risk ranking scheme, similar to the *Preliminary Hazard Analysis* (PHA), method can be adapted. The scheme, published in MILSTD-882B, is still is use in industrial practice. Many variations of this method, redefined by the companies and PHA teams, exist and have been successively used in practice.
The qualitative risk ranking scheme, similar to the PHA method can be used. The risk levels to be assessed may be classified as follows: R_1 – acceptable, R_2 – acceptable conditionally, only if costs of the risk reduction is very high (unacceptable), R_3 – the risk must be reduced in given time horizon, R_4 – the risk must be reduced in a relatively short time horizon agreed upon, R_5 – the installation must be shut-down; start up is possible after proving that the security risk was reduced at least to the level R_2. How risk should be reduced is based on results of safety and security related analyses and available countermeasures.
The security vulnerability analysis team should make some determination based on expert judgement, that if the selected measures were implemented, what level of risk reduction will be achieved. There are two approaches for identifying protections [16]:

- The asset-based approach applies a predetermined security performance standard to increase protection for given target.
- The scenario-based approach may yield more cost effective solutions, as the solutions are tailored to each of the scenarios developed.

Depending on the scenario, the policy or procedural changes, physical security upgrades, barriers, rings, software upgrades, the addition guard, etc. are considered [23]. For instance, the access control system classification considers the security level based on two basic items: *identification class* and *access classification*.
There is a substantial problem to protect the computer resources of hazardous distributed installation, which can be supported by *Information Security Management System* (ISMS), designed e.g. according to principles of the ISO/IEC 27001 [12]. It is worth to mention that such ISMS should additionally include security related management of programmable control and protection systems with regard to results of relevant risk assessments.
Thus, in the context of functional safety management the ISMS should be designed to support effectively the cyber security management of programmable control and protection systems (BPCS/DCS and SIS/ESD) of technological processes and other computerized information systems in given complex IT network considered.

4.5. Functional safety and security management in the framework of RIDM

A concept of risk-informed decision making has been developed at some regulatory and research institutions of nuclear industry in USA [8]. 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 [8].
Regulatory Guide (RG) 1.200 [8] 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.
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 [8].

Taking into account these principles some main areas of functional safety-related decision making were identified, which are shown in *Figure 16.* 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.

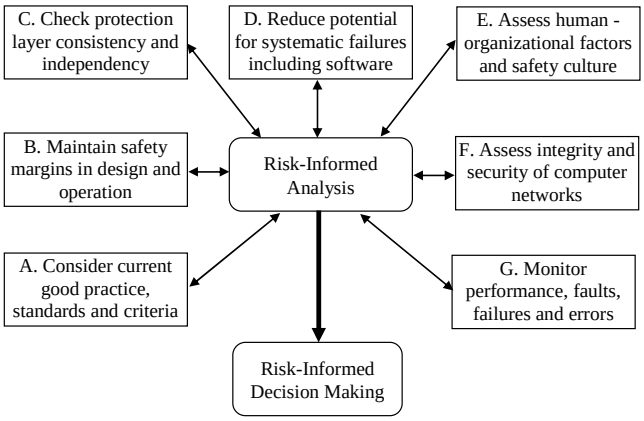


Figure 16. Main areas of functional safety analyses for decision making

In complex technical system different types of subsystems are distinguished and their malfunctions can be caused by hardware, software and human components [13]. Their operation is influenced by various factors: environmental, technical and human. Human errors are rooted in organisational deficiencies, so potential causes of human failures should be carefully considered in probabilistic modelling of these systems.

A methodology for aggregating the probabilistic evaluations within the risk model consisting of accident scenarios or their categories is illustrated in *Figure 17.* Final aggregation of the risk model is performed within a possibilistic framework that uses the fuzzy intervals for representing and evaluating of uncertainty [13].

The interval risk model is evaluated for given system that consists of a set pairs of fuzzy intervals for consecutive (*k*-th) accident scenarios

$$\Re = \{(\tilde{F}_k, \tilde{C}_k)\}, k = 1,2,...,K \qquad (1)$$

where $(\tilde{F}_k, \tilde{C}_k)$ are fuzzy intervals of respectively frequency and consequences for *k*-th accident scenario.

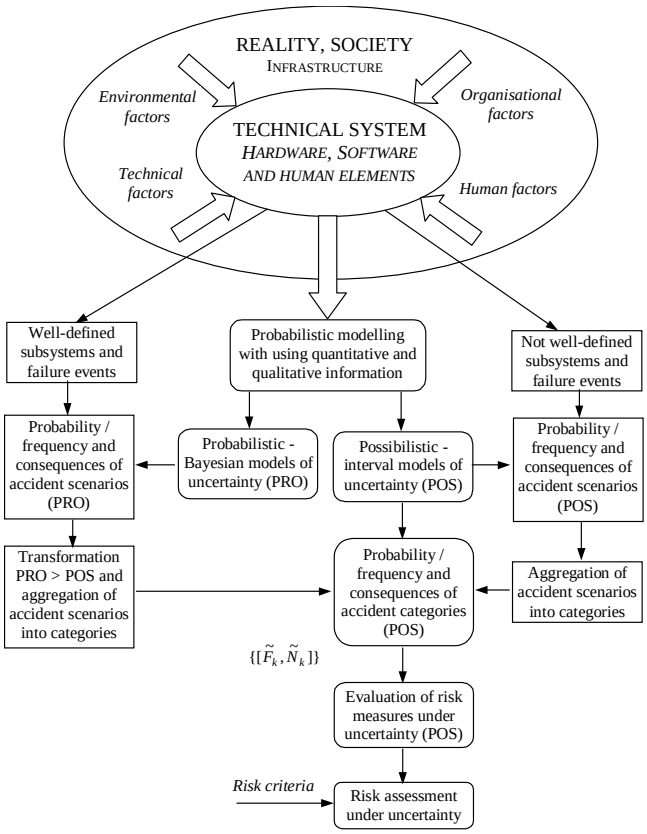


Figure 17. Methodology outline for risk assessment under uncertainty based on intervals

Based on the set of pairs of fuzzy intervals (1) the risk measures are calculated, and the F-N curve (CCDF - *complementary cumulative distribution function*) is constructing for characteristic points of fuzzy intervals. The method is suitable for:

- compliance demonstration of results obtained with defined criteria functions, as e.g. for safety integrity levels (SILs) [9] verifying according to Tab.1,
- compliance demonstration of F-N curves constructed on the basis of (1) with criteria lines,
- cost-benefit analysis of risk control options (RCOs) for the representative values of fuzzy intervals or characteristic values of the fuzzy intervals.

The representative value of fuzzy interval (defined using a possibility distribution) has similar meaning as the expected value of the probabilistic distribution for representing uncertainty. It was verified for several distributions obtained from transformation of given probabilistic distribution into possibilistic one.

The methodology outlined is especially useful for predictive risk evaluations, when the risk control options (RCOs), e.g. functional safety or security related solutions are proposed and assessed, especially in cases of systems consisting of not well-defined subsystems (hardware, software and human elements), influenced by various technical,

environmental, human and organisational factors.

5. Conclusion

The industry is currently in the face of a need to assess whether current security measures effectively address new threats and make enhancements to provide effective safety and security measures to protect adequately the workers, public and the environment. Security of industrial hazardous plants has to be balanced with other objectives to be commensurate with the threat and likelihood of potential critical scenarios. In some industrial plants, like refineries and chemical plants, the range of hazards is relatively high. In such plants managing the security related vulnerabilities is becoming a key issue.

The risk assessment methods used for the safety management are not fully applicable for the security management. The system security analysis and risk assessment for the security management are based intensively on expert opinions who use qualitative information. Due to importance of the problem for industrial practice and critical infrastructures, further research should be undertaken to develop integrated methodology that include defining criteria for the safety and security related assessments.

In this work some methodological challenges for uncertainty representation and assessment for probabilistic modelling and risk assessment of complex hazardous installations are specified. Due to various factors influencing the safety and security of such installations, which are usually modelled using qualitative and quantitative methods, a possibilistic framework for uncertainty representation is proposed. The possibility theory, related to the fuzzy set theory, offers a sound theoretical background for semi quantitative risk assessments.

If for some failure events the probabilistic data form the field are available and subsystems are well-defined, then probabilistic Bayesian framework for representing uncertainty can be applied. However, if there are not well-defined elements in the system (e.g. using of programmable systems within computer networks and human factors are involved) the evaluations are based on significant amount of qualitative information and using the possibilistic framework seems to be more justified.

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] ARC (2011). White Paper. Risk Drives Industrial Control System Cyber Security Investment. arcweb.com.

[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. & Śliwiński, M. (2010). Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issues. *PSAM*, Seattle.

[5] 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.

[6] Białas, A. (2008). Semiformal Common Criteria Compliant IT Security Development Framework. *Studia Informatica*, Silesian University of Technology Press, Gliwice.

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

[8] 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.

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

[10] IEC 61511 (2003). Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.

[11] ISO/IEC 15408 (1999). Information Technology. Security Techniques. Evaluation Criteria for IT security.

[12] ISO/IEC (2005). 27001. Information technology. Security techniques. Information security management systems. Requirements.
[13] Kosmowski, K.T. (2004). Modelling and uncertainty in system analysis for safety assessment. Proceedings of the International Conference on Probabilistic Safety Assessment and Management, PSAM 7 - ESREL '04, Berlin, Springer.
[14] Kosmowski, K.T. (2006). Functional Safety Concept for Hazardous System and New Challenges. *Journal of Loss Prevention in the Process Industries* 19(1), pp. 298-305.
[15] 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.
[16] Kosmowski, K.T. (Ed.) (2007). *Functional Safety Management in Critical Systems*. Gdansk University of Technology. Wydawnictwo Fundacji Rozwoju Uniwersytetu Gdańskiego.
[17] Kosmowski, K.T. (2011). Functional Safety Analysis including Human Factors. *International Journal of Performability Engineering* 7 (1), 61-76.
[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] OECD/IFP (2011). Project on Future Global Shocks. Reducing Systemic Cybersecurity Risk. IFP/ WKP/ FGS.
[20] SINTEF (2007). The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems. SINTEF A1626.
[21] SINTEF (2010). Reliability Data for Safety Instrumented Systems - PDS Data Handbook. Edition, SINTEF A13502.
[22] Siemens AG (2011). Operational Guidelines for Industrial Security. Proposals and recommendations for technical and organizational measures for secure operation of plant and machinery.
[23] Stouffer, K., Falco, J. & Scarfone, K. (2011). *Guide to Industrial Control Systems (ICS) Security*. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-82.