Kosmowski Kazimierz T.

Śliwiński Marcin

Piesik Emilian
Gdańsk University of Technology, Gdańsk, Poland

Integrated safety and security analysis of hazardous plants and systems of critical infrastructure

Keywords

hazardous plants, critical infrastructure, safety and security, protection systems, cyber security

Abstract

This article addresses an integrated safety and security analysis approach of hazardous industrial plants and systems of critical infrastructure. Nowadays due to new hazards that emerge there are opinions among experts that these issues require an integrated approach in life cycle, from the design concept, through the design and operation of the plant, to its decommissioning. It is proposed to start from an interesting methodology known as the security vulnerability analysis (SVA) developed for hazardous plants of chemical industry. It is based on rings of protection concept to secure widely understood assets. This concept seems to be compatible with layer of protection analysis (LOPA), which is consistent with functional safety concept of the control and protection systems including cyber security aspects. It is outlined how to use these approaches in an integrated way for safety and security analysis of hazardous industrial plants and systems of critical infrastructure.

1. Introduction

Nowadays the reliability and safety related assessments are not sufficient for decision making within management systems of hazardous industrial plant and systems of *critical infrastructure* (CI). In addition the security-related aspects have to be carefully considered. They include physical security of hazardous plants and technological installations, and cyber security of the computer systems and programmable control and protection systems in these plants [1].

The *security vulnerability analysis* (SVA) methodology [27] has been developed to allow companies to evaluate the vulnerability of their chemical sites to terrorist attack or other malicious acts and, based upon that assessment, to plan enhanced security where appropriate. The high consequence events that are possible from malicious acts at chemical sites should be considered in design and operation of these sites.

The possibility of a terrorist attack on a plant that manufactures or handles chemicals and dangers substances has been not fully considered in chemical release prevention studies. However, on September 11, 2001, this possibility became of greatly increased concern.

Similar events can be considered for other CI systems [21]. Some of them, e.g. power plants and electric grid distributing electrical energy in cases of blackouts of various extent can negatively influence functioning of other systems and safety and/or security of individuals and local society. Therefore, some frameworks are proposed for vulnerability assessment of electric power systems [4], [6], [9] and in particular of smart grid security [7], [28].

Important roles in the CI systems play nowadays computer systems, access control systems, and programmable control and protection systems that in hazardous plants reduce risks of abnormal states and major accidents [20]. These systems are more or less vulnerable on potential attacks, in particular cyber attacks. Therefore, the security of information storage and transmission in such systems and between them is becoming now of increasing concern [16]-[18], [23], [24].

A main difficulty in integrating the safety and security analyses and assessments is the fact that they

consist of two different kinds of requirements [5]. 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. [13], [18], [25]-[26]. 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 [2]-[3], [14], [16]:

- *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 intentional and they should be included in the security oriented risk analyses. 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 [16].

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 [11]-[12] and is applied in the process of design and operation of safety-related *electric, electronic and programmable electronic* (E/E/PE) *systems* [11] or *safety instrumented systems* (SISs) [12] in case of process industry. These systems perform specified functions to ensure that the risks are reduced and then maintained at acceptable levels [20].

Two different kinds of requirements are specified to ensure an 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].

The SISs are especially important for the safety of industrial hazardous 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 [25]. This kind of access will go through a number of networks used for other purposes, including partly the open Internet. This raises a number of security issues, ultimately threatening the safety integrity of SISs [18].

This article deals with current challenges and methodological issues of integrating the safety and security analyses concerning the hazardous plants and CI systems. In particular it concerns integrated analyses of the functional safety and security of the programmable control and protection systems of hazardous installations. The objective is to recognize some existing approaches for such analyses and propose directions of research in the domain.

2. Safety and security vulnerability analysis of hazardous plants

2.1. Concept of security vulnerability analysis

The hazardous industry is nowadays faced with the important need to assess whether current security measures effectively address new and unforeseen before threats, and make enhancements as required to provide for the safety of the public, workers, and the environment. Security improvements may be needed, especially at sites that pose a more attractive target to intentional malicious acts, in particular terrorist attacks due to their economic importance, perceived level of consequences, and other factors [27].

Chemical security has to be balanced with other objectives, and has to be commensurate with the threat and likelihood of occurrence. The security management process requires a systematic approach for analyzing risk of these issues. The process has to identify the potential threats facing the site, analyze how intentional acts may be carried out, and assess whether countermeasures are sufficient.

According to SVA [27] the potential events and consequences of interest include:

- Loss of containment of hazardous chemicals on the plant site from intentional damage of equipment or the malicious release of chemicals, which may cause multiple casualties, severe damage, and public or environmental impacts;
- Chemical theft or misuse with the intent to cause severe harm at the facility or offsite;
- Contamination or spoilage of site products to cause worker or public harm on or offsite;
- Degradation of assets or infrastructure or the business function or value of the facility or the entire company through destructive acts.

The consequences of a security event at a chemical facility are generally expressed in terms of acute health effects (e.g., fatality, injury), property damage, environmental effects, etc. This definition of consequences is the same as that used for accidental

releases, and is appropriate for security-related events. The key difference is that they may involve effects that are more severe than expected with accidental risk. Some examples of relevant consequences in a SVA include [27]:
- Public fatalities or injuries;
- Site personnel fatalities or injuries;
- Large-scale disruption to the national economy, public or private operations;
- Large-scale disruption to company operations;
- Large-scale environmental damage;
- Large-scale financial loss;
- Loss of critical data;
- Loss of reputation or business viability.

The estimate of *consequences* (C) may be different in magnitude or scope than is normally anticipated for accidental releases. In the case of security events, adversaries are determined to find vulnerabilities and to make an attack to maximize damage.

Threat (T) can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Sources of threats may be categorized as [27]:
- Foreign organizations/governments;
- Disgruntled employee or contractor;
- Criminal;
- Violent activist;
- Terrorist (political, religious, environmental).

Adversaries can be categorized as occurring from three general groups: *insiders, outsiders or insiders working as colluders with outsiders*.
Depending on the threat, the analyst can determine the types of potential attacks and, if specific information is available (*intelligence*) on potential targets and the likelihood of an attack, specific countermeasures may be taken.
Next unique term of interest is *vulnerability* (V) [27], which is *any weakness* that can be exploited by an adversary to gain unauthorized access to an asset. Vulnerabilities can result from, but are not limited to, *management practices, physical security weaknesses,* or *operational factors*.
In an SVA, vulnerabilities are evaluated either by broadly considering the threat and hazards of the assets they could attack or affect (which is referred to as the *asset-based approach* to determining vulnerabilities), or analyzed by considering multiple potential specific sequences of events, which is the *scenario-based approach*.
Not all targets are of equal value to adversaries, and this distinction is another factor that influences the likelihood of a security event. *Attractiveness of target* (A_T) is an estimate of the real or perceived value of a target to an adversary. For terrorist attacks, certain assets are likely to be targeted more than others since they better accomplish the terrorist's objectives. Possible target attractiveness factors [27]:
- Potential for mass casualties/fatalities;
- Extensive property damage;
- Proximity to national asset or landmark;
- Possible disruption or damage to company critical infrastructure;
- Disruption of the national, regional or local economy or infrastructure;
- Ease of access to target;
- Extent of media interest;
- Company reputation and brand exposure;
- Iconic or symbolic target.

During the SVA, consideration may be given to a qualitative rough estimate of A_T rather than to attempt to calculate the actual likelihood that an adversary will attack a particular target, since this calculation is not easily performed due to a lack of data. Surrogate factors can be used to relatively rank targets as more or less attractive to adversaries rather than to use a *likelihood of adversary attack* (L_A) estimate, which is a factor that is sometimes used in some security vulnerability analysis models [27].
Another likelihood factor to consider during an SVA is the *likelihood of adversary success* (L_{AS}) in causing a catastrophic event (mathematical complement of protection system effectiveness). L_{AS} is an estimate of the likelihood that the existing security countermeasures will be overcome by the attempted attack.
There are numerous subfactors involved in the analysis of L_{AS} and so this factor is also difficult to quantify. Alternatively, the SVA team can use their judgment to analyze the threat, vulnerabilities, and countermeasures to determine the ability of the adversary to achieve success.
Countermeasures are actions taken to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) (intent and/or capability) as well as the value of an asset or set of assets. The cost of a countermeasure may be monetary, but if the countermeasures are not employed there may also be nonmonetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.
Countermeasures include hardware, technical systems, software, interdictive response, procedures, and administrative controls. Some countermeasures are based on successful recognition and actions by humans, while some operate independently of human input.

During the SVA process, an assessment will be made of the effectiveness and reliability of the countermeasures against the threats and vulnerabilities of the assets. If deemed necessary based on the level of risk, *enhanced countermeasures* may be considered for ways of improving the existing security systems. Examples of such countermeasures include:

- Physical security;
- Access control;
- Loss prevention, material control and inventory management;
- Control room security;
- Crisis management and emergency response;
- Policies and procedures;
- Information/cyber security;
- Intelligence.

Security risk reduction at a site may include the following strategies [27]:

1. Deter, detect, and delay principles.
2. Physical or cyber protection layers of protection and rings of protection.
3. Procedures and administrative controls.
4. Inherently safer systems, to the extent that they can be designed and installed practically, particularly for existing processes.

2.2. Layers of protection

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 as regards random failures in the probabilistic modeling process [11]-[12]. It is important to include in probabilistic models potential dependencies between events representing equipment failures and/or human errors [20].

Figure 1 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 [11], [22].

The protection layers that include *basic process control system* (BPCS), the *alarm system* (AS) *human operators* and *safety instrumented system* (SIS) performing e.g. a function of *emergency shutdown* (ESD). The *protection layer* (PL) should be [22]:

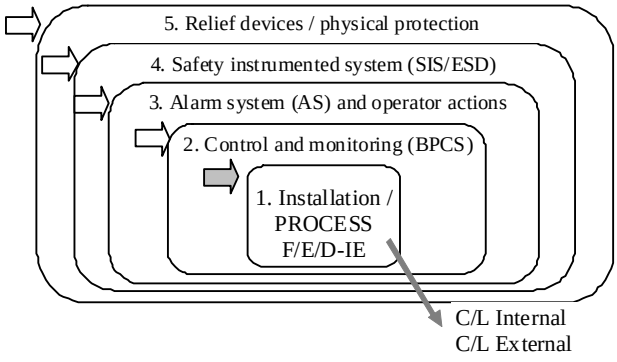
- *effective* in preventing the consequence when it functions as designed,
- *independent* of the initiating event and the components of any other PL already claimed for the same scenario,
- *auditable*, i.e. its effectiveness in terms of consequence prevention and probability of failure on demand (PFD) 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).

As it is illustrated in *Figure 1* an abnormal situation occur due to a combination of equipment *failures* (F), human *errors* (E), process *disturbances* (D) that can lead to an *initiating event* (IE). The range of *internal and external consequences* (C)/*losses* (L) will depend on functioning and dependability of the *protection layers* (PLs) specified in this figure.

Thus, the SVA team can make use of more formal methods of analysis, such as the LOPA, or fault tree analysis to judge the adequacy of sufficient independency of the PLs to the risk of an accident for a given scenario. This concept is based on the idea that for an undesired event to occur (accidental or malicious), a number of protective features and countermeasures must fail, assuming that appropriate layers (or barriers) have been designed into the process or site [27].

However, these systems and layers of protection should be functionally and structurally independent; however, it is not always possible in industrial practice, due to e.g. sharing of common elements, adverse technical and environment factors, the influence of *latent defects* or *human errors*, and a weak *safety culture* [20].



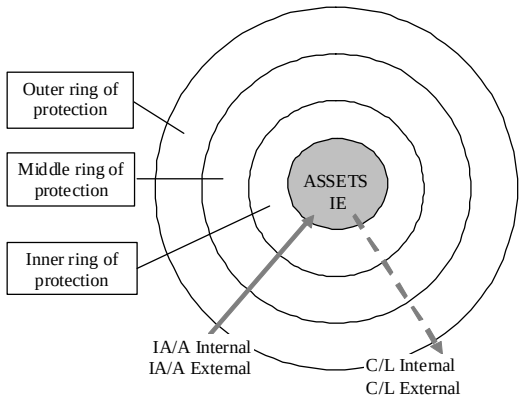
F-failures, E-errors, D-disturbances, IE-initiating events
C-consequences, L-losses

Figure 1. Typical protection layers in hazardous industrial installation

2.3. Rings of protection

A different concept is that of concentric rings of protection. The fundamental basis of this concept is that, if possible, the most important or most vulnerable assets should be placed in the center of concentric levels of increasingly more stringent

security measures. In the concept of rings of protection, the spatial relationship between the location of the target asset and the location of the physical countermeasures is important [27].
For instance, where feasible, the control room of process installation should not be placed right next to the building's reception area, but rather, it should be located deeper within the building. If an *intruder* plans to reach the control room, he would have to penetrate numerous rings of protection, such as a fence at the property line, a locked exterior door, an alert receptionist, an elevator with key-controlled floor buttons, and a locked door to the control room. Examples of typical rings of protection and their component countermeasures are shown in *Figure 2*.



IA-intentional action, A-attack, IE-initiating event
C-consequences, L-losses

Figure 2. Typical rings of protection

The *outer ring* in this figure may include [27]: *lighting, fences, entrance/exit points, bollards, trenches, intrusion detection sensors and smart alarming, guards on patrol at property fence line*, etc.
The *middle ring* may include for instance: *escort of visitors, locked doors, receptionist, badge checks, access control system, window bars, parcel inspection, turnstiles*, etc.
The *inner ring* may include such technical and organizational solutions as [27]*: alert personnel, door and cabinet locks, visitor escort policies, document shredding, access control devices, emergency communications, secure computer rooms, network firewalls and passwords policy*, etc.

In the case of malicious acts, the layers or rings of protection must be particularly robust because the adversaries are intentionally attempting to breach the protective features and can be counted on to use whatever means are available to be successful. This could include explosions or other initiating events that result in widespread common cause failures, the use of toxic gases to incapacitate all inhabitants of the control room simultaneously, or the simultaneous bypass of multiple protective features of process control systems. Some particularly motivated adversaries might commit suicide attempting to breach the security layers of protection [27].
An important objective of the control room and systems security is to establish physical security and procedural control measures to provide for the *integrity of control rooms, distributed control systems (DCS) and process logic controllers (PLC).*
A key feature in the overall system security program is to rigidly restrict access to the system itself. To accomplish this, management must rely heavily on control of physical space and physical connections.
It is necessary to *p*rovide additional and robust barriers for the control rooms, and not allow uncontrolled items and materials to be brought into the control room. Access to the process control equipment should limited to authorized personnel only and the control systems themselves should have appropriate password protection and other protective features (e.g., firewalls). Remote access via modem should be strictly limited and should have additional entry controls and appropriate encryption schemes.
The objective of *information/cyber security* is to protect critical information systems including hardware, software, infrastructure, and data from loss, theft, or damage.
In a hazardous chemical facility, protecting information and computer networks means more than safeguarding a company's proprietary information and keeping the business running, as important as those goals are. It also means protecting chemical processes from hazardous disruptions and preventing unwanted chemical releases [27].

3. Methods for functional safety and security analysis and management

3.1. Programmable control and protection systems for implementing safety-related functions

Industrial plants are equipped with complex programmable control and protection systems operating nowadays within a computer network. For designing such systems a functional safety concept [11] is more and more widely of interest, to be implemented in various industrial sectors, including the process industry [12].
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. [19]-[20].

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 may contribute 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 within DCS (*distributed control system*), e.g. the BPCS as shown in *Figure 1*.
The standard IEC 61511 [12] distinguishes two kinds of programmable systems, namely the *basic process control system* (BPCS) and the *safety instrumented systems* (SISs). The BPCS is designed according to the technical specifications determined for normal, transient and abnormal situations, and the SIS implements some SrFs important in case of potential hazardous situations and major accidents, e.g. a function of *emergency shutdown* (ESD).

3.2. Requirements for data communications in distributed control systems

Dependability of data communication in safety function implemented using relevant transmission channels should be evaluated including such a measure as the probability of undetected failure in the communication process taking into account transmission errors, repetitions, deletion, insertion, re-sequencing, corruption, delay and masquerade (when true contents of a message are not correctly identified) [11].

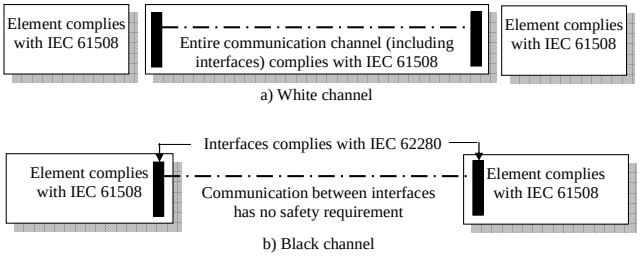


Figure 3. Data communication channels [11]

The techniques and measures necessary to ensure the required level of failure measure (e.g. the probability of undetected failure) of the communication process shall be implemented according to the requirements of part 3 of IEC 61508. Two approaches may be applied:
– the entire communication channel shall be designed, implemented and validated according to IEC 61508 (*white channel* in *Figure 3*), or
– parts of the communication channel are not designed or validated according to IEC 61508 (*black channel* in *Figure 3*); 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 designed in accordance with IEC 62280.

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.
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.
Also the SISs have to carefully considered as regards the data communication, especially in 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 can go through a number of networks used for various purposes, including even the open Internet. This raises a number of security issues, ultimately threatening the safety integrity of SIS [25].

3.3. Idea of the evaluation assurance level

As it was mentioned the standard [11] defines the safety and security respectively 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 [14] defines criteria referred often to as the *common criteria* (CC), used as the basis for evaluating the security properties of *information technology* (IT) products and systems. These criteria permit 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). The TOEs are for instance: *operating systems, computer networks, distributed systems*, and *applications*.
The objective is to protect information from such failures as: *unauthorized disclosure*, *modification*, or *loss*. The *categories of protection* relating to these three types of failure are called *confidentiality*, *integrity*, and *availability*, respectively. The CC may also be applicable to some 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 [14].
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.
The *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). The TOE *security function* (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* is considered as a set of rules that regulate how assets are managed, protected and distributed within a TOE.
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 [14].
The security concept outlined in the standard ISO/IEC 15408 is shown in *Figure 4*. 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.

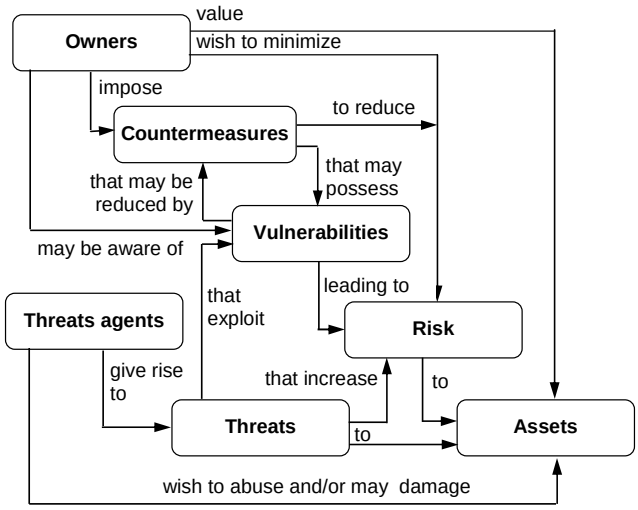


Figure 4. Security concepts and relationships [14]

The *security assurance requirements* (SAR) are grouped into classes. There are 8 *assurance classes* of the CC described in part 3 of ISO/IEC 15408:
- 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 group some sets of security requirements. 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.
In *Figure 5* a decomposition diagram for the *class vulnerability assessment* is presented. In *Table 1* the *evaluation assurance levels* (EALs) from 1 to 7 are presented for vulnerability assessment class for four assurance family positions distinguished in the standard [14].

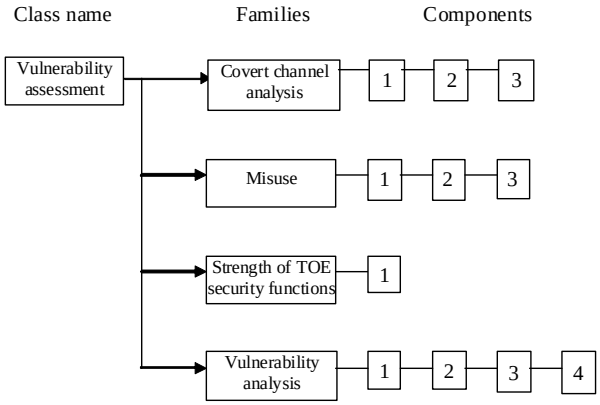


Figure 5. Decomposition diagram for vulnerability assessment class

Table 1. Evaluation assurance levels (EALs) for vulnerability assessment class

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 EALs can be characterised as follows [14]:
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 products and systems and the assurance measures applied to them meet specified requirements. The evaluation results obtained 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*, such as information and data, is needed to protect them from unauthorized *disclosure*, *fraud*, *abuse* or *waste* [14].
Sensitivity is determined with regard to 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, the IT product or system considered should have appropriate protection. This safeguard is strictly connected with estimated levels of sensitivity and criticality. The strength of security level may be determined also by a number of protection rings. For higher EALs the number of protection rings increases.
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 the designer and user 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 [14].

3.4. Idea of the security assurance level

Another approach for security assessment for industrial automation and control systems might be based on the standard ISO/IEC 62443 [13]. This series of standards is organized into four categories of documents:
- *General concept* – relevant documents are overarching in nature and apply to the entire series of standards and technical reports.
- *Policy and procedure* – these documents address the organizational aspects of policies and procedures for cyber security.
- *System* – these documents address the system-level technical aspects of cyber security, including system design principles and system capabilities
- *Component* – these documents address the component-level technical aspects of cyber security, including development processes and component capabilities.

The objective is to develop a comprehensive set of cybersecurity standards for *industrial automation and control systems* (IACS) and *critical infrastructure* (CI). Unlike programs targeted at specific industries, the initiative is applicable to *all key industry sectors* and *critical infrastructure* in recognition of the interrelated nature of industrial computer networks in which cyber vulnerabilities exploited in one sector can impact multiple sectors and infrastructure.
General Concept is applied to subjects that are important to the understanding of the material in the ISO/IEC 62443 series, and are fairly common in the

general area of cyber security. The following general concepts have been identified:
- *Security context,*
- *Security objectives,*
- *Threat risk assessment,*
- *Security levels,*
- *Security lifecycle,*
- *Security program maturity,*
- *Security policies,*
- *Defence in depth,*
- *Security zones and conduits,*
- *Role based access control.*

In addition to the general concepts, the first standard in the series, ISA-62443-1-1, defines a set of foundational requirements which serve as a common frame of reference in the remaining documents in the series. These *foundational requirements* are:
- *Identification and authentication control,*
- *Use control,*
- *System/data integrity,*
- *Data confidentiality,*
- *Restricted data flow,*
- *Timely response to events,*
- *Resource availability.*

These requirements are used for semi-formally describing the security levels as well as to structure the technical requirements on the system and component levels.
A concept of *security assurance level* (SAL) is introduced in this normative document. Four security levels are distinguished (from SAL1 to SAL4). They are assessed for each security zone of interest using the set of seven functional requirements [13].
The SAL is relatively new security measure concerning the control and protection systems which is evaluated based on a defined vector of seven *foundational requirements* specified above for relevant security zone:

$$SAL = \{AC \;\; UC \;\; DI \;\; DC \;\; RDF \;\; TRE \;\; RA\} \quad (1)$$

where: *AC* - identification and authentication control, *UC* - use control,, *DI* - data integrity *DC* - data confidentiality, *RDF* - restricted data flow, *TRE* - timely response to events, *RA* - resource availability.

Requirements for an IACS security management system given in part 2-1 [13], describes the characteristics and requirements for a security program, but it allows individual organizations flexibility in how to implement it. This is important because some organizations already have well established security programs for the IACS.

These requirements include the *identification, classification, and assessment of risk* taking into account the *systematic identification, prioritization and analysis of threats, vulnerabilities and consequences*. Specific requirements include:
- Select a risk assessment methodology,
- Provide risk assessment background information,
- Conduct a high-level risk assessment,
- Identify industrial automation and control systems,
- Develop simple network diagrams,
- Prioritize systems.

4. Integration of the functional safety and security analysis and management

4.1. Integration concept of the safety and security analysis

As it has been discussed in the system development and operation in life cycle both safety and security aspects should be considered and treated for implementing in a rational way in industrial practice. In *Figure 6* an idea is illustrated for integrated safety and security management of critical infrastructure systems in life cycle.

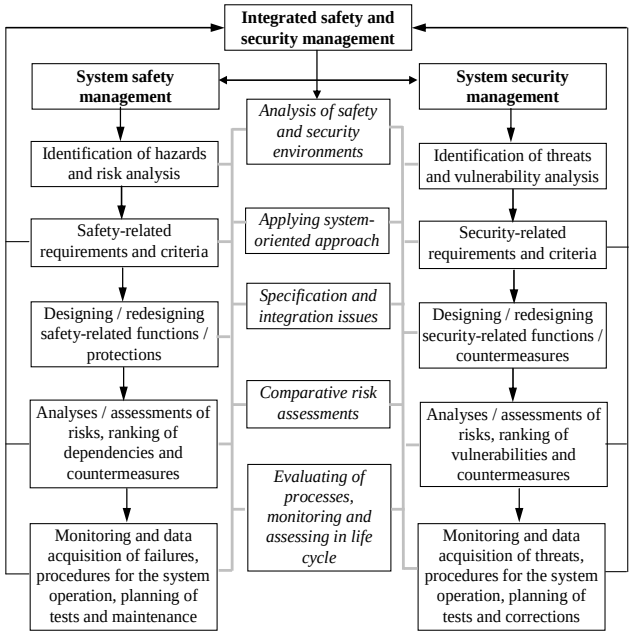


Figure 6. Integrated safety and security analysis and management of critical infrastructure systems

Although the concepts of the functional safety and security of programmable systems are outlined in respectively standards [11], [13], the security techniques for *information technology* (IT) and requirements for the IT management systems are

described in the standard [15]. The security techniques and evaluation criteria for IT proposed in standard [14] are outlined above. In the document [10] there is discussed an interface between safety and security at nuclear power plants.

As it is shown in *Figure 6* there are two paths, respectively, of the safety and security analysis and management. In the middle of this figure there are blocks that may be treated as interfaces between relevant analyses concerning the safety and security. They include:

- *Analysis of safety and security environments,*
- *Applying system-oriented approach,*
- *Specification and integration issues,*
- *Comparative risk assessments,*
- *Evaluating of processes, monitoring and assessing in life cycle.*

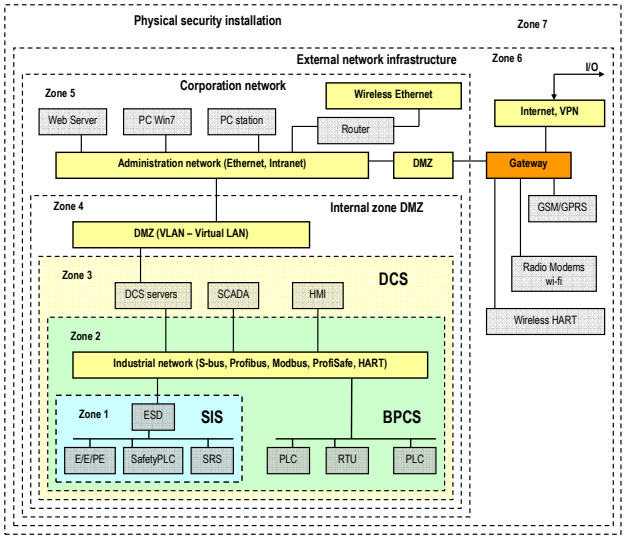


Figure 7. An example of industrial computer system and communication network

Described in *Chapter 3* methods are not integrated. Additional research effort should be undertaken to develop integrated, systemic oriented methodology for the functional safety and security analysis and management. In particular the following issues require attention to be considered to find solutions for implementing in the industrial practice:

- identifying existing and emerging hazards and threats for distinguished categories of IT systems and their operation environments ,
- probabilistic modeling of IT systems with regard to safety and security aspects and development of relevant risk models,
- identifying more important technical and human, organizational and environmental factors influencing risks and vulnerabilities of computer systems and networks,
- integrated risk assessment with regard to quantitative and qualitative information available,
- designing adequate countermeasures including technical and organizational solutions for effective risk reducing,
- development of integrated safety and security policy for operation of hazardous installations, computer systems and networks.

An example of industrial computer system and network is shown in *Figure 7.*

4.2. Methods for integrated functional safety and security analysis

The classification of computerized systems networks is useful for the integrated design and operation requirements with reference to general safety and security aspects. The industrial hazardous installations and CI systems with their safety-related control and protection systems can be classified into three main categories [18]:

I. Concentrated critical installations, e.g. power plant, refinery, chemical plant, etc.,
II. Distributed critical installations, where protection and monitoring system data can be send by outside communication channels, e.g. oil or gas pipelines, energy systems,
III. Distributed critical systems, where protection and monitoring system data is to be sending by external communication channels, e.g. transportation systems like railway, road transport monitoring and control, aviation systems, etc.

Proposed classification is related to the data transfer conduits between subsystems of given system. Important data can be transmitted by: (I) an internal network system for a first category system, (II) using external communication channels (e.g. stationary networks, GSM, satellite communication) for a second category system, or (III) either solution for 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 the SCADA system in given hazardous distributed plant and some CI systems.

As it was discussed the modeling methods proposed in the standards IEC 61508 [11] and IEC 61511 [12]

do not fully include the computer network elements and communication conduits. Thus, the results obtained in the analysis of given safety-related function can be too optimistic.

A communication channel between controllers may be treated in some cases as a hardware block with determined SIL. An example of *reliability block diagram* (RDB) for an industrial computer communication network is shown in *Figure 7*. It requires careful defining of functional and probabilistic parameters of components and communication conduits to obtain correct results of probabilistic modeling to be useful for verifying the SIL of safety-related functions of interest.

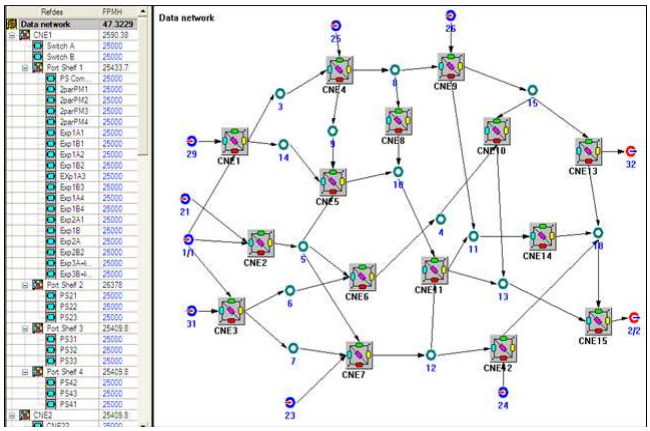


Figure 8. RBD model of an industrial computer network with communication conduits

Knowing from the risk analysis and assessment the required SIL (from SIL1 to SIL4) for given safety-related function it is necessary to verify this SIL taking into account the security-related levels for communication conduits involved, e.g. SAL [13] or EAL [14]. Depending on level of security: *low*, *medium* or *high* (see *Table 2*) in relation to the EAL or SAL it is necessary to verify the SIL as shown for systems of category II (III). For low level of security (EAL 1 or 2; SAL 1) the SIL would be reduced.

Table 2. SIL that can be claimed for given EAL or SAL for systems of category II (III)

Determined *security*			Verified SIL for category II (III) *functional safety*			
EAL	SAL	Level of security	1	2	3	4
1	1	low	- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
2	1		- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
3	2	medium	SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
4	2		SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
5	3	high	SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
6	4		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
7	4		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)

4.3. Distributed computer networks and designing rings of protection

Several cyber security measures can be proposed for more secure operation of programmable control and protection systems, designed e.g. within *distributed control system* (DCS) of an industrial hazardous installation. They are often design according to a concept of protection rings [20], [22], [25]. Examples of such rings are shown in *Figure 9*.

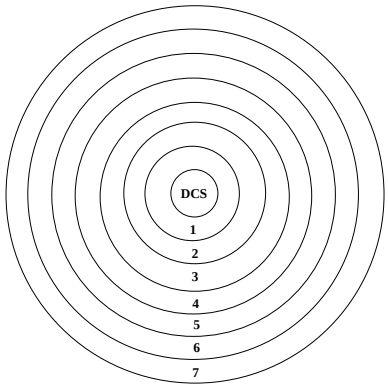


Figure 9. Examples of protection rings within distributed control system

Consecutive rings shown in *Figure 9* are designed applying solutions as follows [20], [25]:

1 – *Malware detection and prevention* (including antivirus and whitelisting),
2 – *Patch management*,
3 – *User account management* (UAM) – administration of the 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),

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.

The design and use in industrial practice of such rings should be done with active contribution of the experienced computer network administrator and supervised in time by certified specialists according to rules developed within an integrated proactive functional safety and security management system [15]-[16], [20], [24], [28].

5. Remarks on selected issues of security analysis

5.1. Defining the risk matrix for security related analysis

An example of the risk ranking matrix for the security vulnerability analysis shown in *Table 3*. Each category of severity and likelihood may be defined with regard to qualitative or preferable quantitative information available for given case of hazardous system considered [22].

Table 3. Example of risk ranking matrix for five levels of severity (S) and likelihood (L)

$S \rightarrow$ $L \uparrow$	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

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 [11], [12].

For the comparative 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 often used in industrial practice. Many variations of this method, redefined by the companies and PHA teams, exist and have been successively used in industrial practice.

The assessed risk levels may be classified as follows (see *Table 3*) : R_1 – *tolerable*, R_2 – *tolerable conditionally*, if costs of the risk reduction is too high, R_3 – *tolerable conditionally*, but the risk must be reduced in given time horizon, R_4 – *intolerable* (the risk must be reduced in a relatively short time horizon agreed upon), R_5 – *inacceptable* (the installation must be shut-down and its 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 [22]:

- *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 and procedural changes, physical security upgrades, barriers, rings, software upgrades, the addition guard, etc. should be considered [16]-[17], [22]. For instance, the *access control system* classification considers the security level based on two basic items: *identification class* and *access classification*.

There are some problems to protect the computer resources of hazardous distributed installation. It is suggested to perform relevant analyses within the *Information Security Management System* (IS MS), designed e.g. according to principles of the standard series ISO/IEC 27000, with requirements specified according to the standard [15]. However, such ISMS should include the security management of the programmable control and protection systems with regard to results of relevant risk assessments [11], [20].

Thus, in the context of functional safety should be included to support effectively the cyber security management of programmable control and protection systems including the BPCS/DCS and SIS/ESD operating within technological installation and other computer systems in industrial IT networks or the CI systems.

5.2. Issues of cyber security in smart grids

The *smart grid* (SG), often referred to as the next-generation power system and is considered as a evolutionary regime of existing power grids. More importantly, with the integration of advanced computing and communication technologies, the SG is expected to greatly enhance efficiency and reliability of future power systems with renewable energy resources, as well as distributed intelligence and demand response [28]. Along with the features of the SG, cyber security emerges to be a critical issue because millions of electronic devices are interconnected via communication networks throughout critical power facilities, which has an immediate impact on reliability of such a distributed, widespread infrastructure.

Power system communication protocols have been evolving for decades, from various proprietary protocols to recently standardized protocols. There are two widely-used protocols in power systems: the distributed networking protocol 3.0 (DNP3) that is currently the predominant standard used in North America power systems, and IEC 61850 that is

recently standardized for modern power substation automation by the *International Electrotechnical Commission* (IEC) [28].

The DNP3 is a power communication protocol originally developed by General Electric that made it public in 1993. DNP3 was first designed for supervisory control and data acquisition (SCADA) applications and is now widely used in electrical, water infrastructure, oil and gas, security and other industries in a number of countries, including North America, South America, Asia and Australia.

The DNP3 was initially designed with four layers: *physical*, *data link*, *transport*, and *application layers*. The original physical layer was based on serial communication protocols, such as *recommended standard* (RS)-232, RS-422, or RS-485. Today the DNP3 has been ported over to the TCP/IP layer to support recent communication technologies, and thus can be regarded as a three-layer network protocol operating upon the TCP/IP layer to support end-to-end communication [28].

The standard IEC 61850 is a recent standard recommended by IEC for Ethernet-based communications in substation automation systems. It differs from DNP3 that is based on TCP/IP protocol. IEC 61850 specifies a series of protocol stacks for a variety of services, including TCP/IP, UDP/IP, and an application directly-to-MAC stack for time-critical messages. In addition, IEC 61850 explicitly defines timing requirements for information and data exchange in power substations.

There are some delay requirements for IEC 61850 messages, which reveals that the power substation communication features a number of time-critical messages with application-layer delay constraints varying from 3 ms to 500 ms [28]. Several types of messages are distinguished including:

- Types 1A/P1 and 1A/P2 that are used for fault isolation and protection purposes, thus having very strict delay constraints.
- Types 1B/P1 and 1B/P2 that are used for routine communications between automation systems.
- Types 2 and 3 are used for less time-critical information exchange, such as monitoring and readings, in substations.

It is worth to mention that IEC 61850 is intended to replace DNP3 in substation communications [28]. However, current IEC 61850 is only limited within a power substation, but it is generally believed that IEC 61850 can be potentially used for outside substation communication in future power systems.

Availability, integrity, and confidentiality are three high-level cyber security objectives for the SG. In addition to such high-level objectives, the *National Institute of Standards and Technology* (NIST) report also recommends specific security requirements for the SG, including both *cyber security* and *physical security* [28]. The *cyber security* part specifies detailed security issues and requirements related to the SG information and network systems; and the *physical security* part specifies requirements pertaining to physical equipment and environment protection as well as employee security policies.

There are following three high-level SG objectives [4], [16], [28]:

- *Availability*: Ensuring timely and reliable access to and use of information is of the most importance in the SG. This is because a loss of availability is the disruption of access to or use of information, which may further undermine the power delivery.
- *Integrity*: Guarding against improper information modification or destruction is to ensure information nonrepudiation and authenticity. A loss of integrity is an unauthorized modification or destruction of information and can further induce incorrect decision regarding power management.
- *Confidentiality*: Preserving authorized restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information. This is in particular necessary to prevent unauthorized disclosure of information that is not open to the public and individuals.

The potential attacks can be categorised as follows [16], [28]:

- Attacks targeting availability, also called denial-of-service (DoS) attacks, attempt to delay, block or corrupt the communication in the SG.
- Attacks targeting integrity aim at deliberately and illegally modifying or disrupting data exchange in the SG.
- Attacks targeting confidentiality intend to acquire unauthorized information from network resources in the SG.

Thus, the design of secure network architectures for the SG includes a very broad scope of issues in networking, computing, securing, and effective cryptographic solutions. Therefore, it requires a comprehensive view on the safety and security policies and requirements for the SG.

6. Conclusions

The industry currently faces problems to assess whether current security measures effectively address new threats and to make enhancements to provide effective safety and security measures to protect adequately the workers, public and the environment.

Security of industrial hazardous plants should 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.

It has been suggested to integrate some existing approaches for the safety and security analyses proposing integrated methodology to be useful in industrial practice. Such methodology should be compatible with existing standards developed by international organizations.

There are challenges and methodological issues of integrating the safety and security analyses of hazardous plants and CI systems. In particular it concerns integrated analysis for the management of the functional safety and security of the programmable control and protection systems.

Cyber security in the smart grid (SG) is a new area of research that has attracted rapidly growing attention in the power industry, innovative institutions and academia.

The system security analyses and risk assessments are supported intensively on expert opinions who use often qualitative information. Further research should be undertaken to develop integrated methodology that include defining compatible criteria for the safety and security related assessments.

References

[1] API (2005). Security Guidelines for the Petroleum Industry. American Petroleum Institute, Washington.

[2] Białas, A. (2007). Advanced IT Security Development Process - through Enhancement of IT Security Development Process to better Assurance. In: Functional safety management in critical systems (Ed. K.T.Kosmowski). Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk.

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

[4] Brinkman, B., et al. (2015). Regulation of Physical Security for the Electric Distribution System. California Public Utility Commission.

[5] Cambacédès, L. P. & Chaudetb, C. (2010). The SEMA referential framework: Avoiding ambiguities in the terms “security” and “safety”. International Journal of Critical Infrastructure Protection 3 (55-66).

[6] Dołęga, W. (2011). The role of distribution system operator in the context of energy security – the case of Poland, Przegląd Elektrotechniczny (Electrical Review) 2 (57-60).

[7] ENISA (2012). Smart Grid Security: Recommendations for Europe and Member States. European Network and Information Security Agency.

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

[9] Holmgren, A. J. (2006). *A Framework for Vulnerability Assessment of Electric Power Systems*. Division of Safety Research, Royal Institute of Technology. KTH Sweden.

[10] IAEA INSAG24 (2010). The Interface Between Safety and Security at Nuclear Power Plants. International Atomic Energy Agency, Vienna.

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

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

[13] IEC 62443 (2008-2013). Network and system security for industrial-process measurement and control. Parts 1-12, International Electrotech-nical Commission. Geneva.

[14] ISO/IEC15408 (1999). Information Technology. Security Techniques. Evaluation Criteria.

[15] ISO/IEC 27001 (2005). Information technology. Security techniques. Information security management systems. Requirements.

[16] Kisner, R. A., et al. (2010). Cybersecurity through Real-Time Distributed Control Systems. Oak Ridge National Laboratory, ORNL/TM-2010/30.

[17] Klimburg, A. (Ed.) (2012). National Cyber Security: Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Tallinn.

[18] Kosmowski, K. T., Śliwiński, M. & Barnert, T. (2006). Functional safety and security assessment of the control and protection systems. ESREL2006, Estoril. Taylor & Francis Group, London.

[19] Kosmowski, K. T., Śliwiński, M., Barnert, T. & Porzeziński, M. (2012). Functional Safety Assessment within the Risk Informed Decision Making Process. Joint PSAM 11 & ESREL 2012 Conference, Helsinki.

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

[21] Lewis, T.G. (2006). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley-InterScience, John Wiley & Sons, Hoboken.
[22] LOPA (2001), Layer of Protection Analysis, Simplified Process Risk Assessment. Center for Chemical Process Safety. American Institute of Chemical Engineers, New York.
[23] OECD/IFP (2011). Project on Future Global Shocks. Reducing Systemic Cybersecurity Risk. IFP/ WKP/ FGS.
[24] Radvanovsky, R. (2006). Critical Infrastructure: Homeland Security and Emergency Preparedness. Taylor & Francis Group, London.
[25] SINTEF SeSa (2007). The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems. SINTEF A1626.
[26] Stouffer, K., Falco, J., Scarfone, K. (2013). Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology. NIST Special Publication, 800-82.
[27] SVA (2003). Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York.
[28] Wang, W. & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. Computer Networks 57, 1344–1371.