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

Towards systemic functional safety and security management in hazardous plants

Keywords

hazards, safety, security, risk, functional safety, control and protection systems, life cycle, decision making

Abstract

The aim of this article is to identify and discuss some issues related to functional safety and security management in hazardous industrial plants. The safety functions are to be realised using the *electric / electronic / programmable electronic systems* (E/E/PESs) or the *safety instrumented systems* (SISs) that are designed and operated respectively according to IEC 61508 and IEC 61511 requirements in life cycle. Although the role of functional safety solutions in effective reducing and controlling the individual and/or societal risks has been widely recognised, the substantial problems emerge when E/E/PEs or SISs operate in industrial distributed computer networks. Thus, the security-related problems appear that can introduce some additional risks. An integrated systemic functional safety and security concept is proposed, which includes general requirements as well as appropriate using specified methods and international standards.

1. Introduction

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 [7].

Two categories 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 [8] but high or continuous ones appear in the machinery or transportation systems.

This article deals with current challenges of functional safety analysis and assessment. There are still some methodological problems concerning the functional safety analysis and management in life cycle. They are related to the issues of potential hardware danger failures, software faults, common cause failures (CCFs), dependencies of equipment and barriers, human errors, organisational deficiencies, security aspects, etc. [12], [14].

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

The human-operator contributes to realization of safety functions through relevant *human system interface* (HSI), which is to be designed to achieve safety goals during abnormal situations taking into account functions of basic process control system (BPCS) safety systems such as E/E/PESs or SISs within protection layers. There is current issue how to design an independent *alarm system* (AS) [4], [17].

Lately problems of security are becoming important in industrial hazardous plants because the installations are controlled and protected using the programmable technology, i.e. the computer systems and networks together with industrial programmable logic controllers (PLSs) performing safety and security - related functions [1], [15], [18], [19].

Such distributed programmable control and protection system is vulnerable to a certain extent to cyber attack [10]. It should be designed and managed in life cycle to avoid or limit externally or internally induced accidents, especially those with serious consequences. These issues are especially important for industrial installations and hazardous plants, e.g. in chemical and nuclear sector.

The article is intended to outline some aspects of safety and security analysis in the context of

international recommendations, standards as well as existing methods to propose an integrated approach.

2. Scope of safety and security management in life cycle within risk-informed decision making approach

Due to complexity of risk management in industrial plants, to overcome difficulties in safety-related decision making under significant uncertainties, it was proposed to apply in industrial practice a approach based on the *Risk Informed Decision Making* (RIDM) [13]. It would enable the decision making in a more transparent and systematic way.

In this methodology the overall *safety management* includes the RIDM and periodic risk reassessment based on performance monitoring of the installation and its vital systems including the control and protection systems. Such methodology is compatible with the functional safety management methodology described in IEC 61508 [7]. However it requires nowadays including some additional aspects, such as security related issues as well as the safety and safety culture in organizations involved.

In known white paper entitled *Risk-Informed and Performance-Based Regulation* (NRC, 1999), the Commission proposed a *risk-informed* approach for regulatory decision-making. It represents a certain philosophy in which the 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.

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. The following principles are global in nature and have been generalised to all activities that are the subject of risk-informed decision-making:

- 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 and mentioned new expectations, the main areas of safety-related decision making have been identified, which are specified in *Figure 1*. They include in addition some new aspects.

Nowadays, the security related systems and the programmable control and protection systems operating in industrial computer networks play an important role in maintaining high performance as well as the safety and security of many technical systems, particularly in complex hazardous plants. Therefore, the relevant risk-informed analyses performed for identification of important factors influencing performance as well as the safety and security related risk should be of a considerable interest for operators and regulators [5], [22]-[23], [27].

Therefore, in the middle of *Figure 1* a block of integrated *safety and security management system* (S&SMS) in an organisation is placed. The staff responsible for operation of such system co-ordinates performing required analyses and assessments and undertakes the *safety & security related decisions* concerning the corrective and preventive actions. The cost benefit analyses of risk reduction measures are also performed within a system oriented risk informed decision making [14], [16].

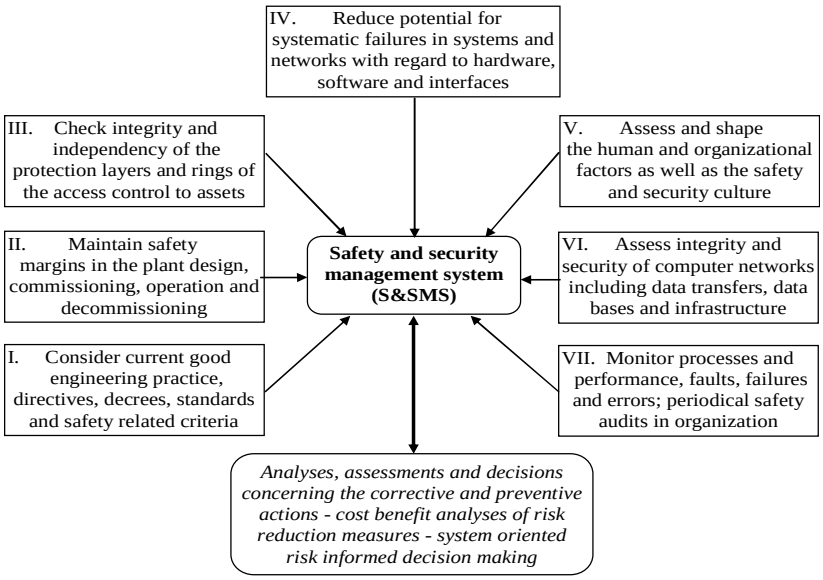

Figure 1. Scope of safety and security management in life cycle of hazardous industrial plants

3. General requirements for systemic safety and security management in industrial plants

In *Figure 2*. some general requirements for system oriented safety and security management in industrial plants are specified. They include:

A. *Council Directive: 96/82/WE (Seveso II) and 94/9/WE (ATEX); Guidance on COMAH (HSE) and safety policy; and*

B. *Environment Protection Act and decrees introducing in Poland Council Directives: 96/82/WE and 94/9/WE.*

Below some remarks are given in the light of published lately the Directive 2012/18/EU known as Directive Seveso III [24].

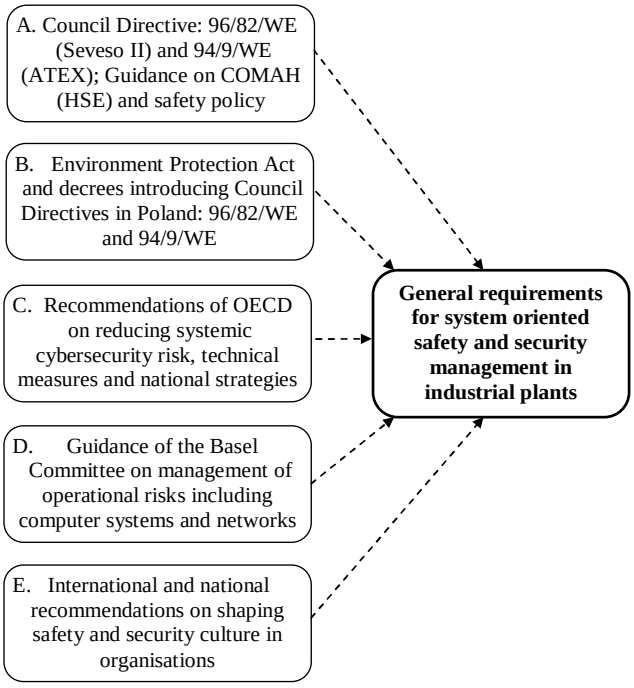

Figure 2. General requirements for system oriented safety and security management in industrial plants

It should be mentioned that this Directive of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, is amending and subsequently repealing Council Directive 96/82/EC.
It emphasises that major accidents can have consequences beyond frontiers, and the ecological and economic costs of an accident are borne not only by the establishment affected, but also by the Member States concerned. It is therefore necessary to establish and apply *safety and risk-reduction measures to prevent possible accidents, to reduce the risk of accidents occurring and to minimise the effects if they do occur, thereby making it possible to ensure a high level of protection* throughout the Union.
In order to reduce the risk of domino effects, where establishments are sited in such a way or so close together as to increase the likelihood of major accidents, or aggravate their consequences, operators should cooperate in the exchange of appropriate information and in informing the public, including neighbouring establishments that could be affected.
When considering the choice of appropriate operating methods, including those for monitoring and control, operators should take into account available information on best practices. Information disseminated to the public should be worded clearly and intelligibly. In addition to providing information in an active way, without the public having to submit a request, and without precluding other forms of dissemination, it should also be made available permanently and kept up to date electronically. At the same time there should be appropriate confidentiality safeguards, to address security-related concerns, among others.
The article 8 states that Member States shall require the operator to draw up a document in writing setting out the *major-accident prevention policy* (MAPP) and to ensure that it is properly implemented. The MAPP shall be designed to ensure a high level of protection of human health and the environment. It shall be proportionate to the major-accident hazards. It shall include the operator's overall aims and principles of action, the role and responsibility of management, as well as the commitment towards continuously improving the control of major-accident hazards, and *ensuring a high level of protection.*
The safety report should demonstrate that *adequate safety and reliability* have been taken into account in the design, construction, operation and maintenance of any installation, storage facility, equipment and infrastructure connected with its operation which are linked to major-accident hazards inside the establishment;
The *safety report* has to contain as minimum the description:

- the main activities and products of the parts of the establishment which are important from the point of view of safety, sources of major-accident risks and conditions under which such a major accident could happen, together with a description of proposed preventive measures;
- the equipment installed in the plant to limit the consequences of major accidents for human health and environment, including for example detection/protection systems, technical devices for limiting the size of accidental releases, including water spray, vapour screens, emergency

catch pots or collection vessels, shut-off- valves, etc.

In Annex III of this directive, i.e. *Information referred to in Article 8(5) and Article 10 on the safety management system and the organisation of the establishment with a view to the prevention of major accidents*, there are requirements specified concerning implementation of the operator's *safety management system* and account shall be taken of several elements.

The safety management system shall be proportionate to the hazards, industrial activities and complexity of the organisation in the establishment and be based on assessment of the risks. It should include the part of the general management system which includes the organisational structure, responsibilities, practices, procedures, processes and resources for determining and implementing the major-accident prevention policy (MAPP).

In addition the following issues shall be addressed by the safety management system:

(i) organisation and personnel — the roles and responsibilities of personnel involved in the management of major hazards at all levels in the organisation, together with the measures taken to raise awareness of the need for *continuous improvement*; the identification of training needs of such personnel and the provision of the training so identified; the involvement of employees and of subcontracted personnel working in the establishment which are important from the point of view of safety;

(ii) identification and evaluation of major hazards — adoption and implementation of procedures for systematically identifying major hazards arising from normal and abnormal operation including subcontracted activities where applicable and the *assessment of their likelihood and severity*;

(iii) operational control understood as adoption and implementation of *procedures and instructions for safe operation*, including maintenance, of plant, processes and equipment, and for *alarm management* and temporary stoppages; taking into account available information on *best practices* for monitoring and control, with a view to reducing the risk of system failure; *management and control of the risks associated with ageing equipment* installed in the establishment and corrosion; inventory of the establishment's *equipment, strategy and methodology for monitoring and control of the condition of the equipment*; appropriate follow-up actions and any necessary countermeasures;

Thus, the meaning of operational control was emphasised including best practices for monitoring and control, which obviously are related to the *programmable monitoring, control and protection systems* operating within the *industrial computer systems and networks*. As it is well known these *systems and networks are vulnerable to intentional cyber attacks* that contribute to the cybersecurity risk.

C. Recommendations of OECD on reducing systemic cybersecurity risk, technical measures and national strategies

Significant and growing risks of localised events and loss as a result of compromise of computer and telecommunications services have been identified. In addition, reliable Internet and other computer facilities are essential in recovering from most other large-scale disasters [22].

Likely breaches of cybsersecurity such as malware, distributed denial of service, espionage, and the actions of criminals, recreational hackers and hacktivists, for most events are to be relatively easily localised in short term impact. Successful prolonged cyberattacks need to combine: attack vectors which are not already known to the information security community and thus not reflected in available preventative and detective technologies.

Careful research of the intended targets; methods of concealment, both of the attack method and the perpetrators, the ability to produce new attack vectors over a period are needed. The recent Stuxnet attack apparently against Iranian nuclear facilities points to the future but also the difficulties of preventive actions. In the case of criminally motivated attacks the method of collecting cash without being detected are of interest [22].

The vast majority of attacks about which concern has been expressed apply only to Internet-connected computers. As a result, systems which are stand-alone or communicate over proprietary networks or are air-gapped from the Internet are in principle safe from these. However *these systems are still vulnerable due to management carelessness and insider threats*.

Rates of change in computer and telecommunications technologies are so rapid that threat analyses must be constantly updated. Managerial measures include: risk analysis supported by top management; secure system procurement and design as retrofitting security features is always more expensive and less efficient; facilities for managing access control; end-user education; frequent system audits; data and system back-up; disaster recovery plans; an investigative facility; where appropriate – standards compliance [22].

Technical Measures include: secure system procurement and design; applying the latest patches

to operating systems and applications; the deployment of anti-malware, firewall and intrusion detection products and services; the use of load-balancing services as a means of thwarting distributed denial of service attacks [18].

Large numbers of attack methods are based on faults discovered in leading operating systems and applications. Although the manufacturers offer patches, their frequency shows that the software industry releases too many products that have not been properly tested.

A number of OECD governments have outsourced critical computing services to the private sector; this route offers economies and efficiencies but the contractual service level agreements may not be able to cope with the unusual quantities of traffic that occur in an emergency. Cloud computing also potentially offers savings and resilience; but it also creates security problems in the form of loss of confidentiality if authentication is not robust and loss of service if internet connectivity is unavailable or the supplier is in financial difficulties [22].

The efficient provision of utility services such as electricity, gas, water and oil requires constant monitoring of supply systems. Since the 1970s these systems have been increasingly monitored and controlled using SCADA computing equipment. More recent systems incorporate load forecasting, adjusting the state of a supply network ahead of actual demand, etc. Earlier SCADA systems were proprietary to specific vendors, but are now moving to an open networked model. Newer SCADA devices communicate using Internet protocols, sometimes over the public Internet to remove the cost of dedicated communications links. Such systems are much more vulnerable to attack [18], [22].

The OECD Guidelines has been developed to promote a culture of security among all participants as a means of protecting information systems and networks and raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.

Creating a general frame of reference has been postulated that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks [19].

Promoting co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures have been postulated including the consideration of security as an important objective among all participants involved in the development or implementation of standards.

The nine principles published by the OECD are considered to be complementary and should be treated as a whole. They concern participants at all levels, including policy and operational levels. All participants should be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. These principles are as follows:

(1) Awareness
(2) Responsibility
(3) Response
(4) Ethics
(5) Democracy
(6) Risk assessment
(7) Security design and implementation
(8) Security management
(9) Reassessment

As regards the principle 7 the systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities.

Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

The principle 8 of the OECD concerns the security management that should be based on risk assessment in life cycle, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit.

Information system and network security policies, practices, measures and procedures should be coordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements [19].

D. Guidelines of the Basel Committee on management of operational risks including computer systems and networks

Although the Basel Committee [2] deals mainly with the risk-related to management issues in banking systems some research works coordinated and recommendations published by this committee are of interest also for other sectors.

Operational risk is defined as the risk of losses resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk [2].

There are opinions that in the industry practice, the first line of defence is business line management. This means that sound operational risk governance will recognise that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

A functionally independent *corporate operational risk function* (CORF) is typically the second line of defence, generally complementing the business line's operational risk management activities. The degree of independence of the CORF will differ among banks [2]. For small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the bank.

The third line of defence is an independent review and challenge of the bank's operational risk management controls, processes and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the Framework. This review may be done by audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.

If operational risk governance utilises the three lines of defence model, the structure and activities of the three lines often varies, depending on the bank's portfolio of products, activities, processes and systems; the bank's size; and its risk management approach. A strong risk culture and good communication among the three lines of defence are important characteristics of good operational risk governance.

Because operational risk management is evolving and the business environment is constantly changing, management should ensure that the framework's policies, processes and systems remain sufficiently robust. Improvements in operational risk management will depend on the degree to which operational risk managers' concerns are considered and the willingness of senior management to act promptly and appropriately on their warnings.

Several fundamental principles of operational risk management have been defined including:

Principle 1: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.

Principle 2: Financial institutions should develop, implement and maintain a Framework that is fully integrated into overall risk management processes. The Framework for operational risk management chosen by an individual institution will depend on a range of factors, including its nature, size, complexity and risk profile.

Internal operational risk culture is taken to mean the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of operational risk management. The internal operational risk culture is somehow related to the safety and security culture in the industry [14].

E. International and national recommendations on shaping safety and security culture in organisations

Lately, in some publications the selected aspects of safety and ethics are discussed, in particular in the context of the risk informed decision making [13]. Ethics, also known as moral philosophy, is a branch of philosophy that involves systematizing, defending and recommending concepts of right and wrong conduct. Ethics is divided into four major areas of study: *meta-ethics*, *normative ethics* - about the practical means of determining a moral course of action; *applied ethics* - about how moral outcomes can be achieved in specific situations; and *descriptive ethics* known as comparative ethics, is the study of people's beliefs about morality.

Engineering ethics is the field of applied ethics and a system of moral principles that apply to the practice of engineering. The field examines and sets the obligations by engineers to society, to their clients, and to the profession. As a scholarly discipline, it is closely related to subjects such as the *philosophy of science*, the *philosophy of engineering*, and the *ethics of technology*.

In times of dynamic changes of technology it has been often emphasized the responsibility of scientists and engineers [13]. The majority of engineers recognizes that the greatest merit is the deep knowledge and professional work to serving society for the welfare and progress of the majority. By transforming nature for the benefit of mankind, the engineer must increase his awareness of the world and knowledge of nature and society to make the world more fairer, safe and possibly happier. The paramount value recognized by engineers is the safety and welfare of the public.

There is no doubt that tragic episodes like *Three Mile Island NPP* accident (1979), *Bhopal* disaster (1984), *Chernobyl NPP* disaster (1986), *Fukushima NPP* disaster after tsunami (2011) and many other disasters happened not only due to technical causes but first of all because of the organizational inadequacies rooted in forgetting basic principles of engineering ethics resulting in human errors with serious consequences. It is obvious that managers and engineers should reject any technical and organizational solution within a project that can potentially harm the general interest, thus avoiding a situation that might be hazardous or threatening to the environment, life, health, or other rights of human beings.

The engineer and his employer must ensure the continuous improvement of his knowledge, particularly profession, disseminate knowledge, share experience, provide opportunities for education and training of workers. As a professional, the engineer is expected to commit himself to follow high standards of engineering ethics.

There exists definition that safety culture is related to the ways in which safety is managed in the workplace, and often reflects the attitudes, beliefs, perceptions and values that employees share in relation to safety [14]. Another widely used definition, proposed by the Advisory Committee on the Safety of Nuclear Installations (ACSNI), describes the safety culture of an organization as the product of individual and group values, attitudes, perceptions, competencies and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization's health and safety management.

In reports/guidelines of the IAEA: INSAG-4 and INSAG 15 the safety culture was defined as: that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.

Lately, there was also proposed definition of nuclear security culture as the assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security. An appropriate nuclear security culture aims to ensure that the implementation of nuclear security measures receives the attention warranted by their significance [14].

Nuclear security is defined as the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear or other radioactive substances or their associated facilities. It should be noted that "nuclear security" includes "physical protection", as that term is to be understood from consideration of the Physical Protection Objectives and Fundamental Principles, the Convention on the Physical Protection of Nuclear Material (CPPNM), and the Amendment to the CPPNM.

In March 2005, the IAEA international conference on Nuclear Security: Global Directions for the Future, held in London, recognized that the risk of successful malicious attacks remains high and stated: The fundamental principles of nuclear security include embedding a nuclear security culture throughout the organizations involved. By the coherent implementation of a nuclear security culture, staff remain vigilant of the need to maintain a high level of security.

In addition, it should be noted that the IAEA Code of Conduct on the Safety and Security of Radioactive Sources contains the following basic principle*: Every State should, in order to protect individuals, society and the environment, take the appropriate measures to ensure the promotion of safety culture and of security culture with respect to radioactive sources*.

There are various factors that influence the security culture. One of such important factors related to the functional safety is the information security. Controlling access to sensitive information is a vital part of the security function. Accordingly, the organization must implement classification and control measures for protecting sensitive information. The security culture indicators for information security are as follows [14]:

- classification and control requirements are clearly documented and well understood by staff;
- clear and effective processes and protocols exist for classifying and handling information both inside and outside the organization;
- classified information is securely segregated, stored and managed;
- staff members are aware of and understand the importance of adhering to the controls on information;
- cyber systems are maintained to ensure that they are secure, that they are accredited by an

appropriate authority and are operated in accordance with procedures.

As it was mentioned, the programmable control and protection systems operating in industrial computer networks play an important role in maintaining high performance as well as safety & security of many technical systems, in particularly in complex hazardous plants. Therefore, the analyses performed for identification of hazards and important factors influencing performance and risks should be of a considerable interest of operators and regulators in relevant risk-informed decision making.

As it was described the functional safety solutions contribute significantly to the safety and security of hazardous plants, in particular nuclear power plants, providing vital functions for the control, protection and monitoring, especially in abnormal and accident conditions.

Thus, their designing and operating should include both safety and security aspects. In the work [14] an approach is proposed to include the functional safety management as an important part of the integrated safety and security management system, taking into account general quality assurance aspects in the design and operation as well as personnel training, at relevant levels in organizations, responsible for safety and security of hazardous industrial plants.

4. Systemic functional safety and security management in hazardous process plants

4.1. Scope of the functional safety management in lifecycle

As it has been described in previous chapter, the safety-related systems that include programmable control and protection systems play nowadays an increasing role in reducing the risk related to operation of hazardous industrial plants. There are frameworks for the functional safety management in life cycle described in IEC 61508 [7] and some sector standards, e.g. IEC 61511 [8] and IEC 61513 [9]. They require careful identification of hazards and the risk analysis for defining safety-related functions (S-RFs) and determining their safety integrity level (SIL).

Then the SILs of consecutive safety-related functions have to be verified forappropriate architectures of E/E/PES (*Electric / Electronic / Programmable Electronic System*) [7] or SIS (*Safety Instrumented System*) [8] considered, using relevant probabilistic models for relevant modes of operation, i.e. low demand mode or high/continuous mode.

These analyses should include also such issues as: the architectural constraints, possibility of systematic failures and potential software faults and failures, *common mode failures* (CCFs), and the influence of human factors and potential errors committed by operators. All these aspects have been described in details in the monograph [14].

There is considerable uncertainty involved in the risk assessment to determine SIL for consecutive safety-related functions and its verifying. In the risk assessment for decision making also the results of *cost-benefit analysis* (CBA) are valuable to indicate, which *risk control option* (RCO) gains the advantage over a basic considered option, fulfilling relevant requirements and criteria. It was shown in case studies that a more costly option as regards the capital investment for increasing SIL of given safety function, e.g. from SIL2 to SIL3, can be more justified due to lower *life cycle costs* (LCC) [13]-[14]. The methodology developed is also applicable for the layer of protection analysis (LOPA) [21] with defined protection layers and potential dependencies between them.

As it was mentioned due to complexity of the problem, to overcome difficulties in safety-related decision making under significant uncertainties it was proposed to apply a methodology based on the *Risk Informed Decision Making* (RIDM) approach [13]. The methodology proposed is compatible with the functional safety management methodology described in IEC 61508 [7]. 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.

As it is known, the requirements for safety functions are determined taking into account the results of hazards identification, while the safety integrity requirements result from analysis of potential hazardous events. The higher the safety integrity level (SIL) is for given S-RF the lower *average probability of failure on demand* (PFD) 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 architecture design of a safety-related system.

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 [7] adopts an overall framework for safety management in lifecycle. A modified scheme is shown in *Figure 3* that include in addition the security related aspects.

All activities related to the *functional safety and security management* including the determination of SIL and its verification are not shown on this scheme for reasons of clarity. They should be specified for

the E/E/PE system (hardware), software and human factors to avoid as much as possible the random failures and systematic failures. The requirements concerning functional safety and security management shall run in parallel with the overall safety lifecycle phases.

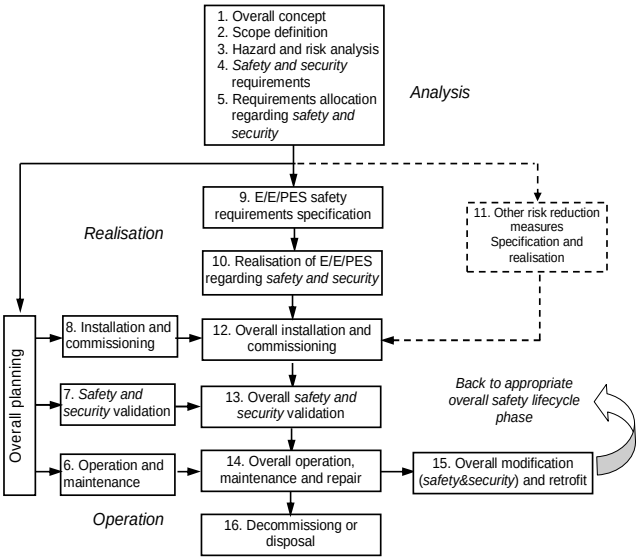

Figure 3. Overall functional safety-related lifecycle (based on [7])

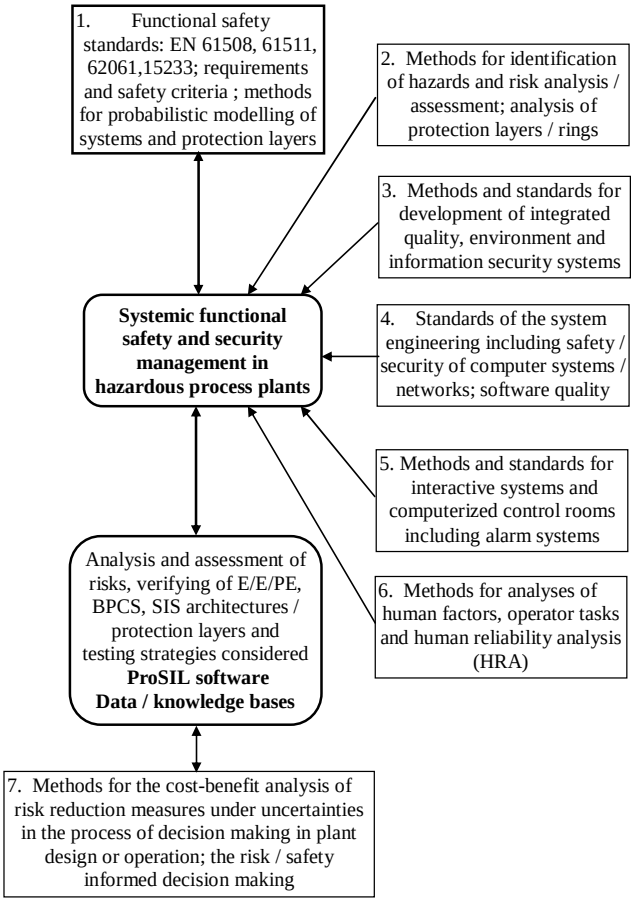

Figure 4. Systemic functional safety and security management in hazardous process plants

According to IEC 61508 the safety validation should be performed in terms of the overall safety function requirements and the 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 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 for given SIL. Below, the issue of architectural and security related constraints in designing of subsystems are discussed.

4.2. Methods and standards helpful in systemic functional safety and security management

The proposed framework for systemic functional safety and security management is shown in *Figure 4*. The methods and standards of interest for that purpose are specified below.

1. The international standards used for functional safety analysis include the generic standard IEC/EN 61508 [7] and sector standards: EN 61511 [8] (the process industry), EN 62061 (machinery), EN 15233 (ATEX related industry) and IEC 61513 [9] (nuclear power plants). Addressing the human factors in functional safety analysis is becoming important [3], [20].

2. There are some appreciated methods for identification of hazards and risk analysis/assessment including analysis of protection layers (safety) and protection rings (security), for instance: SR (safety review), CA (checklist analysis), RR (relative ranking), PHA (preliminary hazard analysis), HAZOP (hazard and operability study), HAZID (hazard identification studies), FMECA (failure mode, effects and criticality analysis), FTA (fault tree analysis), ETA (event tree analysis), LOPA (layer of protection analysis), BORA (barrier and operational risk analysis) , SeSa [25] (assessing secure remote access to safety instrumented systems).

3. There are commonly used known standards for integrated quality, environment and security management such as: EN ISO 9001 (quality), EN ISO 14001 (environment), EMAS (European Eco-Management and Audit Scheme), as well as EN/ISO 27001 and ISO/IEC 17779 for information security assessment.

4. Standards of the system engineering including safety / security of computer systems / networks; software quality include: ISO/IEC 26702 (systems

engineering - application and management of the systems engineering process), ISO/IEC 15408 [11] (common criteria for information technology security evaluation), IEC 62280 (railway applications - communication, signalling and processing systems - safety related communication in transmission systems), IEC 62443 (industrial communication networks – network and system security), EN 61131 (programmable controllers), EN 61784 (industrial communication networks), EN 61158 (digital data communications for measurement and control – fieldbus for use in industrial control systems), and US-CERT report [27]

5. Methods and standards for interactive systems and computerized control rooms including alarm systems include: EN ISO 942-210 (ergonomics of human-computer interaction), EN ISO 11064 (ergonomic design of control centres), EEMUA 191 (alarm systems: a guide to design, management and procurement), ISA 18.02 (management of alarm systems for the process industries).

6. Methods for analyses of human factors, operator tasks include: HTA (hierarchical task analysis), FAST (function analysis system technique), TLA (timeline analysis), ET (event trees), CES (cognitive environment simulations), and human reliability analysis (HRA) methods [6]: THERP (technique for human error rate prediction), SPAR-H (standardized plant analysis risk model - Human Reliability Analysis Method), and CREAM (Cognitive Reliability Error Analysis Method by E. Hollnagel) [19].

The block 7 in *Figure 4* indicates the methods for the cost-benefit analysis of risk reduction measures under uncertainties in the process of decision making in plant design or operation; the risk / safety informed decision making. They have been described in the monograph [14]. The analyses of the safety integrity levels (SILs) based on assessments of risks, verifying SILs of the E/E/PE, BPCS, SIS architectures / protection layers considered are supported by the ProSIL software that includes relevant data / knowledge bases [14], [19].

4.3. The architectural and security related constraints

The design of the E/E/PE safety-related system should be carried out in accordance with the E/E/PE design requirements specification [7]. The design of the E/E/PE safety-related system includes the overall hardware and software architecture, sensors, actuators, programmable electronics, embedded software, application software, data etc.

Below some selected aspects of these requirements and related analyses will be of interest, especially those concerning the hardware safety and security integrity comprising:

- the fault tolerance requirements;
- the architectural constraints related to the hardware safety integrity level (SIL) [7] and security assurance (SAL) [10].

When the failure rates are treated as the constant failure rates the *safe failure fraction* (S_{FF}) of the element or a channel treated as a serial reliability structure of elements can be evaluated from the formula [14]:

$$S_{FF} = \frac{\sum \lambda_S + \sum \lambda_{Dd}}{\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du}} \tag{1}$$

where: λ_S is the rate of safe failures; λ_{Dd} the rate of dangerous failures, which are detected by the diagnostic tests; and λ_{Du} the rate of dangerous undetected failures.

The standard IEC 61508 introduces two types of elements: A and B in the E/E/PE safety-related systems. An element can be regarded as type A if, for the components required to achieve the safety function, can be characterized as follows [7]:

a) the failure modes of all constituent components are well defined; and
b) the behaviour of the element under fault conditions can be completely determined; and
c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met.

An element shall be regarded as type B if, for the components required to achieve the safety function, can be characterized as follows [7]:

a) the failure mode of at least one constituent component is not well defined; or
b) the behaviour of the element under fault conditions cannot be completely determined; or
c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures.

If at least one of the components of an element itself satisfies the conditions for a type B element then that element must be regarded as type B rather than type A element.

The hardware fault tolerance (HFT) requirements apply to the subsystem architecture that is used under normal operating conditions. The HFT requirements may be relaxed while the E/E/PE safety-related system is being repaired on-line. However, the key parameters relating to any such relaxation should be previously evaluated, taking into account the *mean*

time to restoration MTTR, to demonstrate that the system unavailability due to a channel failure and restoration is low compared to the probability of failure on demand [7].

If all the elements of a subsystem have achieved safe failure fractions S_{FF} that are in the same range specified in *Table 1* the following procedure is to be followed:

a) determine the safe failure fraction S_{FF} of an element;
b) determine the hardware fault tolerance of the subsystem;
c) determine the maximum SIL that can be claimed for the subsystem if the elements are of type A from *Table 1*;
d) determine the maximum safety integrity level that can be claimed for the subsystem if the elements are of Type B from *Table 1* (in parentheses).

Thus, *Table 1* specifies a set of highest safety integrity levels (SILs) that can be claimed for the safety function to be implemented using subsystems that consist of components of type A and type B (SILs in parentheses) taking into account two parameters: M and S_{FF}. These are rather strong requirements and constrains criticized lately by functional safety experts and analysts.

The novelty proposed is that additional parameter SAL (security assurance level) according to IEC 62443 [10] is proposed to be applied for the system operating in industrial computer network.

Table 1. Max allowable safety integrity level for a subsystem carried out safety function using elements of type A (type B)

Safety / Security S_{FF} / SAL	Hardware fault tolerance M		
	0	1	2
<60% / Low (SAL1)	SIL1 (- - -)	SIL2 (SIL1)	SIL3 (SIL2)
[60%, 90%) / Mod. (SAL2)	SIL2 (SIL1)	SIL3 (SIL2)	SIL4 (SIL3)
[90%, 99%) / High (SAL3)	SIL3 (SIL2)	SIL4 (SIL3)	SIL4 (SIL4)
≥99% / Very high (SAL4)	SIL3 (SIL3)	SIL4 (SIL4)	SIL4 (SIL4)
A hardware fault tolerance of M means that M + 1 faults could cause a loss of the safety function.			

Described above approach including the SAL parameter is justified especially when obtaining the evaluation assurance level (EAL) according to IEC 15408 [11] may be difficult to be implemented during the evaluation of the programmable control and/or protection systems realising defined safety functions. The SAL (security assurance level) is relatively new security measure concerning the control and protection systems which is evaluated based on a defined vector of seven requirements for relevant security zone [10].

5. Conclusion

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

However, the distributed programmable control and protection systems are vulnerable to a certain extent to cyber attack. They should be designed and managed in life cycle to avoid or limit externally or internally induced accidents, especially those with serious consequences. These issues are especially important for industrial installations and hazardous plants, e.g. in chemical and nuclear sector.

The article outlined some aspects of safety and security analysis in the context of international recommendations, standards as well as existing methods to propose an integrated approach towards systemic functional safety and security management in industrial hazardous plants.

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

There is also challenge in Europe to identify emerging cyber related hazards and develop a common operating vision for cyber-security to achieve operational consistency across the EU.

Acknowledgments

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

References[

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

[2] Basel Committee (2011). Sound Practices for the Management and Supervision of Operational Risk.
[3] Carey, M. (2001). Proposed Framework for Addressing Human Factors in IEC 61508. A Study prepared by Amey VECTRA Ltd. for Health and Safety Executive (HSE), U.K., Research Report 373.
[4] EEMUA (2007). Publication 191: Alarm Systems, A Guide to Design, Management and Procurement, Second Edition, The Engineering Equipment and Materials Users' Association, London.
[5] Froome, P. & Jones, C. (2002). Developing Advisory Software to comply with IEC 61508. Contract Research Report 419. Series: HSE Books.
[6] Gertman, I.D. & Blackman, H.S. (1994). *Human Reliability and Safety Analysis Data Handbook*, A Wiley-Interscience Publication, New York.
[7] IEC 61508 (2010). Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, Parts 1-7. International Electrotechnical Commission. Geneva.
[8] IEC 61511 (2003). Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.
[9] IEC 61513 (2011). Nuclear power plants, Instrumentation and control for systems important to safety, General requirements for systems, International Electrotechnical Commission, Geneva.
[10] ISA/IEC 62443 (2013). Security for industrial automation and control systems.
[11] ISO/IEC 15408 (1999). Information technology – Security techniques – Evaluation criteria for IT security, Parts 1-3.
[12] 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.
[13] Kosmowski, K.T. (2011). Functional Safety Analysis including Human Factors. *International Journal of Performability Engineering*, 7, 1, 61-76.
[14] Kosmowski, K.T. (2012): Current challenges and methodological issues of functional safety and security management in hazardous technical systems. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars*, 3, 1, 39-51.
[15] Kosmowski, K.T. (2013). *Functional safety and reliability analysis methodology for hazardous industrial plants*. Gdańsk University of Technology Publishers.
[16] Kosmowski, K.T. (2013). Problems in designing and operating the functional safety solutions of higher integrity levels. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars*, 4, 1, 83-99.
[17] Kosmowski, K.T. (Ed.) (2007). *Functional Safety Management in Critical Systems*. Publishing House OF Gdansk University of Technology.
[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. (2013). *Guidelines on functional safety analysis and assessment in system oriented safety and security management*. Internal report (in Polish), Gdańsk University of Technology.
[20] Kosmowski, K.T., Śliwiński, M. & Barnert, T. (2006). Functional safety and security assessment of the control and protection systems. *European Safety & Reliability Conference - ESREL*, Taylor & Francis Group, Estoril, London.
[21] LOPA (2001). Layer of Protection Analysis, Simplified Process Risk Assessment. Center for Chemical Process Safety. American Institute of Chemical Engineers, New York.
[22] OECD (2002). Guidelines for the Security of Information Systems and Networks. Towards a culture of security.
[23] OECD Report (1998). Critical Operator Actions – Human Reliability Modeling and Data Issues, Nuclear Safety, NEA/CSNI/R; OECD Nuclear Energy Agency.
[24] Seveso III (2012). Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC.
[25] SINTEF (2007). The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems. SINTEF A1626.
[26] SPAR-H (2005). Human Reliability Analysis Method, NUREG/CR-6883, INL/EXT-05-00509, US NRC.
[27] US-CERT (2011). Control Systems Security Program (CSSP) - Overview of Cyber Vulnerabilities.