Kosmowski Kazimierz T., 0000-0001-7341-6750
Gdańsk University of Technology, Gdańsk, Poland, kazkosmo{at}pg.edu.pl

Business continuity management framework for Industry 4.0 companies regarding dependability and security of ICT and ICS/SCADA system

Keywords

business continuity management, Industry 4.0, information technology, operational technology, industrial control system, dependability, functional safety, cyber security, organisational culture

Abstract

This chapter addresses a business continuity management (BCM) framework for the Industry 4.0 companies including the organizational and technical solutions, regarding the dependability and security of the information and telecommunication technology (ICT), and the industrial control system (ICS) / supervisory control and data acquisition (SCADA) system. These technologies and systems play nowadays important roles in modern advanced manufacturing systems and process plants due to their openness to external systems and networks using various communication channels. It gives on the one hand, some advantages in effective realization of technological and business processes, logistics and distribution of goods, but, on the other hand, makes the company assets and resources potentially vulnerable to some threats with relevant risks. The chapter outlines some ideas related to designing a business continuity management system (BCMS) based on defined processes and procedures. Such system includes planning of changes in organization / industrial company, nonconformity issues, and planning corrective actions. In a final part of this chapter the leadership importance, and staff awareness and responsibility are emphasized to create a robust and healthy corporate culture based on accepted values, properly spread among the employees. It is beneficial for shaping good organizational culture, and then safety and security culture. The BCM approach outlined in this chapter distinguishes both preventive and recovery activities regarding suggestions in selected international standards and domain publications.

1. Introduction

An important issue in the Industry 4.0 companies (IS, 2019; Kosmowski, 2021) is the business continuity management (BCM) (ISO/DIS 22301, 2019) that requires careful consideration of various aspects within an integrated RAMS&S (reliability, availability, maintainability, safety, and security) framework. In such analyses the risk evaluation and management in life cycle is of special interest for both the industry and insurance companies (Gołębiewski & Kosmowski, 2017; Kosmowski & Gołębiewski, 2019).
These issues are also important in the domain of performability engineering that has been stimulated by Misra for many years (Misra, 2021).

In this chapter a framework is proposed for the BCM that enables to deal systematically with potential influences on the industrial plant's dependability, safety, and security due to various reasons. A special attention is paid to the ICT and ICT/SCADA systems that operate in industrial computer systems and networks using the wire and lately also wireless communication channels. These systems and networks have been considered in some publications and reports from a conceptual perspective of the systems engineering (SE, 2001; Kosmowski, 2020) or cyber-physical systems (CISA, 2020; Leitão et al., 2016). Some research projects were undertaken concerning integrated analyses and modelling of the ICS safety

Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2021.

DOI: 10.26408/srsp-2021-13.

and security (MERgE, 2016; SESAMO, 2014). Interesting scientific works were also published concerning the business continuity management, for instance (Boehmer, 2009) and monograph (Zawiła-Niedźwiecki, 2013).

The functional safety and cyber security issues of the industrial automation and control systems (IACS) are often emphasized as especially important in the design and operation of hazardous plants (HSE, 2015; Kosmowski, 2020).

In this chapter current scientific issues are considered from a general perspective of BCM regarding the dependability and security of ICT and ICS/SCADA systems with distinguishing required functionality and architectures of the information technology (IT) and operational technology (OT) systems and networks (Kosmowski et al., 2019). These systems require effective convergence to obtain manufacturing functionality and better effectiveness in realization of advanced business-related processes in Industry 4.0 companies.

Some security-related issues of the industrial automation and control system (IACS) are also considered in the context of protection solutions proposed for improving its resilience and security according to the standard IEC 62443 (IEC 62443, 2018). The dependability and safety integrity of the ICS safety-related part are usually analysed regarding a generic functional safety standard IEC 61508 (IEC 61508, 2016).

An approach is outlined for integrated functional safety and cybersecurity management in life cycle based on determining and verifying the safety integrity level (SIL) of the safety-related ICS system regarding the security assurance level (SAL) assigned to relevant security domain.

The main objective of this chapter is to outline a conceptual framework for the business continuity management (BCM) regarding mentioned systems. It outlines a holistic management process that identifies potential hazards and threats to an organization and their potential impact on business operations that those threats, if realized, might cause including disruptions with relevant losses. Its purpose is to provide a framework for building organizational resilience and preparing an effective response of safeguards being important for the key stakeholders, authorities, brand, reputation, and value-creating activities.

The BCM includes the recovery managing and/or the continuation of business activities in the situation of business disruption, and integrated management of the overall program through training, exercises, and reviews, to ensure the business continuity plan(s) stays current and up to date.

The organization should elaborate a process for identifying and delivering the BCM awareness requirements in the organization and evaluating its effectiveness. The BCM staff should make themselves aware of any external BCM related information. This may be done in conjunction with seeking guidance from emergency services, local authorities, and regulators (BS 25999–1, 2006).

Raising and maintaining awareness of BCM with all the organization's staff is important to ensure that they are convinced about BCM importance to the organization in changing conditions. They should be also aware that this is a lasting initiative and has an ongoing support of the top management.

2. Proactive strategy for business continuity management

2.1. Business continuity management concept and requirements

Business continuity management (BCM) is usually understood as the capability and specified activity of an organization to continue delivery of products and/or services of required quality within acceptable time frames at predefined capacity relating to the scale of potential disruptions (Gołębiewski & Kosmowski, 2017).

A disruption is defined as an incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objective. The objective includes a result to be achieved and can be strategic, tactical, or operational in relevant time horizon.

The objective can be expressed in terms of an intended outcome, a purpose, an operational criterion, or using other words with similar meaning (e.g., aim, goal, or target). Objectives can be related to different disciplines such as financial, health and safety, also environmental objectives to be applied at various activities, e.g., strategic, organization-wide, project, product, and process (ISO/DIS 22303, 2019).

For a business continuity management system (BCMS) to be designed and implemented in in-

dustrial practice, some business continuity objectives should be set by the organization, consistent with the business continuity policy, to achieve specific objectives. Thus, the BCMS refers to a management system for supporting required business continuity activities. It is known that an effective management system includes the organizational structure, policies, planning activities, responsibilities, processes and/or procedures, and required resources. The BCMS, like any other modern management system, includes following components (ISO/DIS 22301, 2019):

- policy, goals, knowledgeable staff, and competent personnel with carefully defined roles and responsibilities,
- management processes, related to planning, implementation and operation, performance assessment, audits, management reviews, and continual improvement,
- documented information supporting operational control and enabling performance evaluation.

The BCMS should also include two important elements:

- business continuity plan,
- business impact analysis.

Business continuity plan (BCP) consists of documented information that guides an organization to respond to a disruption and resume, recover and/or restore the delivery of products and services consistent with its business continuity objectives.

Business impact analysis (BIA) is a process of analyzing the impact of a disruption on the organization. The outcome is a statement and justification of business continuity requirements. Resilience is understood as an ability to absorb and adapt in a changing environment to avoid abnormal and/or danger situations that can lead to hazardous events and major losses.

An event can be occurrence or change of a particular set of circumstances that could have several causes and several consequences. An abnormal event due to a hazard or threat is considered as a source of risk. An emergency is a result of sudden, urgent, usually unexpected occurrence, or event requiring immediate action. Emergency is understood as a disruption or condition that can be anticipated or prepared for, but seldom exactly foreseen (ISO/IEC 24762, 2008).

The organization shall implement and maintain a systematic risk assessment process. Such process could be made, for instance, regarding general suggestions of the ISO 31000 standard. Interested organization, as it is illustrated in Figure 1, should:

- identify risks of disruption to the organization's prioritized activities and to their supporting resources,
- systematically analyze and assess risks of potential disruptions,

  evaluate risks of disruptions that require special treatment.

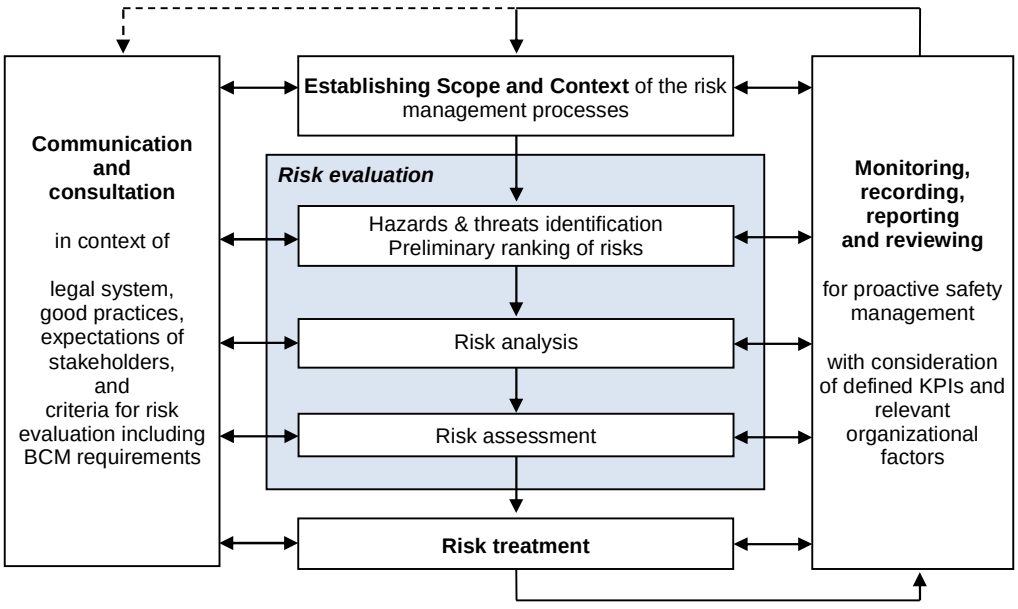

Figure 1. Risk management process, based on (ISO/IEC 27005, 2018).

In this standard risk is defined generally as an effect of uncertainty on objectives. The effect is a deviation from the expected and can be positive, negative or both, and it can address, create, or result in opportunities and threats. Objectives can have different aspects and some categories to be applied at relevant level of the hierarchy. Thus, the risk can be expressed in terms of the risk source and potential event with its consequence, and likelihood or probability.
The risk evaluation is to be considered as an overall process of hazards/threats identification, risk analysis and risk assessment (ISO/IEC 27005, 2018). Risk management is a process of coordinated activities to direct and control an organization regarding risk.
General purpose is to reduce an industrial system vulnerability as required or increase its resilience as justified considering current legal and/or regulatory requirements. Relevant protection measures should be proposed that safeguard resources and enable an organization to prevent or reduce the impact and consequences of potential disruptions.
After the disruption, the recovery process must be undertaken to effectively restore the system and improve, where appropriate, activities, operations, facilities, and conditions of affected organization, including efforts to reduce in the future operation process more effectively important risk related factors identified and increase the business effectiveness.

2.2. Scope of BCM in industrial companies

There are various approaches proposed to apply in industrial practice the BCM concept outlined above. The standard BS 25999–1 (BS 25999–1, 2006) provides a proposal based on so called a good practice. It is intended for using by anyone with responsibility for business operations or the provision of services, from top management through all levels of the organization. It can be active on a single site, or with a global presence, ranging from a sole trader, through a small-to-medium enterprise (SME) to a big company employing thousands of people. It is therefore applicable to anybody who holds responsibility for any operation, and thus the continuity of that operation.
It outlines a holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause disruptions with related losses. Its purpose is to provide a framework for building organizational resilience and preparing an effective response of safeguards being important for key stakeholders, authorities, brand, reputation, and value-creating activities.
The BCM includes the recovery managing and/or the continuation of business activities in the situation of the business disruption, and an integrated management of the overall program through training, exercises, and reviews, to ensure the business continuity plan(s) stays current and up to date.
An objective of the recovery target time can be set for:

- resumption of product or service delivery after an incident, or resumption of given performance activity after an incident,
- recovery of the ICT (information and communication technology) system or computer application after an incident including a hacker attack, or an OT (operational technology) system failure or functional abnormality, including abnormal performance of the industrial automation and control system (IACS).

The recovery time objective should be lower than the maximum tolerable period of disruption.
The incident consequences may significantly vary and can be far-reaching to major accident with internal and external losses. These consequences might involve loss of life, environmental losses, and loss of assets or income due to the inability to deliver products and services on which the organization's strategy, reputation or even economic survival might depend.
In the context of Industry 4.0 companies, it is proposed to take into consideration following categories of potential disruption reasons:

- failures in logistics chains, delays in delivery of raw materials or semi-finished products by the business partners, and/or delays in providing services, spare parts etc.,
- physical or cyber attack,
- failures and outages of the ICT and CT (cloud technology) systems and networks designed using the wire and/or wireless technology,
- failures and outages of the OT systems and networks including production lines and storage, and/or malfunctions of the industrial automation and control system (IACS),
- extremal environmental phenomena, storm with lightings, heavy rain, local flooding,

flood, hurricane, or tornado, extremely high or low temperature, great snowfall, icing etc.,
- disturbances in the critical infrastructure objects and systems to deliver water, electricity, gas etc.,
- fire and/or explosion due to various reasons,
- extremal emission of pollutants and/or danger substances,
- destruction due to potential critical events in surroundings and infrastructure installations,
- failure to comply the product quality or safety requirements,
- failure to meet health or sanitary requirements, bad quality or pollution of products,
- cases of potential bacteria diseases (e.g., due to errors in the ventilation system maintenance and/or disinfection), or infectious virus leading to an epidemic or pandemic situation,
- earthquake, and/or tsunami at some sites close to the ocean shore,
- sabotage, terrorism, or cyberterrorism on the critical infrastructure objects/systems inspired by an external principal or agent.

In this chapter only some selected categories of potential disruption will be discussed.

2.3. Framework proposed for business continuity planning in Industry 4.0 companies

A BCM framework including business continuity plan (BCP) in an Industry 4.0 company is presented in Figure 2.

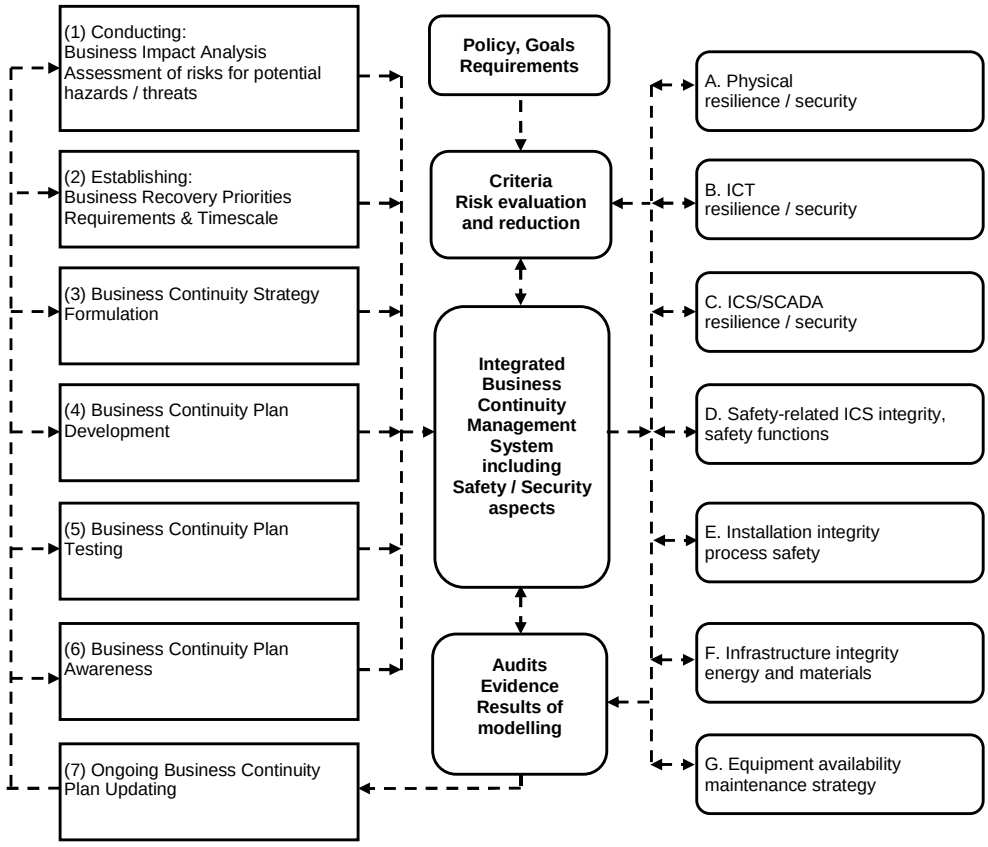

Figure 2. Proposed BCM framework for business continuity planning in Industry 4.0 company.

Left site of Figure 2 of this framework consists of specified discrete stages aimed at developing a comprehensive business continuity planning that will meet the company business requirements including the service providers. It will be useful in developing the recovery procedures (RP) for abnormal situations, failure events, or so-called disaster recovery plan (DRP) (ISO/IEC 24762, 2008) for cases of major disruptions and potential disasters.

Seven mentioned stages, adapted from the standard (ISO/IEC 24762, 2008), are as follows.

(1) Conducting the business impact analysis (BIA) and preliminary risk assessment regarding identified hazards / threats.
(2) Establishing business recovery priorities,

timescales for recovery, and related requirements.
(3) Business continuity strategy formulation (options for meeting priorities including technical and organizational aspects).
(4) Business continuity plan development (organization, responsibilities, logistics, and detailed action task lists).
(5) Business continuity plan testing (verification of the strategy and plan elaborated).
(6) Ensuring business continuity awareness (for all staff).
(7) Ongoing business continuity plan updating including maintenance activity.

In the middle part of Figure 2 some elements of an approach proposed are specified for integrated BCM that includes the dependability, safety, and security aspects. The management activities are based on domain knowledge, current information, evidence, and results of modelling in areas:

- formulating policy and goals for the domain including legal and regulatory requirements, relevant standards and appreciated publications on good industrial practice,
- criteria for the risk evaluation and reduction regarding the dependability, safety and security aspects including domain key performance indicators (KPIs),
- updated evidence, results of audits in the design and then plant operation, and results of modelling for supporting relevant decisions.

On the right site of Figure 2 seven areas are specified to be included in the process of business continuity planning for the Industry 4.0 plant that require considering relevant technical and organizational solutions in following areas.

A. Physical resilience and security of company resources and assets.
B. Information and communication technology (ICT) resilience and the security management in life cycle.
C. Industrial Automation and Control System (IACS) and Supervisory Control and Data Acquisition (SCADA) system to be adequately resilient and secure in specific industrial network of required security assurance level (SAL).
D. Safety-related control systems to be designed and operated according to functional safety concept with required safety integrity level (SIL).
E. Industrial installations and processes with required physical, integrity and functional protection measures.
F. Infrastructure integrity for delivery of raw materials and energy (electricity, gas, oil) needed for production processes.
G. Equipment reliability/availability to be adequately maintained according to strategy developed to achieve for instance a high level of overall equipment effectiveness (OEE).

Due to scope of the problems outlined above only selected issues will be discussed in this chapter. In following sections some fundamental aspects related to the Industry 4.0 concept are presented, namely the ICT systems and networks (B), the ICS/SCADA resilience and security (C), as well as the safety-related ICS (D) designed for implementing defined safety functions (IEC 61508, 2016) of required safety integrity level (SIL) to reduce relevant risks to be verified in the context its architecture and communications.

These systems and networks require special attention during the design and operation of the Industry 4.0 solutions due to their complexity, advanced functionality as well as required internal and external communications. Their architectural complexity and openness make them susceptible to malfunctions and failures, as well as venerable to external attacks. According to published data the probability of such attacks is relatively high in various industrial systems and networks of most European countries.

The importance of shaping the organizational culture, and related safety and security culture is also discussed, because it is a fundamental prerequisite of successful activities and avoiding failures in any organization and particularly modern industrial company to be actively present in a competitive market.

Expected outcomes of an effective BCM program implemented in the industrial company are as follows:

- key products and services are identified and protected to ensure required quality and effectiveness,
- an incident management capability is enabled to provide an effective response,
- the company understands its relationships with cooperating companies/organizations, relevant regulators and authorities, and the emergency services,

- staff are trained to respond effectively to an incident or disruption through appropriate training and exercising,
- stakeholders' requirements are understood and able to be delivered,
- staff receive adequate support and communications in a disruption event,
- the company's supply chain is better secured,
- the organization's reputation is protected and remains compliant with its legal and regulatory obligations.

3. Selected issues of BCM concerning ICT and safety-related ICS

3.1. OT and IT systems

A traditional reference model is based on the ISA99 series of standards derived from the generic model of ANSI/ISA–95.00.01 (Enterprise-Control System Integration). It represents a manufacturing system to be represented using five functional and logical levels as shown in Figure 3. These levels are often assigned to two technology classes: the Operational Technology (OT) and Information Technology (IT) with relevant security zones.

Level 3 (site manufacturing and control) includes the ICS/SCADA system with relevant Human-System Interface (HSI), and Manufacturing Execution System (MES). Level 4 (site business planning and logistics) comprises an Enterprise Resource Planning (ERP) system for managing and effectively coordinating the business and enterprise resources required for manufacturing processes. Level 5 (enterprise network) is designated for the business and logistics activities. It can be supported using some applications based on the Cloud Technology (CT) (Felser et al., 2019; Kosmowski et al., 2019).

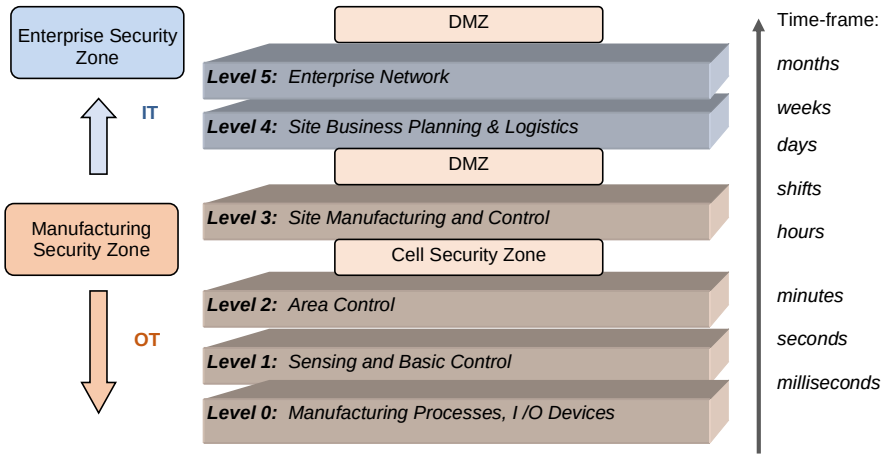

Figure 3. Traditional reference model of industrial system based on the ANSI/ISA95 standard.

In an open manufacturing system assigning the safety and security-related requirements require special attention of the designers and operators (Li et al., 2017; NIST SP 800–82r2, 2015). From the information security point of view an important requirement is to make segmentation of the complex industrial computer system and network distinguishing some cell security zones and to design the DeMilitarized Zone (DMZ) as it is illustrated, for instance, in Figure 3. The DMZ, sometimes referred to as a perimeter network or screened subnet, is a physical or logical subnetwork for controlling and securing internal data and services from an organization's external services using an untrusted, usually larger network, such as a corporate wide area network (WAN), an Internet network, and a cloud technology (CT).

Thus, the purpose of using DMZ is to add an additional layer of security to an organization's local area network (LAN). An external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled (IS, 2019; NIST SP 800–82r2, 2015).

A comprehensive list of internal and external influences, hazards and threats should be considered that are relevant during the operation of the OT and IT systems and networks. Basic features of these systems are presented in Figure 4.

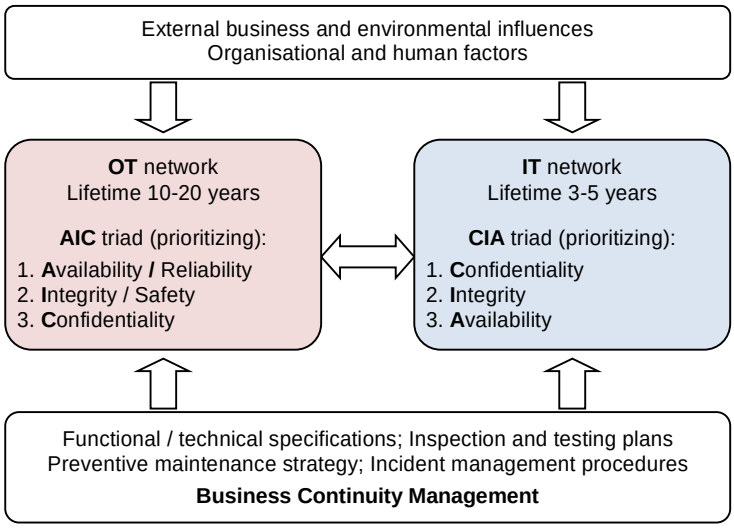

Figure 4. Basic features for characterizing the OT and IT systems and networks.

Expected lifetime of the OT system is often evaluated in the range of 10–20 years, but only 3–5 years in case of the IT (Kosmowski, 2021). For characterizing of the OT system an AIC triad (Availability, Integrity, and Confidentiality) is used to prioritize some basic requirements, and a CIA triad (Confidentiality, Integrity, and Availability) for the IT network.

The dependability, safety and security of the OT and IT systems are dependent on various external and internal influences, including the organizational and human factors (Kosmowski & Śliwiński, 2016). Traditionally, a general MTE (Man-Technology-Environment) approach have been used for systemic analyses and management of industrial installations in life cycle. An interesting framework for dealing with complex technical systems offers the systems engineering (SE), (SE, 2001).

The IT network and the OT system together with the industrial automation and control system (IACS) (IACS Security, 2020; IEC 62443, 2018) and safety-related ICS can be also considered as elements of a complex cyber physical system (Leitão et al., 2016).

Below a framework is proposed for dealing with integrated cyber security and functional safety analysis regarding mentioned above systems and networks in the BCM process. It is worth to mention that dealing with safety and security of the OT system in life cycle is quite challenging due to complex architectures of hardware and software used in practice from various equipment producers. It makes substantial difficulties in management of patching and maintaining high security, dependability, and safety of the OT system including its IACS (Belal, 2021).

3.2. Functional safety and cyber security of industrial control systems

For high dependability and safety of the OT system an operational strategy within BCM should be elaborated that includes inspections and periodical testing of the safety-related ICS, for instance as described in cases of the electrical / electronic / programmable electronic (E/E/PE) system (IEC 61508, 2016) or the safety instrumented system (SIS), (IEC 61511, 2016) with their sensors, logical component (e.g., PLC) and the equipment under control (EUC).

The operational equipment of manufacturing lines (machinery, drives, operational control systems etc.) require implementing an advanced preventive maintenance strategy (see the bottom right block in Figure 2) for achieving high as possible the OT availability and reducing risks of outages with related production losses. The incident management procedures must be developed for reducing risks of potential hazardous events with major losses.

A set of safety functions are to be implemented in the safety related ICS of required safety integrity level (SIL_r), determined in the risk assessment process in relation to the criteria specified (Kosmowski, 2020), to be assigned, for instance, to the E/E/PE system or SIS (see the OT block in Figure 5).

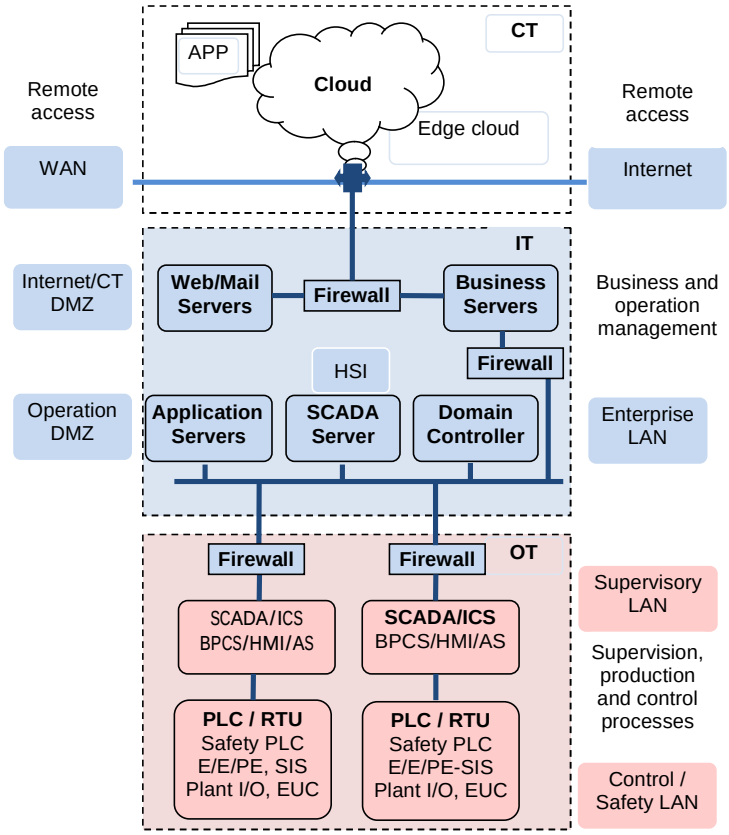

Figure 5. Typical ICT architecture including the IT and OT systems, and the SCADA/ICS.

Two different requirements should be specified to ensure appropriate level of functional safety (Holstein & Singer, 2010; Kosmowski, 2018):

- the requirements imposed on the performance of a safety function designed for the hazard identified,
- the safety integrity requirements, i.e., the probability that the safety function will be performed in a satisfactory way when potential hazardous situation occurs.

The safety integrity is defined as the probability that a safety-related system, such as the E/E/PE system or SIS, will satisfactorily perform defined safety function under all stated conditions within given time. For the safety-related ICS, in which defined safety function is implemented, two probabilistic criteria are defined as presented in Table 1 for four categories of the SIL (IEC 61508, 2016), namely:

- the average probability of failure on demand (PFD_{avg}) of the safety-related ICS in which the safety function considered is implemented, operating in a low demand mode (LDM), or
- the probability of a dangerous failure per hour (PFH) of the safety-related ICS operating in a high or continuous mode (HCM).

Table 1. Categories of SIL and probabilistic criteria to be assigned to the safety-related ICS that operates in LDM or HCM

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

The SIL requirements assigned for the safety-related ICS to be designed for implementing specified safety function stem from the results of the risk analysis and assessment to reduce sufficiently the risk of losses regarding specified risk criteria, namely for the individual risk and/or the group or societal risk (IEC 61508, 2016).

If the societal risk is of interest, the analyses can be generally oriented on three distinguished categories of losses, namely (IEC 61508, 2016), (IEC 61511, 2016): health (H), environment (E) or material (M) damage, and then the SIL required (SIL_r) for particular safety function, is determined as follows

$$SIL_r = \max\left(SIL_r^H, SIL_r^E, SIL_r^M\right) \quad (1)$$

As it was mentioned above, the SIL verification can be carried out for two operation modes, namely: LDM or HCM. The former is characteristic for the process industry (IEC 61511, 2016), and the latter is typical for the machinery (IEC 62061, 2005) or the railway transportation systems, and for monitoring and controlling in real time of an industrial hazardous installation or a critical infrastructure object using the ICS/SCADA system.

Typical hardware architecture of the E/E/PE system, shown in Figure 6, usually consists of three subsystems (Kosmowski, 2018): (A) sensors and input devices (transducers, converters etc.), (B) logic device (safety PLC or safety relay modules), and (C) actuators, i.e., the EUC or other output devices, for instance signalling or alarming device.

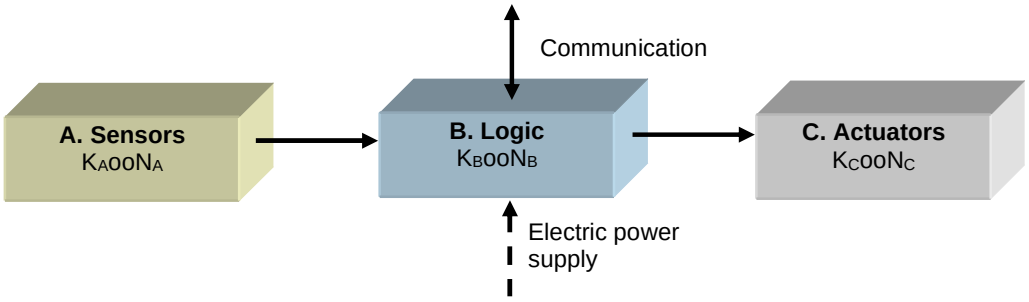

Figure 6. Typical architecture of the E/E/PE system or SIS for implementing safety functions.

Such safety-related system constitutes a specific architecture of hardware and software modules, and communication conduits. The logic device comprises typically a safety PLC with its input and output modules. The subsystems shown in Figure 6 can be generally of K out of N (KooN) configuration, for instance 1oo1, 1oo2 or 2oo3.
Their hardware fault tolerance (HFT) is understood as ability of the subsystem to perform a required function in the presence of faults or errors. The HFT (0, 1, 2) is an important parameter to be considered in the final SIL verification of given subsystem, together with known value of a safe failure fracture (S_{FF}) (Kosmowski, 2020) presented in Table 2.
From the industrial cybersecurity perspective, the systems, and networks within the business environment (see level 4 of ISA95 model shown in Figure 3) should be considered as potentially insecure because the IT contains the computer systems with relevant applications (see simplified architecture in Figure 5). For required functionality it uses the remote access paths and external communications.
Therefore, the IT and OT systems connected to the Internet and and/or a wide area network (WAN), or when the cloud technology (CT) is applied, should be secured at required security assurance level (SAL) to be assigned to respective zones (IEC 62443, 2018). It has been postulated to include the SAL level to be achieved in given domain for verifying the safety integrity level SIL of the safety-related ICS in which given safety function is implemented (Holstein & Singer, 2010; Kosmowski et al., 2019).

Table 2. Proposed correlation between SI^{Do} / SAL for evaluated domain and final SIL to be attributed to the safety-related ICS of a critical installation

Security indicator	SIL verified according to IEC 61508*			
SI^{Do} / SAL	1	2	3	4
$SI^{Do1} \in [1.0, 1.5)$ / SAL 1	SIL 1	SIL 1	SIL 1	SIL 1
$SI^{Do2} \in [1.5, 2.5)$ / SAL 2	SIL 1	SIL 2	SIL 2	SIL 2
$SI^{Do3} \in [2.5, 3.5)$ / SAL 3	SIL 1	SIL 2	SIL 3	SIL 3
$SI^{Do4} \in [3.5, 4.0]$ / SAL 4	SIL 1	SIL 2	SIL 3	SIL 4

* verification includes the architectural constrains regarding S_{FF} and HFT of subsystems

The security-related risks shall be mitigated through the combined efforts of component suppliers, the machinery manufacturer, the system integrator, and the machinery end user (IEC 62443, 2018; IACS Security, 2020). Generally, the responses to security risks should consider following steps (IEC 63074, 2017):

- eliminate the security risk by design (avoiding vulnerabilities),
- mitigate the security risk by risk reduction measures (limiting vulnerabilities),
- provide information about the residual security risk and the measures to be adapted by the user.

The standard IEC 62443 (IEC 62443, 2018) proposes an approach to deal systematically with the security-related issues of the IACS. Four security levels (SLs) are defined that are understood as a confidence measure that the IACS is free from vulnerabilities, and it will be functioning in an intended manner. These SLs are also suggested in the standard IEC 63074 (IEC 63074, 2017) to deal with security of the safety-related ICS to be designed for machinery in a manufacturing plant.
These levels (SL number from 1 to 4 as in Table 3) represent a qualitative information addressing relevant protection scope of the domain or zone considered against potential violations during the safety-related ICS operation, designed for given OT zone.

Table 3. Security levels and protection description of the IACS domain (IEC 62443, 2018; IEC 63074, 2017)

Security levels	Description
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Relevant SL number can be assigned to 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).

It has been suggested in the dependability and security-related evaluations to apply a defined vector consisting of relevant FRs from those specified above. Such vector can be generally defined for a zone, conduit, component, or system. This vector contains the integer numbers characterizing SL from 1 to 4 (or 0) to be assigned to relevant FRs.
A general format of the security assurance level (SAL) to be evaluated for given domain is defined as follows (IEC 62443, 2018):

SL-? ([FR,] domain)

= [IAC UC SI DC RDF TRE RA]. (2)

It makes significant problems in assigning SAL to the domain or zone as a single integer number from 1 to 4 (Holstein & Singer, 2010). To overcome this difficulty the security indicator SI^{Do} for the domain (Do) was defined (Kosmowski et al., 2019) for determined security levels SL_i in a set of relevant (Re) fundamental requirements (FR_i) with relevant weights w_i evaluated based on the opinions of ICT and ICS experts. This indicator is a real number from the interval [1.0, 4.0] to be calculated from the formula

$$SI^{Do} = \sum_{i \in \mathrm{Re}} w_i SL_i \ . \quad (3)$$

Four intervals of the domain security index SI^{Do} (from SI^{Do1} to SI^{Do4}) are proposed in first column of Table 2 for assigning the SAL category using the integer number from 1 to 4. Such approach corresponds with attributing SAL for the domain in some earlier publications, based on dominant SL_i for relevant fundamental requirements FR_i.
Three types of vectors describing SL_i for consecutive FR_i of the domain are distinguished (IEC 62443, 2018):

- SL-T (target SAL) – a desired level of security,
- SL-C (capability SAL) – the security level that device can provide when properly configured,
- SL-A (achieved SAL) – the actual level of security of a particular device / domain.

Proposed correlations between security index to be assigned to the domain SI^{Do} / SAL and final SIL attributing to the safety-related ICS in hazardous installation are presented in Table 2. It was assumed that SIL has been verified according to IEC 61508 requirements based on the results of

probabilistic modelling (Kosmowski, 2020), regarding common cause failures (CCFs) and human factors, and the architectural constrains for evaluated the safe failure fraction (S_{FF}) and the hardware fault tolerance (HFT) of consecutive subsystems (Kosmowski, 2018).

Thus, the verification of the SIL requires probabilistic modelling of the safety-related ICS of proposed architecture regarding S_{FF} and HFT of subsystems. In a case study (Kosmowski et al., 2019), the safety integrity level SIL 3 was obtained.

Considering the domain of the safety-related ICS in which the safety function was implemented including the communication conduits, the SL-A vector was evaluated as follows: [3 2 3 2 2 3 2]. Assuming that weights of all SL_i are equal (w_i = 1/7) and using the equation (3), the result obtained using the formula (3) is SI^{Do} = 2.43 and assigned security assurance level is SAL 2. Looking at the column 3 of Table 2 the final safety integrity level, validated regarding the security aspects in given domain is SIL 2, lower than required SIL 3. Therefore, improved security measures for the domain of interest should be proposed (Kosmowski et al., 2019).

3.3. Recommendations concerning ICS/SCADA and recovery of services

Below the information security management will be discussed in the context of BCM activities that require consideration of two aspects:

(A) Preventive activities to reduce the probability of failures leading to relatively short outages and minor losses, also due to potential not sophisticated cyber attacks of lower consequences.

(B) Recovery activities due to long lasting malfunction due to a major failure (including ICT infrastructure and relevant communication networks), or sophisticated cyber attacks with potential major consequences and losses.

As it was mentioned above three categories of losses, namely: health (H), environment (E) or material (M) damage are distinguished in the context of functional safety management.

Regarding aspect (A) some high-level recommendations have been proposed by ENISA (ENISA, 2016) to improve the resilience and security of the ICS/SCADA system as follows:

- include security as a main consideration during the design phase of ICS SCADA systems.
- identify and establish roles of human operators of the ICS/SCADA system,
- define network communication technologies and architecture with interoperability in mind,
- establish brainstorming and communication channels for different participants on lifecycle of the devices to determine needs and solutions,
- include the periodic/SCADA device updating and patching processes as part of the main operations of the systems,
- establish periodic ICS/SCADA security training and awareness campaign within the organization,
- promote increased collaboration amongst policy decision makers, manufacturers, and operators at the EU Level,
- define guidelines for the establishment of reliable and appropriate cybersecurity insurance requirements.

Insurance related issues are important due to the system complexity and significant uncertainties involved as discussed in the publication by Kosmowski & Gołębiewski (2019).

The aim of information security management (ISM) is to fulfill specified requirements concerning the triad CIA (confidentiality, integrity, and availability) of the ICT systems regarding the information storage and transfer, and related services. When an organization implements an ISMS (information security management system) the risks of interruptions to business activities for any reason should be identified and evaluated (Boehmer, 2009; Felser et al., 2019).

The BCM can be considered as an integral part of a holistic risk management that safeguards the interests of the organization's key stakeholders, reputation, brand, and value creating activities through (Gołębiewski & Kosmowski, 2017):

- identifying potential threats that might cause adverse impacts on an organization's business operations, and associated risks,
- providing a framework for building resilience for business operations,
- providing capabilities, facilities, processes, and elaborated action task lists, etc., for effective responses to disasters and failures.

Thus, in planning for business continuity, the fallback arrangements for information processing and communication facilities become beneficial

during periods of minor outages and is also essential for ensuring information and service availability during a major failure or disaster that require complete and effective recovery of activities over a period. Such fallback arrangements may include third-party support in the form of reciprocal agreements, or commercial subscription services (ISO/IEC 24762, 2008).

Regarding aspect (B) – the recovery activities, these are described in the standard ISO/IEC 24762 (2008) as the information and telecommunications technology disaster recovery (ICT DR) services. They should be based on formulated policies to enable the service providers to set the direction on related areas and services including clear communication to the relevant parties. A performance measurement should be determined that enables the service providers to review and improve their services and demonstrate that their services meet organization requirements.

A formal set of procedures should be established to deal with information security incidents and identified weaknesses, also physical. This should encompass (ISO/IEC 24762, 2008):

- detection of all information security incidents (and weaknesses), and related escalation procedures and channels,
- reporting and logging of all information security incidents (and weaknesses),
- logging the responses, and preventive and corrective action taken,
- periodic evaluation of all information security incidents (and weaknesses),
- learning from reviews of information security incidents (and weaknesses) and making improvements to security and to the information security incident (and weakness) management scheme.

Service providers should ensure that all ICT systems essential for disaster recovery are tested regularly to ensure their continuing capability to support DR plans. Tests should also be conducted when there are any significant changes in organization requirements and/or changes in service provider capacity and capability that affect services to organizations. Examples of such changes include relocation of DR sites, major upgrades of ICT systems or new ICT systems commissioned.

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are two of the most important parameters of a disaster recovery or data protection plan. The RPO & RTO, along with a business impact analysis, provides the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan of the BCM in relation do discussed above standards (BS 25999–1, 2006; ISO/DIS 22301, 2019)).

Another important indicator is the Real-Time Recovery (RTR) understood as the ability to recover a piece of IT infrastructure, such as a server, from an infrastructure failure or human-induced error in a time frame that has minimal impact on business operations. The RTR is used in a new market segment in the backup, recovery and disaster recovery market that addresses the companies that have historically faced with regards to protecting, and more importantly, recovering their data (ISO/IEC 24762, 2008; ISO 22400, 2014).

An important issue concerns personnel restriction and segregation. Service providers should establish a means to identify and segregate different personnel at their recovery facilities from access to the ICT systems and information, based on the need, to ensure that:

- there are restrictions on physical access to facilities housing ICT systems; for instance, ICT systems with different protection requirements should be in separate buildings or areas/rooms to enable physical access control to be properly implemented,
- work areas used by service provider, organization and vendor personnel are planned and designed with information privacy and confidentiality as a prime consideration, e.g., with buildings and/or assigned separate areas/rooms for use by different personnel.

Service providers and organizations should also ensure that the types of training to be provided to staff are commensurate with their assigned tasks and responsibilities. The types of training include:

- introduction training, to provide basic understanding and awareness,
- advanced level training, to equip staff with specific knowledge and skills to undertake assignments,
- continuous training, to keep staff up-to-date and ensure that they remain competent in performing their assigned tasks,
- training to assess and maintain the competency and readiness of staff.

The choice of types and numbers of performance measurements depends on the requirements of organizations.

In the process of identifying performance metrics, ICT DR service providers can consider the following types of indicators (ISO/IEC 24762, 2008):

- resource and operation readiness indicators: e.g., percentage of staff who have received ICT DR training and qualifications, percentage of equipment and facilities under regular maintenance,
- ICT DR plan maturity indicators: e.g., frequency of exercises, extent of exercises, percentage of ICT,
- systems tested perodically,
- exercise effectiveness indicators: e.g., exercise effectiveness to achieve pre-set business objectives,
- exercise effectiveness to meet SLAs,
- simultaneous disaster invocation risk indicators: e.g., subscription ratios for shared services,
- industry best practice compliance indicators: e.g., number of internal or external audit findings, percentage of compliance to the standard.

In addition to undertaking the risk mitigation measures the property should be insured. ICT DR service providers, particularly outsourced service providers, should purchase insurance against loss or damage of equipment and storage media, which could be caused by theft, fire, water pipe burst, failure of environmental control equipment, and computer abuse by staff.

Some insurance related aspects and proposed key performance indicators (KPIs) to be evaluated in the management process of hazardous industrial plants are discussed in publications (Gołębiewski & Kosmowski, 2017; Kosmowski & Gołębiewski, 2019).

3.4. Safety-related ICS testing, maintenance and recovery

Management of the OT system and IACS in lifecycle is especially challenging in industrial practice to achieve specified requirements concerning the AIC triad (availability, integrity, confidentiality) due to various reasons, because these systems contribute significantly to the realization of required quality and quantity of products in time and influence the overall equipment effectiveness (OEE). High equipment availability is to be achieved thanks to a proactive preventive maintenance strategy developed for using in industrial practice within the BCM system (see block G in Figure 3).

An important objective is also to ensure the required safety integrity using appropriate functional safety solutions within the safety-related ICS (see block D in Figure 3). The safety-related industrial control systems, like the E/E/PE systems or SISs, are designed using redundant architecture when required to reduce sufficiently the risk. They include the sensors and the equipment under control (EUC) that are periodically tested and undergo of preventive maintenance in life cycle.

Thus, an important objective is to formulate requirements, as well as to develop and implement in practice appropriate technical and organizational solutions necessary for safe and effective overall operation regarding preventive maintenance and restore fully the safety functions implemented in given E/E/PE system or SIS. Relevant requirements and procedures should be provided to those responsible for the operation and maintenance of these systems (IEC 61508, 2016; IEC 61511, 2016).

Following items should be specified for implementing in industrial practice:

- the plan for operating and maintaining the E/E/PE safety-related systems or SIS,
- the operation, maintenance, and repair procedures for these systems in life cycle.

Implementation of these items shall include initiation of the following actions:

- the implementation of procedures,
- the following of maintenance schedules,
- maintaining relevant documentation,
- carrying out, periodically, the functional safety audits,
- documenting any modifications of hardware and software in the E/E/PE systems.

Thus, all modifications that have an impact on the functional safety of any E/E/PE safety-related system shall initiate a return to an appropriate phase of the overall, E/E/PE system or software safety lifecycles. All subsequent phases shall then be carried out in accordance with the procedures specified for the specific phases regarding the requirements in mentioned above standards.

For each phase of the overall functional safety lifecycles, a plan for the verification and validation should be established concurrently with the

development for consecutive phases. The verification plan shall document or refer to the criteria, techniques, tools to be used in the verification activities.

The verification shall be carried out according to a plan prepared. Selection of techniques and measures for verification, and the degree of independence for the verification activities, will depend upon some factors specified in related sector standards or general requirements and rules based on good engineering practice in given industrial sector. The factors could include, for example, size of project, degree of complexity, degree of novelty of design, and degree of novelty of technology.

Chronological documentation of operation, repair, and maintenance of the safety-related systems should be maintained and must include the following information:

- the results of functional safety audits and tests,
- documentation of the time and cause of demands on the E/E/PE safety-related systems (in actual operation), together with the performance of the E/E/PE safety-related systems when subject to those demands, and the faults found during routine testing and maintenance,
- documentation of modifications that have been made to the safety-related ICS including the equipment under control (EUC).

The requirements concerning a chronological documentation should be sufficiently detailed for specific context of the safety system operation.

3.5. OT and IACS management in life cycle

There are significant problems concerning the OT system and network security related to, inter alia, limitations in performing on-line software patching. The OT system and network has usually a lot of diversity in terms of the ICS systems that asset owner need to operate, such as sensors, DCS/BPCS, safety PLC, SIS, EUC, etc., often from various vendors. That is why an effective patch management is important to identify vulnerabilities and reduce the risk to an acceptable level before potential attackers find them (Belal, 2021). However, unlike in case of the IT system and network all missing patches (necessary due to security reasons) cannot be installed on specific OT assets. There are several reasons of this limitation including (Belal, 2021):

- ICS or operating system (OS) patches can not be implemented due to non-compatible hardware,
- ICS vendor did not approve the OS patches,
- the patches are not approved by asset owner, i.e., the patch crashed the OT assets while testing.

In such scenarios, either the patches cannot be installed, or they need to wait until the next installation shutdown. Therefore, the vulnerabilities will be present until the next shutdown or the modernization of the OT assets. These issues can deteriorate operation process in relation to the AIC requirements.

If for some reason, the patch can not be deployed, then other controls need to be applied to reduce the risk to a tolerable level. Such controls include, but are not limited to (Belal, 2021):

- disconnect the OT assets from business LAN or DMZ,
- restrict user's permission to the OT assets,
- apply whitelisting or application baselining to run the required services only and block other services.

It can be a substantial problem in companies using multiple versions of the control system software. Multiple ICS software versions complicate patching tasks because it is more difficult to understand if the vulnerable asset or software in present in the company. Due to such situation some organizations using the common vulnerability scoring system (CVSS) – in version 2 (NIST 7435, 2007) or version 3 – faced difficulties to realize if this vulnerability exists in any of their installations.

It is because of missing in depth OT inventory such as safety system software versions, OS details, safety system application versions, and ICS communication model details. Keeping one latest version of the IACS software across all plants will make the patching process smoother. In the publication (Belal, 2021) it is suggested to decide what to patch depending on the CVSS score. It seems to be justified to support relevant decisions with regard also the SIL of safety-related ICS and SAL of relevant domain as it was discussed above.

Below a holistic approach is outlined based on relevant parts of the IEC 62443 standard. This standard proposes an approach to the IACS security management activities that are distributed regarding sites and time in the processes of design, verification, and validation of the hardware (HW)

and software (SW). Figure 7 shows the actors involved and basic activities of the product supplier that is responsible to carry out successful CFAT, and the system integrator for successful CSAT, Key roles and responsibility of the service pro vider and asset owner should be stressed. All of them should follow guidelines specified in relevant parts of IEC 62443 as shown in Figure 7.

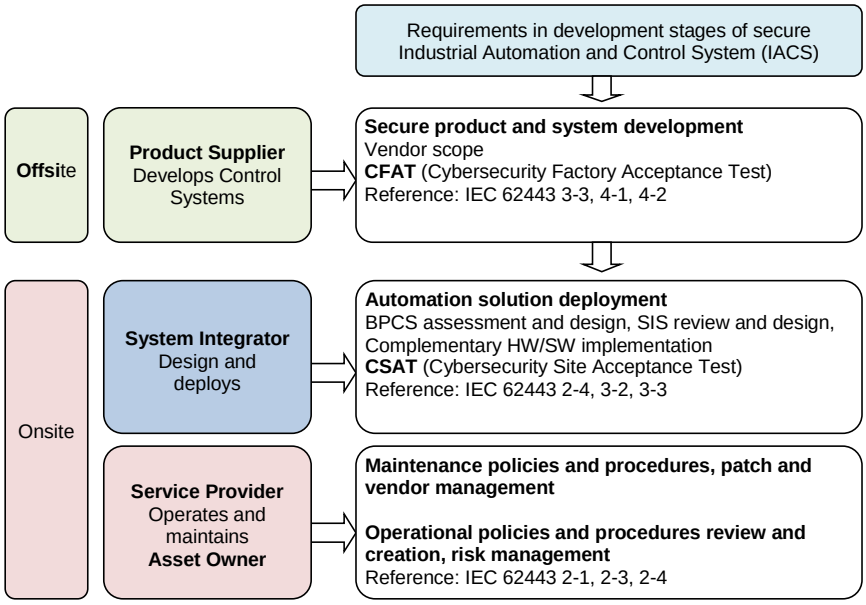

Figure 7. Holistic approach to the IACS security management in life cycle, based on (IEC 62443; IEC 62443, 2018).

It should be emphasized that the security of the safety-related ICS shall depend strongly on scope and quality of the information security management system (ISMS) to continuously control, monitor, maintain and, wherever justified to increase the IT and OT security based on evaluations of relevant risks. As it is known the IEC 62443 standard concerns mainly the OT system and relevant IACS. In the process of security management of the IT systems other relevant standards are also to be used (ISO/IEC 15408, 2009), (ISO/IEC 27001, 2013) and (ISO/IEC 27005, 2018).

In integrated dependability, safety, and security management system of complex industrial plants the technical and organizational factors should be carefully evaluated. It is worth to mention that shaping organizational culture requires good leadership and awareness. Organizational culture in the company significantly affects the safety and security culture (Kosmowski & Śliwiński, 2016). Conscious shaping these cultures is necessary for successful implementing in industrial practice the proactive management systems that deals with the dependability, safety, and security aspects in an integrated way.

4. Towards integrated dependability, safety and security management in industrial companies

4.1. General framework for the business continuity management system

Four following steps have been distinguished in a holistic management system including BCM aspects based on evaluation of relevant risks (Kosmowski & Gołębiewski, 2019):

- identify hazards/threats to evaluate and rank risks,
- identify techniques and strategies to manage risks (reduction, retention, or transfer to insurance company) including business continuity aspects,
- develop and implement risk management strategy and define relevant processes within BCMS,
- monitor technical and organizational solutions, and effectiveness of processes within the BCMS.

Some risks may stem from the changes within the organization / industrial company in time. The im-

plementation of a proactive approach and innovative solution within the BCMS requires creative thinking in the context of leadership, policy, and goals, considering required assets, resources, personnel competences, and current organizational culture etc.

Significant uncertainties or new challenging situations can be encountered due to changes in environment, including disturbances on relevant markets, and those related to the legal and regulatory requirements. It requires a good leadership, advanced organizational structure, coordinated activities of competent specialists to establish and implement an integrated and effective BCMS. General framework for a process-based management system (Kosmowski & Gołębiewski, 2019) is illustrated in Figure 8.

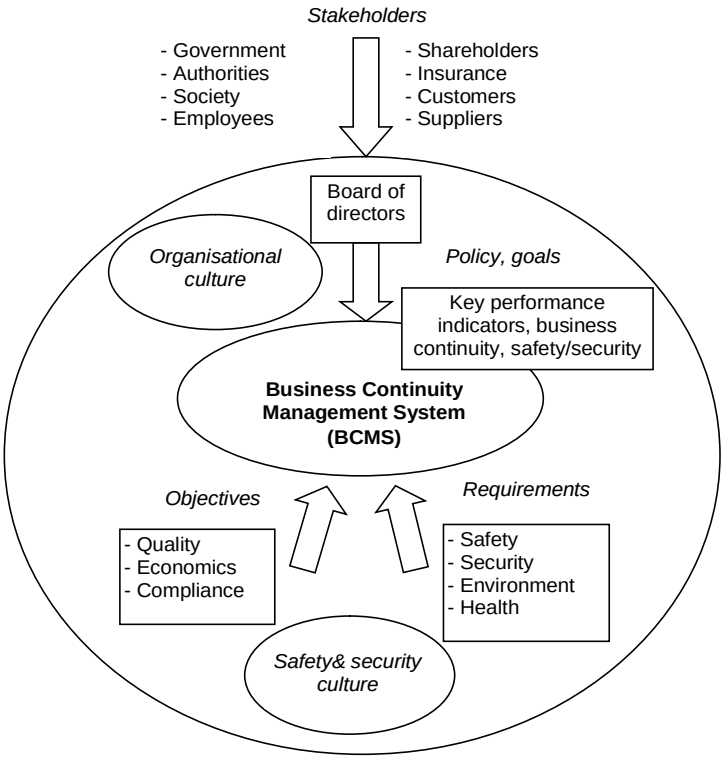

Figure 8. General framework for business continuity management system, based on (Kosmowski & Gołębiewski, 2019).

The BCMS concept is based on current trends in developing integrated management systems that include the quality and environmental aspects, as well as the dependability, safety, and security issues based on the risks evaluations in life cycle. All these aspects are important in the BCM in Industry 4.0 organizations / companies. A hierarchy of decisions, information flow, documents and activities within the process-based management system are presented in Figure 9. The strategic plans and decisions are undertaken at level 1 regarding opinions of interested stakeholders (Figure 8) and are to be transferred to lower levels of hierarchy: level 2 – coordinated processes, and level 3 – coordinated activities and documentation.

As it was mentioned audits are of a key importance in any management system, especially implemented in a hazardous industrial plant, to deal systematically with discrepancies detected. An audit documentation was prepared and used in industrial practice for a third-party audit in a refinery. It was directed towards the design and operation of safety-related ICS in relation to a set of criteria defined (Rogala & Kosmowski, 2012). The audit results with conclusions drawn were then discussed with the staff responsible for the functional safety to mitigate risks and improve specified technical and organizational solutions.

An important objective to implement the BCMS in hazardous plant is to satisfy expectations of stakeholders, specified in Figure 8, and an insurance company (Gołębiewski & Kosmowski, 2017) to assure a satisfactory level of business continuity, safety, and security. It can be achieved thanks to implementation in industrial practice an advanced and effective BCM system.

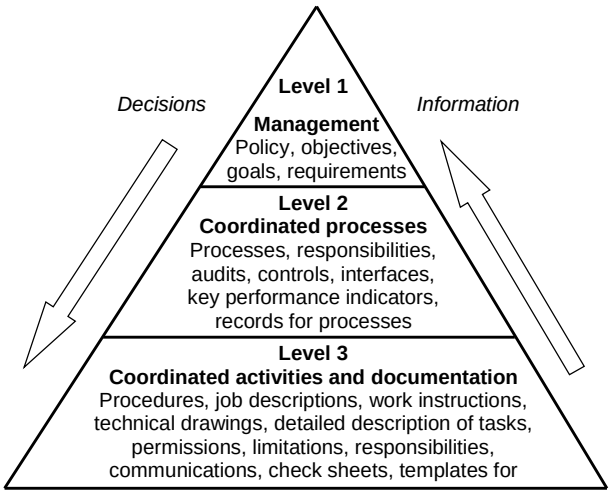

Figure 9. A hierarchy of decisions, information flow, documents, and activities in a management system.

Three categories of processes are to be distinguished in such BCMS for detailed elaborating in given hazardous plant (Kosmowski & Gołębiewski, 2019):

- executive processes,
- core processes, and
- support processes.

Some examples of these processes are as follows.

Executive Processes (EP)

- EP1 Managing the organization and business continuity,
- EP2 Managing the processes and procedures,
- EP3 Evaluating in time defined KPIs to support decision making,
- EP4 Coordinating external relations including stakeholders, etc.

Core Processes (CP)

- CP1 Monitoring operation of installations, equipment, and infrastructure,
- CP2 Scheduling services, tests and establishing maintenance programs,
- CP3 Monitoring environmental conditions, emissions, and effluents,
- CP4 Managing operation and assessing safety and vulnerability of installations, and site physical security,
- CP5 Managing IT security in the information and telecommunication technology (ICT) computer systems and networks,
- CP6 Managing OT security and functional safety of ICS, and cyber security of IACS, etc,

Support Processes (SP)

- SP1 Providing human resources and training,
- SP2 Providing personnel occupational health and safety services,
- SP3 Providing IT services and updating software and protection equipment,
- SP4 Providing procurement and contracting,
- SP5 Providing environmental and emergency services, etc.

As it can be seen some of these processes correspond to distinguished areas from A to G proposed in the BCM framework for business continuity planning in the Industry 4.0 company (Figure 2). For these processes, some specific procedures and instructions are to be elaborated according to specific technical and organizational solutions in given industrial company.

Several sets of the performance influencing characteristics that and key performance indicators (KPIs) are listed in publication (Kosmowski & Gołębiewski, 2019) for using in evaluations and audits within the BCMS of industrial plant to support relevant decisions, for instance.

Information and Communication Technology (ICT)

- ICT computers, digital systems, and networks, communication channels and DMZ solutions, encryption issues, performance indicators, records of disturbances, failures, repairs, recoveries and preventive maintenance, availability indicators for specified periods, patching, etc.

Information Technology (IT)

- protections for information storage and transfer, protocols in communication channels and DMZ solutions, vulnerability evaluation (CVSS), VPN, firewalls, encryption issues, access limitation to interfaces, performance characteristics, security incidents, hardware and software problems and recovery, records of

malfunctions/failures or cyber attacks, quality of procedures for abnormalities and failures, procedures for the system recovery, patching, etc.

Operational Technology (OT) and ICS/SCADA

- OT architecture and DCS/SCADA, communication channels and protocols used, hardware and software diversity, vulnerability evaluation (CVSS), network segmentation, and DMZ solutions, quality of HSI interface and procedures, alarm system (AS) design, quality of procedures, operator training/retraining, procedures for the system recovery, patching strategy, etc.
- OT and safety-related ICS performance (BPCS in relation to the SIS safety functions), hardware and software architectures, vulnerability evaluation (CVSS), access to HMI interfaces, communication channels, electro-magnetic compatibility (EMC) of electrical/electronic devices, functional safety, and security solutions for defined criteria (PL/SIL, SAL), testing and calibrating intervals of components, records of failures, repairs, and preventive maintenance, quality of procedures, analyses of technical and organisational solutions to avoid common cause failures (CCF) and systematic hardware and/or software failures.

Thus, the proposed BCMS offers methodology for systemic and proactive approach. It specifies various interrelated process-based activities and procedures for identification of hazards and threats to evaluate relevant risks for the safety and security-related decision making in life cycle in changing conditions.

Proposed approach includes an idea of good engineering practice, relevant international standards and available reports published by appreciated institutions. Due to complexity involved, especially in larger companies, it requires creating and maintaining organizational culture in interested industrial company.

4.2. Awareness and shaping organizational culture

There are opinions encountered (Kosmowski & Śliwiński, 2016) that organizational culture is based on shared attitudes, beliefs, customs, and written and unwritten rules that have been developed over time and may be considered as valid. In some cases, it is also called as corporate culture being expressed as follows:

- the ways the organization conducts its business, treats its employees, customers, and the wider community,
- the extent to which freedom is allowed in decision making, developing new ideas, and personal expression,
- how power and information flow up and down through its hierarchy, and
- how employees are involved and committed towards collective objectives.

Undoubtedly, this culture affects the organization's productivity and performance, and provides guidelines on customer care and service, product quality and safety, attendance and punctuality, and concern for the environment.

According to some publications, listed in (Kosmowski & Śliwiński, 2016), organizational culture represents the collective values, beliefs, and principles of the staff and is a product of such factors as history, product, market, technology, strategy, type of employees, management style, national culture, and tradition. Culture includes the organization's vision, values, norms, systems, symbols, language, assumptions, beliefs, and habits.

There are opinions that organizational culture can be depicted using four dimensions as in the Denison's model (1990):

- mission – strategic direction and intent, goals and objectives and vision,
- adaptability – creating change, customer focus and organizational learning,
- involvement – empowerment, team orientation and capability development,
- consistency – core values, agreement, coordination, and integration.

Each of these general dimensions is to be further described by sub-dimensions. Denison's model allows to describe cultures broadly as externally or internally focused as well as flexible versus stable. The model has been typically used to diagnose cultural problems in organizations.

This model was considered as useful for the analysis of safety and security-related awareness and culture in hazardous industrial companies and was adopted in developing the audit document for the safety-related control systems regarding the technical and organizational influencing factors (Rogala & Kosmowski, 2012).

Creating and embedding the BCMS within an organization can be a difficult and lengthy process which might encounter some resistance that was not anticipated (BS 25999–1, 2006). An understanding of existing culture in the organization will assist in the development of an appropriate BCM program (Gołębiewski & Kosmowski, 2017). All staff should understand that BCM is a serious issue for the organization and that they have an important role to play in maintaining the delivery of products and services to their clients and customers on time at required quality.

Building, promoting, and embedding the BCM approach in industrial company ensures that it becomes a part of the organization's core values and support effective management in other areas. An organization with positively oriented BCM culture will be able (BS 25999–1, 2006):

- develop an advanced BCM program more efficiently,
- instill confidence in its stakeholders (especially the staff and customers) in its ability to handle efficiently business disruptions,
- increase its resilience over time by ensuring BCM implications are considered in decisions at all levels and
- minimize the likelihood and impact of disruptions.

Development of a BCM culture is supported by (BS 25999–1, 2006):

- leadership from the top management and senior personnel in the organization,
- assignment of responsibilities,
- awareness raising,
- training programs, and
- exercising plans elaborated.

The organization should create a program for identifying and delivering the BCM awareness requirements and evaluate its effectiveness. The BCM staff should make themselves aware of external BCM information. This may be done in conjunction with seeking guidance from emergency services, local authorities, and regulators (BS 25999–1, 2006).

Raising and maintaining awareness of BCM with all the organization's staff is important also for better understanding the safety and security issues in changing conditions. They should be convinced that this is a lasting initiative that has an ongoing support of the top management.

5. Conclusion

In this chapter a framework for the business continuity management (BCM) is outlined that enables to deal systematically with potential influences on the industrial plant's dependability, safety, and security due to various reasons. A special attention is paid to the ICT and ICT/SCADA systems that operate in the industrial computer systems and networks using wire and lately also wireless communication channels.

These issues are considered from a general perspective of BCM regarding the dependability and security of ICT and ICS/SCADA systems with relevant functions and architectures of the information technology (IT) and operational technology (OT) systems and networks (Kosmowski et al., 2019). These systems require effective convergence to obtain manufacturing functionality and better effectiveness in realization of advanced business-related processes in Industry 4.0 companies.

Potential problems are identified related to the OT security if this technology consists of devices (hardware and software) from several producers / suppliers. It can make substantial difficulties in pathing software in relevant computer systems. This issue requires special attention in designing, implementing, and maintaining the business continuity management system in the Industry 4.0 companies.

The dependability and security of safety-related industrial control systems (ICS) in which defined safety functions are implemented can be influenced both by technical and organizational factors. These aspects are related to the hardware (HW) and software (SW) quality and reliability, and relevant organizational factors. They require further research, especially in the context of the design and operation of high complexity hazardous industrial installations regarding the functional safety and cybersecurity aspects including the defense in depths (D-in-D) solutions.

Traditionally, the manufacturing installations include the information technology (IT) and the operational technology (OT). Lately, using the cloud technology (CT) is frequently of interest as an external network important for the business management and external communications in cooperating Industry 4.0 companies.

Advanced automation and control systems are also in dynamic development based, for instance,

on the open platform communication unified architecture (OPC UA) protocol for improved network scalability and implementing new AutomationML concepts (Kosmowski et al., 2019). These solutions enable advanced production flexibility and effectiveness.

However, some quality and security related problems have been lately identified that require further analyses and testing of proposed new hardware and software solutions for industrial computer systems and networks. There are similar problems in other domains, and therefore, the methodology of cyber physical system (CPS) becomes more attractive (Leitão et al., 2016) to deal with their potential vulnerability and shape effectively resilience to external attacks.

Industrial plants are characterized by the venture capital, production capacity, existing or emerging hazards and threats that influence various risks in changing environment. To deal systematically with such challenging and interrelated issues the business continuity management framework outlined in this chapter seems to be interesting not only for industrial companies, but also for the domain researchers and risk engineers of the insurance company (Kosmowski & Gołębiewski, 2019). Some insurers offer expertise during the design and operation of conceptually new industrial plants and manufacturing systems.

Acknowledgment

The chapter presents some results developed within the HAZARD project that received funding from the Interreg Baltic Sea Region Programme 2014-2020 under grant agreement No #R023, and research support of the Polish Safety and Reliability Association as organiser of the SSARS 2021 conference, as well as the Gdańsk University of Technology, Faculty of Electrical and Control Engineering, under statutory activity.

References

Belal, S.M. 2021. The Top 7 Operational technology patch management best practices. *ISA Global Cybersecurity Alliance*, https://gca.isa.org/blog/author/sayed-m-belal (accessed 7 May 2021).

Boehmer, W. 2009. Survivability and business continuity management system according to BS 25999. *Third International Conference on Emerging Security Information, Systems and Technologies* 1, 142–147.

BS 25999–1. 2006. *Business Continuity Management – Part 1*: *Code of Practice*. British Standard.

CISA. 2020. *Assessments: Cyber Resilience Review*, us-cert.gov/resources/assessments (accessed 10 Feb 2020).

ENISA. 2016. *Communication Network Dependencies for ICS/SCADA Systems*. European Union Agency for Network and Information Security.

Felser, M., Rentschler, M. & Kleinberg, O. 2019. Coexistence standardisation of operational technology and information technology. *Proceedings of the IEEE* 107(6).

Gołębiewski, D. & Kosmowski, K.T. 2017. Towards process-based management system for oil port infrastructure in context of insurance. *Journal of Polish Safety and Reliability Association* 8(1), 23–37.

Holstein, D.K. & Singer, B. 2010. Quantitative security measures for cyber & safety security assurance. *ISA Safety & Security Symposium*.

HSE. 2015. *Cyber Security for Industrial Automation and Control Systems, Health and Safety Executive (HSE) Interpretation of Current Standards on Industrial Communication Network and System Security, and Functional Safety*.

IACS Security. 2020. *Security of Industrial Automation and Control Systems, Quick Start Guide: An Overview of ISA/IEC 62443 Standards*. June 2020, www.isa.org/ISAGCA (accessed 7 May 2021).

IEC 61508. 2016. *Functional Safety of Electrical / Electronic/ Programmable Electronic Safety-Related Systems, Parts 1–7*. International Electrotechnical Commission, Geneva.

IEC 61511. 2016. *Functional Safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1–3*. International Electrotechnical Commission, Geneva.

IEC 62061. 2005. *Safety of machinery – Functional safety of safety-related electrical, electronic, and programmable electronic control systems*. International Electrotechnical Commission, Geneva.

IEC 63074. 2017. *Security aspects related to functional safety of safety-related control systems*. International Electrotechnical Commission, Geneva.

IEC 62443. 2018. *Security for industrial automation and control systems. Parts 1–14* (some parts in preparation). International Electrotechnical Commission, Geneva.

IS. 2019. *Industrial Security*. Siemens, siemens.com/industrial-security (accessed 7 May 2021).

ISO/DIS 22301. 2019. *Security and Resilience – Business Continuity Management Systems – Requirements.*

ISO 22400. 2014. *Automation Systems and Integration – Key Performance Indicators (KPIs) for Manufacturing Operations Management, Parts 1 and 2.*

ISO/IEC 15408. 2009. *Information Technology, Security Techniques – Evaluation Criteria for IT Security. Part 1–3.* Geneva.

ISO/IEC 24762. 2008. *Information Technology – Security Techniques – Guidelines for Information and Communications Technology Disaster Recovery Services.*

ISO/IEC 27001. 2013. *Information Technology – Security Techniques – Information Security Management Systems – Requirements.* Geneva.

ISO/IEC 27005. 2018. *Information Technology – Security Techniques – Information Security Risk Management.* Geneva.

Kosmowski, K.T. 2018. Safety integrity verification issues of the control systems for industrial power plants. *Advanced Solutions in Diagnostics and Fault Tolerant Control.* Springer Int. Publishing AG, 420–433.

Kosmowski, K.T. 2020. Systems engineering approach to functional safety and cyber security of industrial critical installations. K. Kołowrocki et al. (Eds.). *Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2020*. Gdynia Maritime University, Gdynia 135–151.

Kosmowski, K.T. 2021. Functional safety and cybersecurity analysis and management in smart manufacturing systems. *Handbook of Advanced Performability Engineering, Chapter 3.* Springer Nature, Switzerland AG.

Kosmowski, K.T. & Gołębiewski, D. 2019. Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 10(1) 99–126.

Kosmowski, K.T. & Śliwiński, M. 2016. Organizational culture as prerequisite of proactive safety and security management in critical infrastructure systems including hazardous plants and ports. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7(1) 133–145.

Kosmowski, K.T., Śliwiński, M. & Piesik, J. 2019. Integrated functional safety and cybersecurity analysis method for smart manufacturing systems. *TASK Quarterly* 23(2) 1–31.

Leitão P., Colombo, A.W. & Karnouskos, S. 2016. Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Computers in Industry* 81, 11–25.

Li, S.W., Murphy B., Clauer E., Loewen U., Neubert R. Bachmann G., Pai M. & Hankel M. 2017. *Architecture Alignment and Interoperability, An Industrial Internet Consortium and Platform Industry* 4.0, IIC: WHT:IN3:V1.0:PB:20171205.

MERgE. 2016. *Recommendations for Security and Safety Co-engineering*, Multi-Concerns Interactions System Engineering ITEA2 Project No. 11011.

Misra, K.B. (Ed.) 2021. *Handbook of Advanced Performability Engineering*. Springer Nature Switzerland AG.

NIST 7435. 2007. The common vulnerability scoring system (CVSS) and its applicability to federal agency systems. *NIST Interagency Report.*

NIST SP 800–82r2. 2015. *Guide to Industrial Control Systems (ICS) Security*.

Rogala, I. & Kosmowski, K.T. 2012. *Audit document concerning organizational and technical aspects of the safety-related control system design and operation at a refinery* (access restricted). Automatic Systems Engineering, Gdańsk and Gdańsk University of Technology.

SE. 2001. *Systems Engineering Fundamentals*. Defense Acquisition University Press, Fort Belvoir, Virginia 22060–5565.

SESAMO. 2014. *Integrated Design and Evaluation Methodology. Security and Safety Modelling*. Artemis JU Grant Agreement, No. 2295354.

Zawiła-Niedźwiecki, J. 2013. *Operational Risk Management in Assuring Organization Operational Continuity* (*in Polish*), edu–Libri.