*XXVI Seminarium*

*ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE 2016*

Oddział Gdański PTETiS

# CURRENT RISK ANALYSIS AND MANAGEMENT ISSUES IN TECHNICAL SYSTEMS

**Kazimierz T. KOSMOWSKI**

Gdańsk University of Technology
tel.: 48 58 347 2439 e-mail: kazimierz.kosmowski@pg.gda.pl

**Summary:** Dealing with the reliability and safety of industrial hazardous plants requires taking into account relevant interdisciplinary scientific knowledge and some existing approaches based on so-called good engineering practice, also those included in the international standards and guidelines. In this article an approach is proposed how to integrate the functional safety concept with information security aspects in the design and management of the industrial automation and control systems during operation of an industrial hazardous plant.

**Key words:** risk analysis, technical systems, risk management, protection systems, functional safety, information security.

## 1. INTRODUCTION

Nowadays companies become more complex and interrelated, being active on international increasingly competitive markets, where costs and innovation of products are of prime importance to be successful in long-term business. In addition there are increasing requirements in companies concerning *quality of products*, *environmental protection* as well as *health and occupational safety* (H&OS). These aspects are to be controlled using relevant management systems that in modern firms are integrated to reach elaborated goals in changing environment under often significant uncertainties, especially for longer time horizons.

Therefore, the managers, engineers and stakeholders have become more and more concerned with existing and emerging *threats and hazards*. Due to such circumstances, potential abnormal events and related risks, the *risk management* (RM) is becoming an increasingly important activity in various organizations and firms [1]. The RM is treated even as the *business driver* due to focusing attention on identified hazards and threats, and then elaborating careful plans of activities in relevant time horizons to support strategic decisions regarding evaluated risks.

Paying more attention in the enterprise on these issues might enable to evaluate the potential influence of identified types of hazards and threats on levels of risks in realization of activities, processes, services and products, according to expectations of cooperating firms, stakeholders and clients. Thus, implementing a more comprehensive approach would result in benefits from more diligent identifying hazards and threats, evaluating and reducing risks when achievable, and limiting uncertainties in decision making processes.

This article addresses current issues of the risk analysis and management in organisations responsible for reliable and safe operation of technical systems. These include hazardous industrial plants, and also distributed installations of the critical infrastructure, e.g. refineries, chemical plants, pipelines, power plants, electric power distribution system etc. Such interrelated complex plants and systems are treated in some publications as *large technical systems* (LTS). Special attention is focused on the *industrial automation and control systems* (IACS) [2, 3] designed with support of the *information and communication technologies* (ICT) to fulfil the safety and security requirements, especially important in cases of the industrial computer systems and networks.

Dealing with such complex industrial plants and supporting systems requires taking into account relevant interdisciplinary scientific knowledge and approaches based on so-called *good engineering practice*, also those expressed in international standards and guidelines.

Many publications have been written concerning information security issues in computer systems and networks, however less with consideration of specific design and operation safety and security-related aspects of the IACS including a concept of functional safety [4]. An approach is proposed in this article outlines how to integrate this concept with information security aspects in the design and operation of the IACS.

## 2. RISK EVALUATION REQUIREMENTS

### 2.1. General requirements

Today organizations face various problems due to internal and external influences that make them uncertain to achieve business and operation related objectives. The effect of uncertainty on these objectives is popularly expressed as risk [1]. Almost all activities of an organization involve risk. Thus, the organizations should manage risk by identifying and evaluating it in order to meet certain criteria.

Risk management can be applied to entire organization, at its distinguished levels and areas, and to specific projects and activities, processes and functions [1]. Establishing the context of risk management requires to consider the environment in which the objectives might be achieved, opinions of proposed by stakeholders and relevant risk tolerance criteria. It should help in revealing and assessing the nature of hazards and threats that potentially could influence some consequences and risks.

The objectives can be related to different aspects and goals, such as financial, health and safety of employees, technological safety, and environmental protection, etc. They can be formulated for different organization's levels, such as strategic, organization-wide, project, and defined processes in realization of operation tasks and final products.

Risks being of interest to managers are characterized regarding potential *hazardous events* (e.g. *accident scenarios*) and their *consequences*. The risk measures related to the operation of technical systems are often expressed as a combination of the *consequences* of abnormal (hazardous) events being considered in the process if risk analysis and the *likelihood (probability) or frequency* occurring of these events. Two kinds of risk are distinguished in technical systems, namely: an *individual risk* and a *societal (or group)* risk [5].

The *societal risk* associated with operation of given complex technical system is evaluated on the basis of a set of triples [5] as follows:

$$\Re = \{< S_k, F_k, C_k >\} \tag{1}$$

where: $S_k$ is $k^{\text{th}}$ accident scenario (usually representing an accident category) defined regarding the results of deterministic modeling, $F_k$ is the frequency of this scenario (probability per time unit, usually per year), and $C_k$ denotes the consequence of $k^{\text{th}}$ scenario (e.g. health, environmental or economic losses), or the number of injuries / fatalities denoted often as $N_k$ to be placed in (1) instead of $C_k$.

*The risk management process* includes systematic application of management policies, procedures and good practices to the coordinated activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risks to direct and control an organization regarding elaborated objectives, however often in conditions of significant uncertainty [1]. *Uncertainty* is understood here as the state of deficiency of information related to knowledge about an event of interest (e.g. accident scenario) in evaluating its consequence and/or likelihood (frequency).

The risk management process is illustrated in Figure 1. *Risk assessment* is defined as overall process of hazards and/or threats identification, preliminary ranking of specific risks (during risk identification), risk analysis and risk evaluation regarding the risk criteria [1]. Risk identification process is aimed at finding, recognizing and describing risk sources, and hazardous events with their causes and consequences. Risk identification can involve historical data, theoretical analysis, and expert opinions regarding emerging risks, and stakeholder's needs.

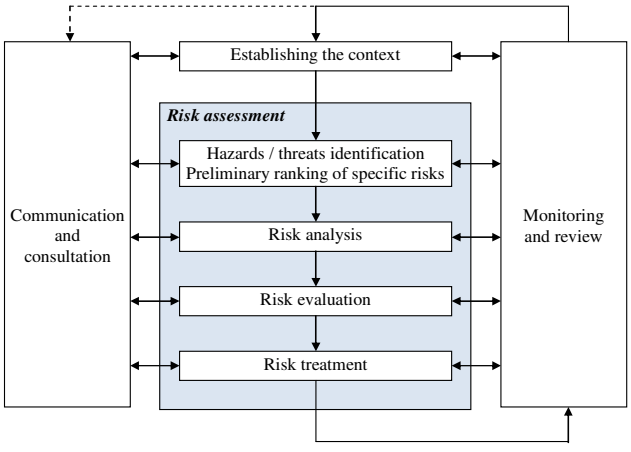


Fig. 1. Risk management process (based on [1])

*Risk criteria* are defined as terms of reference against which the significance of a risk is evaluated. Risk criteria are based on organizational objectives, and external and internal context. Risk criteria can be derived from standards, laws, policies, expert opinions and/or other sources if available.

Several sources of uncertainty in risk analysis may exist and it is worth mentioning about the distinction between *epistemic uncertainty* and *aleatory uncertainty,* because it is essential for careful risk assessment to provide honest support for safety-related decision making [5]. Uncertainties are characterized as *epistemic*, if the modeler sees a possibility to reduce them by gathering more data or by refining models (assuming randomness of repeatable phenomena). Uncertainties are categorized as *aleatory* if the modeler does not foresee the possibility of reducing them, because knowledge about issues of interest is not sufficient at present.

Following principles have been formulated for the *risk management* (RM) to be successfully applied at relevant organization's levels, because a careful RM [1]:

a) creates and protects values,
b) is an integral part of organizational processes,
c) is part of conscious decision making in solving complex problems,
d) explicitly addresses uncertainty issue,
e) is systematic, structured and timely,
f) is based on the best available information,
g) is tailored but taking into account important external influences,
h) takes human and cultural factors into account,
i) is transparent and inclusive,
j) is dynamic, iterative and responsive to internal and external changes,
k) facilitates continual improvement of the organization.

The outlined above risk management approach should be fully integrated with the organization's governance structure regarding requirements of the quality management system based on defined *processes* and *procedures* [1].

### 2.2. Risk-related management in technical systems

#### *2.2.1. Business continuity management*

Nowadays one of the most important issue in industrial practice is to provide the *business continuity management* (BCM). Basic requirements for setting up an effective *business continuity management system* (BCMS) are specified in the international standard ISO 22301 [6]. The BCMS should be a part of the overall *management system* (MS) that establishes, implements, operates, monitors, reviews, maintain and improves business continuity [7]. Such overall MS includes organisational structure, policies, planning activities, responsibilities, processes, procedures and resources as it is specified in the standard ISO 9001.

According to requirements given in ISO 22301 the organisation shall establish, implement, and maintain formally documented the *risk assessment process* that systematically identifies, analyses, and evaluates the risk of potential disruptive incidents within the organization. It is suggested to made this assessment in accordance with ISO 31000, characterized above. An organisation should [6]:

1) identify risks of disruption to the organisation's prioritized activities and the processes, systems, information, people, assets, outsource partners and other resources that support them,
2) systematically analyse related risks,
3) evaluate which disruption related risks require treatment,

4) identify treatments commensurate with *business continuity objectives* and organisation's *risk appetite*.

The organisation should be aware that certain financial or governmental obligations require the communication of relevant risks at varying levels of details. The organisation should also conduct evaluations of its business continuity procedures and capabilities in order to ensure their continuing suitability, adequacy and effectiveness. These evaluations are expected to be undertaken through periodic reviews, exercising, testing, post-incident reporting and performance analyses. Significant changes arising should be reflected in the procedure(s) in a timely manner [6].

### *2.2.2. Information security management*

The standards of ISO 27000 series are still in development process. Their objective is to describe how to create in an organisation effective *information security management system* (ISMS). As it is known all kinds of information hold and processed in organizations are subjected to threats of attacks, errors, hazardous event (e.g. flood, fire, etc.). Thus, each kind of information should be characterized by a degree of *vulnerability* inherent in its storage, transmission and no authorized use.

The term *information security* generally is related to information being considered as an asset which has a value that requires appropriate protection, for example, against the loss of *availability, confidentiality, and integrity*. Enabling accurate and complete information to be available in a timely manner to those with an authorized need is a key catalyst for business efficiency [8].

Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are basic elements of the *information security management* [8].

The ISMS consists of the policies, procedures, guidelines, resources and activities, collectively managed by an organization to protect its information assets. It enables to introduce an approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security to achieve business objectives, and is based upon a periodic evaluation of risks regarding defined organization's risk acceptance criteria.

The standard ISO/IEC 27005 (*Information security risk management*) provides guidelines on implementing the *process oriented risk management* to assist in implementing the information security management requirements specified in ISO/IEC 27001.

### *2.2.3. Integrated management including the quality, environmental and occupational safety aspects*

The *health and occupational safety* (H&OS) management is nowadays significant challenge not only in the industrial hazardous plants. An *integrated management system* in a company is often designed taking into account requirements specified in international standards: ISO 9001 (quality management system), ISO 14001 (environmental management system), OHSAS 18001 (occupational health and safety assessment) and recently also ISO 45001 (occupational health and safety management system).

The OHSAS 18001 was designed to help organizations in implementing a framework that identifies and controls the *health and occupational safety risks* for reducing potential accidents. It aids also legislative compliance and improves overall performance within an organization. The standard describes how to develop and implement a policy with the right objectives for organizations of all types and sizes, covering geographical, cultural and social conditions.

New standard ISO 45001 is aimed at supporting areas of management for ensuring better compatibility and governance, making more effective implementations within an organization wishing to:

a) establish and implement an internationally recognized occupational health and safety management system to reduce risks to personnel and other relevant parties,
b) maintain and constantly improve their health and safety performance, and
c) keep all operations in line with their stated health and safety policies in relation to internationally recognized standard.

This standard seems to be beneficial for *small, medium and large organizations* in any sector. It can set the benchmark for their health and safety governance, policies and practices across different geographical areas, countries, cultures and jurisdictions. Its purpose is also to promote better communication on shared issues, principles and *best available practice in global trade*.

## 3. CONTROL SYSTEMS FOR REDUCING RISKS

### 3.1. Reference model

A reference model selected describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels [3]. The reference model based on the ISA99 series of standards is shown in Figure 2. This model is derived from a general model used in ANSI/ISA-95.00.01-2000, *Enterprise-Control System Integration* in which following levels are distinguished:

Level 0 – *Technological processes*. It includes the physical process and basic equipment: sensors and actuators directly connected to the process and process equipment, named often as *equipment under control* (EUC).

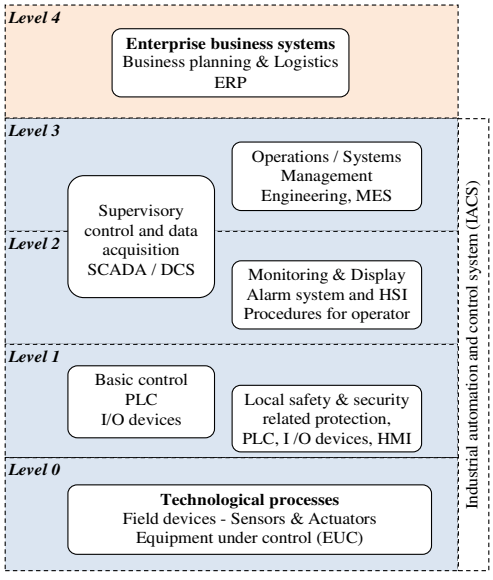


Fig. 2. Reference model for the operational management and control of production system (based on [3])

Level 1 – *Basic control and local safety & security related protections.* This level includes continuous control,

sequence control, batch control, and discrete control. The control and protection algorithms are implemented using *programmable logic controllers* (PLCs), that monitor the process and should return the process to a *safe state* if it exceeds defined limits. This level includes also systems that diagnose the processes and devices, and alert operators of impending unsafe conditions to undertake actions according to procedures using *human-machine interface* (HMI).

Level 2 – *Supervisory control*. This level includes the functions of monitoring and controlling the physical process using *distributed control system* (DCS) and *supervisory control and data acquisition* (SCADA) software. There are typically multiple production areas in industrial plants and this level include: operator *human-system interface* (HSI), operator alarms, supervisory control functions and gathering the process and equipment operation history data.

Level 3 – *Management of operations*. This level includes engineering aspects of operation and management using implemented *manufacturing execution system* (MES).

Level 4 – *Enterprise business systems*. This level is characterized by business planning and related activities, including logistics, using for instance an *enterprise resource planning* (ERP) system to manage and coordinate effectively business and engineering processes.

### 3.2. Functional safety management using the control and protection systems

The functional safety is a part of general safety, which depends on proper functioning (as designed) of the programmable control and protection systems. The concept of functional safety in life cycle was formulated in the international standard IEC 61508 [9]. It includes defining, for given hazardous installation, a set of *safety functions* (SFs) that are implemented using the *electric, electronic and programmable electronic* (E/E/PE) *systems,* or so called in the process industry sector, the *safety instrumented systems* (SIS) [10]. The subsystems of these systems belong to the levels: 1 and partly 2 (the alarm system) shown in Figure 2, and the field devices, i.e. sensors and actuators - equipment under control (EUC) are situated at level 0.

Two different requirements have to be specified to ensure appropriate functional safety solutions [5]:

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

The requirements concerning performance of safety functions are determined regarding hazards identified and distinguished potential accident scenarios, while the *safety integrity level* (SIL) requirements stem from the results of the risk assessment taking into account some specified risk criteria [5]. The SIL of given SF is expressed by a natural number from 1 to 4 and it is related to the necessary risk reduction. The allocation of safety requirements to the safety functions using the E/E/PE systems, and other safety-related systems or external risk reduction facilities is shown in Figure 3. The E/E/PE system or SIS consist of subsystems to be designed regarding a *hardware fault tolerance* (HFT) related to the configuration $K_x$oo$N_x$, e.g. HFT is 1 for 2oo3.

For the *safety functions* to be implemented using the E/E/PE system or SIS two types of interval probabilistic criteria are defined in IEC 61508, specified in Table 1, for two modes of operation:

- the *average probability of failure* $PFD_{avg}$ of given safety function on demand for the system operating in a *low demand mode*; or
- the *probability of a dangerous failure per hour PFH* for a *high demand or continuous mode* of operation.

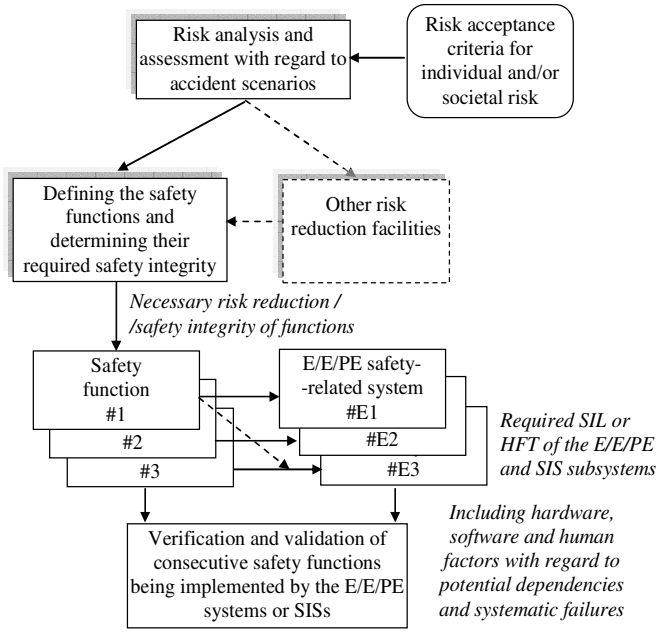


Fig. 3. Allocation of requirements for the safety functions and implementing them safety-related systems

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

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

The E/E/PE system or SIS has a typical configuration shown in Figure 4. It consists of three subsystems, generally of KooN configuration, as follows:

A. Input devices including sensors, transducers, *etc.*,
B. Logic device, e.g. safety PLC with its input and output modules,
C. Actuators and *equipment under control* (EUC), and other final devices, e.g. light indicators.

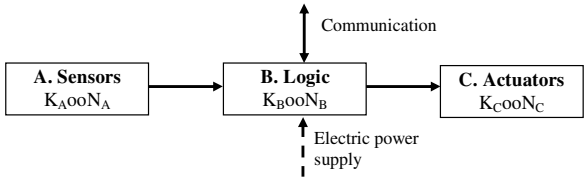


Fig. 4. Typical configuration of the E/E/PE system or SIS for implementing safety functions

Figure 5 illustrates the concept of risk reduction. The model adapted assumes that [5]:

– there is certain configuration of *equipment under control* (EUC) and its control/protection system;
– there are associated human factor issues;

– the protection comprises the E/E/PE system or SIS, and there can be other safety measures for reducing risks.

Thus, a risk model for a specific application has to be developed taking into account the specific manner in which the necessary risk reduction is being achieved by the E/E/PE implementing given SF regarding other risk reduction measures. The risk measures indicated in Figure 5 are as follows:

– the *EUC risk* $R_{np}$ - the risk existing for specified hazardous event (no designated safety protective features are considered),
– the *tolerable risk* $R_t$ - the risk which can be presumably accepted regarding the expert opinion based on current societal values, and
– the *residual risk* $R_r$ - remaining risk for specified hazardous events after the risk reduction.

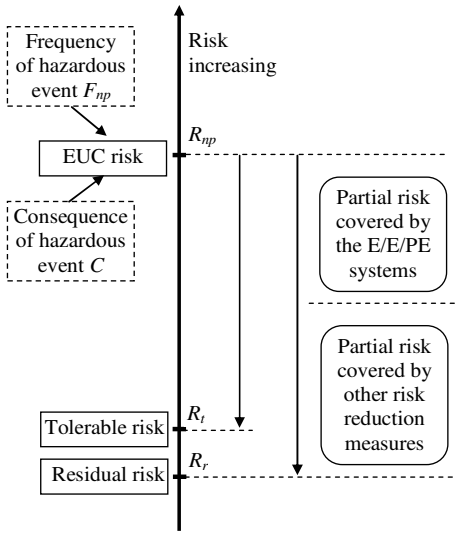


Fig. 5. Risk reduction for low demand mode of operation

The risk measure $R_{np}$ can be evaluated using the formula as follows

$$R_{np} = F_{np} C \tag{2}$$

where: $F_{np}$ is the frequency of a hazardous event (without considering protection), i.e. the demand rate on the safety-related system [$a^{-1}$]; and $C$ denotes a consequence of this hazardous event (in units of a consequence).

For this operation mode the required *average probability of protection system failure on demand* $PFD^{r}_{avg}$ can be calculated, assuming $C$ = const, from the formula

$$PFD^{r}_{avg} \le R_t / R_{np} = F_t / F_{np} \tag{3}$$

Knowing the value of $PFD^{r}_{avg}$ the required SIL for SF of interest, implemented using the E/E/PE system, is to be determined regarding relevant criteria interval in the second column of Table 1. For instance, if $PFD^{r}_{avg} = 3\text{x}10^{-4}$, then from this table the level of SIL3 is determined for random failure of hardware [5, 9]. Requirements concerning the SIL for software of E/E/PE system or SIS, implementing given SF are specified in part 3 of IEC 61508 [9].

Having required SIL for given SF, some architectures of the E/E/PE system or SIS (see Fig. 4) are considered. For each architecture the $PFD^{Sys}_{avg}$ is calculated using developed probabilistic model, to meet relevant interval criterion specified in Table 1 (preferably $PFD^{Sys}_{avg} \le PFD^{r}_{avg}$).

For the low demand mode the average probability of failure on demand of the E/E/E system can be calculated from following formula [5]

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

where: $T_A$, $T_B$ and $T_C$ denote the testing intervals to discover danger failures respectively for subsystems A, B, and C (see Figure 4) having relevant KooN configuration.

The probabilistic model for consecutive subsystems is to be built with regard to the reliability data for hardware elements and some parameters concerning *common cause failures* (CCF). In some cases potential *human errors* are to be considered, within relevant method of *human reliability analysis* (HRA) to calculate, with regard to *human factors*, the *human error probability* (HEP) [5].

In case of finding alternative architectures that meet the criterion for $PFD^{Sys}_{avg}$, some additional aspects are to be considered in selection of final architecture, for instance: costs, available diagnostics, programming requirements, experience in using similar solutions, testing requirements, training required, etc.

### 3.3. Functional safety and information security management in distributed control systems

One of the approaches to be proposed for security assessment and management within computerized control systems might be based on the series of standards ISO/IEC 62443 [3]. The objective was to develop a comprehensive set of cybersecurity standards for designing the *industrial automation and control systems* (IACS), also those for implementing within the *critical infrastructure* (CI) [3].

The assessment of *security levels* (*SLs*) is based in these standards on seven *foundational requirements* (*FRs*):

*FR 1 - Identification and authentication control (IAC),*
*FR 2 - Use control (UC),*
*FR 3 - System integrity (SI),*
*FR 4 - Data confidentiality (DC),*
*FR 5 - Restricted data flow (RDF),*
*FR 6 - Timely response to events (TRE), and*
*FR 7 - Resource availability (RA).*

Instead of compressing *SLs* down to a single number, it was proposed to apply a vector of *SLs* that uses the seven *FRs* specified above. Such vector allows definable separations between *SLs* for the different *FRs* [3].

Thus, a vector is to be used to describe the security requirements for a *zone, conduit, component, or system* instead of a single number. This vector may contain either a specific *SL* requirement or a zero value for each of the foundational requirements. General format of the *security assurance level* (SAL) description is as follows [3]:

$$\text{SL-?}([FR,]domain) = \{AC\ UC\ DI\ DC\ RDF\ TRE\ RA\} \tag{5}$$

where:

SL-? = *(Required)* the SL type, and the possible formats are: SL-T = *Target* SAL, SL-A = *Achieved* SAL, and SL-C = *Capabilities* SAL,

[*FR*,] = *(optional)* field indicating the *FR* that the *SL* value applies; *FRs* can be written out in abbreviated form instead of numerical form for better readability,

*domain* = (*required*) is the applicable domain that the *SL* applies; in the standards development process, this may be *procedure*, *system* or *component* - when applying the SL to a system, it may be for instance: Zone A, Pumping Station, Engineering Workstation, etc.

Some examples according to the standard [3]:
(a) SL-T(Control System Zone) = {2 2 0 1 3 1 3},
(b) SL-C(Engineering Workstation) = {3 3 2 3 0 0 1},
(c) SL-C(RA, Safety PLC) = {4}.

In the example (c) only the RA component is specified, of a 7-dimension SL-C. If *achieved* SAL < *target* SAL, some additional countermeasures are requested.

In Table 2 a risk matrix is proposed for combining the functional safety SIL-related requirements and the information security SAL-related requirements for four categories of criticality of consequences, four categories of probability, and four categories of risk: *very high risk* (VHR), *high risk* (HR), *medium risk* (MR), and *low risk* (LR). As it can be seen the level of SAL should be at least as high as SIL level, otherwise achieving SIL for given *safety function* (SF) could not be guaranteed.

Table 2. Risk matrix consisting of requirements for functional safety and information security for distinguished risk categories.

| SIL & SAL for **risk levels** | | Criticality of consequences | | | |
|---|---|---|---|---|---|
| | | *Minor* | *Low* | *Major* | *Severe* |
| Probability | *High* | ***MR*** SIL 2 SAL $2^+$ | ***HR*** SIL 3 SAL $3^+$ | ***VHR*** SIL 4 SAL 4 | ***VHR*** SIL 4 SAL 4 |
| | *Medium* | ***MR*** SIL 2 SAL $2^+$ | ***HR*** SIL 3 SAL $3^+$ | ***VHR*** SIL 4 SAL 4 | ***VHR*** SIL 4 SAL 4 |
| | *Low* | ***LR*** SIL 1 SAL $1^+$ | ***MR*** SIL 2 SAL $2^+$ | ***HR*** SIL 3 SAL $3^+$ | ***HR*** SIL 3 SAL $3^+$ |
| | *Rare* | ***LR*** SIL 1 SAL $1^+$ | ***LR*** SIL 1 SAL $1^+$ | ***MR*** SIL 2 SAL $2^+$ | ***HR*** SIL 3 SAL $3^+$ |

The countermeasures to apply for increasing SAL include:
- technical measures (antivirus, antispyware, firewalls, encryption, virtual private networks - VPN, passwords, authentication systems, access control, intrusion detection and prevention, network segmentation, etc.),
- security management (rights management, patch management for system & application, security incident management, training, etc.).

One of countermeasures to be considered is a *demilitarized zone* (DMZ) that aims to enforce the control network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the control network from outside attacks [2, 3].

## 4. CONCLUSIONS

In this article an approach is proposed how to integrate the functional safety concept with information security aspects in the design and management in operation of the industrial automation and control systems. The requirements concerning safety functions are expressed by the *safety integrity level* (SIL), and requirements referring to the information security are defined by the *security assurance level* (SAL) introduced in relevant standards. These levels are determined in risks evaluation processes and are verified for technical and organisational solutions considered.

## 5. BIBLIOGRAPHY


1. ISO 31000: Risk management -Principles and guidelines. Int. Organization for Standardization, 2012.
2. Stouffer K., Falco J., Scarfone K.: Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82. U.S. Depart. of Commerce, 2013.
3. IEC 62443: Network and system security for industrial process measurement and control. Parts 1-12, Int. Electrotechnical Commission. Geneva, 2008-2013.
4. Kosmowski K.T.: Current challenges and methodological issues of functional safety and security management in hazardous technical systems. Journal of Polish Safety and Reliability Association, 2012, Vol. 3 (1), pp. 39-51.
5. Kosmowski K.T.: Functional safety and reliability analysis methodology for hazardous industrial plants. Gdańsk University of Technology Publishers, 2013.
6. ISO 22301: Societal security - Business continuity management systems - Requirements, International Organization for Standardization, 2012.
7. Zawiła-Niedźwiedzki J.: Operational risk management in assuring business continuity of organization (in Polish). Wydawnictwo Edu-Libri, Kraków 2013.
8. ISO/IEC 27001: Information technology. Security techniques. Information security management systems. Int. Electrotechnical Commission, Geneva 2005.
9. IEC 61508: Functional safety of Electrical/ Electronic/ Programmable Electronic safety-related systems, Parts 1-7. Int. Electrotechnical Commission. Geneva 2010.
10. IEC 61511: Functional safety: Safety instrumented systems for the process industry sector. Parts 1-3. Int. Electrotechnical Commission, Geneva 2014.


# AKTUALNE KWESTIE ANALIZY I ZARZĄDZANIA RYZYKIEM W SYSTEMACH TECHNICZNYCH


Zajmowanie się niezawodnością i bezpieczeństwem obiektów przemysłowych wysokiego ryzyka wymaga uwzględnienia stosownej wiedzy interdyscyplinarnej i podejść opartych na tzw. dobrych praktykach inżynierskich, również tych, zawartych w międzynarodowych normach i poradnikach. W artykule zaproponowano podejście jak integrować koncepcję bezpieczeństwa funkcjonalnego z aspektami ochrony informacji w projektowaniu i zarządzaniu przemysłowej automatyki i systemów sterowania w procesie eksploatacji instalacji.



**Słowa kluczowe:** analiza ryzyka, systemy techniczne, zarządzanie ryzykiem, bezpieczeństwo funkcjonalne, ochrona informacji.