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

Towards strategic resilience of process plants and critical infrastructure regarding functional safety and cybersecurity requirements

Keywords

resilience, business continuity management, industrial automation and control system, functional safety, cybersecurity, Industry 4.0, human factors, cognitive human reliability, organisational culture

Abstract

This chapter addresses selected issues of strategic resilience of Industry 4.0 process installations and critical infrastructure systems that are designed and operated using converged technologies OT/IT/CT (operational technology/information technology/cloud technology) for effective business management in changing and uncertain environment. Two kinds of strategic resilience are distinguished: (I) the resilience concerning business processes to be evaluated and supported applying in industrial practice, e.g., a methodology of business continuity management (BCM), and (II) the resilience related to the safety and security technologies. Selected issues of these two areas of the overall resilience are discussed in relation to current references and reports. In area (II) the resilience of industrial automation and control systems (IACS) is emphasized that includes the requirements imposed on solutions of the functional safety (FS) and cybersecurity (CS) to be designed according to the defence in depth (DinD) concept using defined protection layers (PL). Responsible tasks in abnormal and accident situations are executed by the human operators that make use of an alarm system (AS) and its interface within overall human system interface (HSI). The human error probability (HEP) for relevant human operator behaviour type is evaluated using a human cognitive reliability (HCR) model. It is concluded that the resilience engineering (RE) concept is useful, but additional research effort is needed to develop integrated approaches and tools for supporting real engineering and organisational issues of strategic resilience.

1. Introduction

An important issue in the Industry 4.0 companies (Kosmowski, 2021b) 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 (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).

This chapter addresses selected issues of strategic resilience of the process installations and critical infrastructure systems that are designed and operated using converged technologies OT/IT/CT (operational technology / information technology/cloud technology) for passable business management in changing and uncertain environment.

Two kinds of strategic resilience are distinguished: (I) the resilience concerning business processes to be evaluated and supported applying in industrial practice, e.g., a methodology of business continuity management (BCM), and (II) the resilience related to the safety and security technologies to be implemented.

Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2022.

DOI: 10.26408/srsp-2022-08.

Selected issues of these two areas of the overall resilience are discussed in relation to current references and reports.

In area (II) the resilience of industrial automation and control systems (IACS) is emphasized that includes the requirements imposed on solutions of the functional safety (FS) and cybersecurity (CS) to be designed according to the defence in depth (DinD) concept using relevant protection layers (PL).

Responsible tasks in abnormal and accident situations execute the human operators that make use of an alarm system (AS) and its interface within overall human system interface (HSI). The human error probability (HEP) for relevant human operator behaviour type is evaluated using the human cognitive reliability (HCR) model. Mentioned above systems and computer 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 (Leitão et al., 2016). Several research projects have been undertaken concerning integrated analyses and modelling of the ICS safety and security (MERgE, 2016; SESAMO, 2014). This chapter concerns selected issues of the systemic resilience concept and, in particular, the resilience engineering (RE).

Resilience is defined generally as the ability of a system to succeed under varying and adverse conditions. Specifically, resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions (Dekker et al., 2008).

Some resilience engineering (RE) concepts and precepts were proposed by authors of a pioneering publication (Hollnagel et al. 2006). They help in developing innovative methods and tools for both the system developers and people responsible for the maintenance and management of system safety, in a number of industries. An interesting integrative review of fundamental concepts and directions of the resilience engineering for future research in safety management can be found in another publication (Pillay, 2017).

In a recent publication (McKinsey, 2022a) an idea of a new approach is outlined to move efforts from the risk management to shaping a strategic organisational resilience. It is a more comprehensive concept to deal with changing environment and decision making under uncertainties. It also concerns the cybersecurity trends that require looking over the horizon (McKinsey, 2022b).

The organisational culture is a prerequisite of the safety culture and obviously also security culture to be shaped in time (Kosmowski & Śliwiński, 2016). It is important for proactive risk management in a dynamic society (Rasmussen & Svedung, 2000), especially in uncertain business conditions and changing environment.

The holistic approach for building resilience advances in an organization is needed, to change from a narrow focus on risk, controls, governance, and reporting to a longer-term strategic view of a more complete environment. An important aspect of a holistic approach involves using crisis scenarios to test for resilience in an economic downturn as it is discussed in relation to the business continuity management (BCM) models (ISO/DIS 22301, 2019, Kosmowski, 2021b).

Nowadays, shaping the cyber resilience requires special attention due to many emerging threats and possible intentional attacks of relatively high frequency (WEF, 2019). It is a significant challenge because hackers are using advanced methods and tools of artificial intelligence (AI), machine learning, and other technologies to launch increasingly sophisticated attacks on industrial installations in many countries (WEF, 2022).

This chapter is structured as follows. In Section 2 some concepts of resilience are described that support idea of strategic resilience. Section 3 describes concept of technological resilience including the OT/IT/CT technologies, functional resilience, and cyber resilience in relation to the functional safety and cyber security requirements. Section 4 outlines issues of human factors, resilience engineering and cognitive resilience engineering. Cognitive aspects in human reliability analysis (HRA) are also discussed. In final part of this chapter selected issues of shaping the safety and security culture for higher resilience of industrial plants in current complicated international situation are emphasized.

2. Towards strategic resilience

2.1. Organisational resilience in changing environment

As defined in an international standard (ISO, 22316), *organizational resilience* is the ability of an organization to absorb and/or adapt in a changing environment to enable it to deliver its objectives and to survive (in relevant time horizon to prosper on competitive markets).

More resilient organizations can anticipate and respond to hazards, threats, and opportunities, arising from sudden or gradual changes in their internal and external context including business environment. Enhancing the resilience can be a strategic organizational goal and an outcome of good business practice to effectively manage resources and mitigate risks evaluated periodically.

An organization's resilience is influenced by a unique interaction and combination of strategic and operational factors. The organization can be relatively more or less resilient. Opinions are expressed that there is no absolute measure or definitive goal for resilience, but some key performance indicators (KPIs) can be useful in industrial practice for decision making as regards the reliability, safety, and security issues (Kosmowski & Gołębiewski, 2019).

Commitments undertaken to enhance gradually organizational resilience can contribute to (ISO, 22316):

- an improved ability to anticipate and address risks and vulnerabilities,
- increased coordination and integration of management disciplines to improve coherence and performance,
- a greater understanding of interested parties and potential dependencies that influence the strategic goals, and operational objectives.

Management is understood here as coordinated activities to direct and control an organization. The organizational culture includes collective beliefs, values, attitudes, and behaviour in an organization that contribute to the unique social and psychological environment in which it operates. They contribute to widely accepted precepts and help individuals to cope with new circumstances (Kosmowski & Śliwiński, 2016).

The organization should prioritize relevant resources for planned activities (ISO 22316, 2017):

- to articulate its vision, purpose, and core values to all interested parties to provide strategic direction, coherence, and clarity in all decision-making activities,
- to ensure that individual goals and objectives are aligned with and committed to the organization's purpose, vision, and values,
- to monitor and regularly review the suitability of the organization's strategies and their alignment with purpose, vision, core values and objectives,
- to recognize the need to reflect on and, if necessary, revise the organization's purpose, vision, and core values in response to external and internal changes,
- to seek out and promote new and innovative ideas to achieve and develop its strategic objectives.

Thus, the organization needs to understand its resilience capabilities and proactively develop a management system to plan activities to underpin strategic and operational capabilities.

2.2. Recent findings

Nowadays, due to existing and emerging new hazards and threats, there are increasing interests in developing holistic multidisciplinary approaches for evaluation and management of risks in changing environment. This issue gained recently substantial attention in some research institutions and industrial companies that have experienced considerable consequences of the COVID-19 pandemic (McKinsey, 2022a).

The survey undertaken drew responses from more than 200 senior executives and the risk and insurance professionals, reflecting a wide range of industry sectors in several countries. Interesting findings are discussed that include the results of research carried out by the Federation of European Risk Management Associations (FERMA) concerning a comprehensive survey of the pandemic's impact on corporate resilience.

The survey probed for views on the relevance for organizations, the capabilities for managing strategic resilience, and the importance of resilience in and across corporate functions, including strategy, operations, and associated risks.

The executives revealed that in the past, their risk management focus was on a small number of well-defined risks, primarily financial risks. They expressed opinions that now, the risks are encompassing the broader mandate of resiliency management. It is woven into long-term strategy development at top organizations, helping companies navigate in a far more dynamic operating environment (McKinsey, 2022a).

Among specific areas of resilience, companies have clearly focused on workplace safety and remote working in managing through the pandemic. More than 75% informed that implementation measures in these two areas are largely completed. About 52% of respondents said that for their organizations, the most effective capabilities are in place to manage financial resilience.

Executives also reported a room for improvement. Management of business operations and the supply chain emerged as weak points during the pandemic. Many companies have yet to fully implement new remedial measures. Senior executives state that risk is still mainly involved in crisis response.

To strengthen resilience in the future, most risk managers (75%) expressed opinions that the most important actions will be to improve risk culture and strengthen the integration of resilience in the strategy development process. Some important areas indicated include improved risk data aggregation and reporting as well as more advanced foresight capabilities. Executives also want to re-evaluate the risk governance approaches for better understanding factors influencing risks.

Thus, the challenge now is to move out a reactive approach in crisis response to a proactive one to integrate the risk evaluations with management functions on a more permanent basis. It becomes clear that the senior executives will tend to guide their organizations in transition from the crisis and risk management to the resilience management.

2.3. Towards holistic resilience strategy

Thus, needed now orientation should be proactive, based on a legal and business perspective. To build resilience regarding long-term strategic decision making, an organization need to develop certain cross-functional capabilities and strengthen resilience in identified strategic areas (McKinsey, 2022a).

The overarching capabilities include foresight skills and crisis response preparedness. To develop foresight capabilities, the organizations should gather and study relevant data, develop pertinent scenarios to discover gaps in resilience to anticipate and prepare for future potential crises. Then, appropriate crisis response capabilities can be effectively pursued:

- those that can be developed and implemented in advance,
- those to be applied quickly and effectively in case of abnormalities and disruptions.

The core resilience areas can be grouped as follows (McKinsey, 2022a):

A. *Financial resilience.* Institutions must balance short- and longer-term financial aims. A solid capital position and sufficient liquidity enable organizations to weather rapid drops in revenue, increased cost, or credit issues. Resilient companies can achieve superior margins by increasing revenue more than controlling costs.

B. *Operational resilience*. Organizations should maintain robust production capacity that can pivot to meet changes in demand or remain stable in the face of operational disruptions without sacrificing quality.

C. *Technological resilience.* Resilient firms invest in secure, and flexible infrastructure to manage cyberthreats and avoid technology breakdowns. They maintain and make use of high-quality data in ways that respect privacy and avoid biases, compliant with all regulatory requirements. It concerns the operational technology (OT), information technology (IT), and cloud technology (CT) to be functionally converged regarding the safety and security requirements (Kosmowski, 2021b).

D. *Organizational resilience*. Resilient firms should attract and develop talent in areas critical to their future growth; where many others fail, they find a way to secure sought-after people with scarce analytics or cybersecurity skills. Such organizations foster a diverse workforce where everyone feels included and can perform at their best.

E. *Reputational resilience.* Resilient institutions align values with actions and words. A wide range of stakeholders. employees, customers, regulators, investors, and society at large are holding firms accountable for their actions, brand promise, and stance on the environmental, social, and governance (ESG) issues.

F. *Business-model resilience*. Resilient organizations develop business models that can adapt to significant shifts in customer demand, the competitive landscape, technological changes, as well as the legal and regulatory terrains.

The holistic approach to building resilience advances in the organization, from a narrow focus on risk, controls, governance, and reporting to a longer-term strategic view of the total environment, is promising. An important issue of holistic approach involves using a crisis scenario to test for resilience in a downturn or outage, similarly as it is made applying the business continuity management (BCM) model (ISO/DIS 22301, 2019, Kosmowski, 2021b).

2.4. Leadership and organizational culture as prerequisites of safety and security culture

Traditionally, the organizational culture is considered in relation to the collective values, beliefs, and principles of the staff behaviour and is understood as a product of such factors as history, product, market, technology, strategy, type of employees, management style, national culture, and tradition. The term culture is related also to the organization's vision, norms, symbols, language, assumptions, beliefs, and habits.

Organizational resilience is enhanced by creative leadership that develops and encourages others to act under a range of conditions and circumstances, including periods of transients, uncertainty, and disruptions. The organization should demonstrate and enhance the following (ISO, 22316):

- effective leadership throughout the organization that encourages a culture supportive for resilience,
- leadership that can adapt to changing environment and operational circumstances,
- leadership that utilizes a diverse set of skills, knowledge, and behaviours within the organization to achieve organizational objectives.

The organization should prioritize and resource following activities (ISO, 22316):

- to develop trusted and respected leaders who act with integrity and are committed to a sustained focus on organizational resilience,
- to assign roles and responsibilities for enhancing organizational resilience,
- to encourage the creation and sharing of lessons learned about success and failure and promote the adoption of better practice,
- to empower all levels of the organization to make decisions that protect and enhance the resilience of the organization.

It will enable rational shaping the organizational culture with conscious involvement of humans in the context of personnel roles and competency for high awareness and more effective decision-making during accidents and disaster recovery activities in the context of organizational structure and staff responsibility assigned, as well as required co-operation with regulatory institutions and insurance company (Kosmowski et al., 2022)

The model proposed for shaping appropriate safety and security culture might include remarks on organisational culture and elements of four-dimensional Denison's model that includes following aspects:

(1) mission (strategic direction and intent, goals and objectives and vision),
(2) adaptability (creating change, requirements focus and organizational learning),
(3) involvement (empowerment, team orientation and capability development), and
(4) consistency (core values, agreement, coordination, and integration).

2.5. Organizational resilience and perceived future challenges by sectors

If one wants to find out more, how given organization can be compared against other organizations, then can complete the BSI Organizational Resilience Benchmark tool located at www.bsigroup.com/organizational-resilience.

The BSI Organizational Resilience Benchmark (ORB) tool is a relatively simple to complete questionnaire.

The shortened questionnaire focuses on the 16 key elements that are vital for building and developing organizational resilience. The results help in perceiving organization's strengths and vulnerabilities compared to other organisations, those that participated in the survey.

The results obtained will allow to review how following four categories that include the 16 key elements (specified in parentheses below) can be compared against the overall benchmark results:

(1) leadership (leadership specifically, vision and purpose, reputational risk, financial management),
(2) people (culture, community engagement, awareness, training and testing, alignment),

(3) processes (governance and accountability, business continuity, supply chain, information / knowledge), and
(4) product (horizon scanning, innovation, adaptive capacity).

However, opinions are expressed that the ORB tool is too generic and do not cover some important specific factors typical for organisations / companies of different industrial sectors.

Some organizations, large, medium, and small, have already made the shift from continuity management to shaping resilience, adapting to an ever more uncertain world. Perceived future challenges with related uncertainty/risk are arranged from the highest (1) decreasingly to lowest (13) as follows (BSI, 2018):

1) risks from technological solutions applied and changes,
2) risk from government policies,
3) skills,
4) competition,
5) financial risks,
6) global economy,
7) leadership changes,
8) market adaptability,
9) environmental changes,
10) customer changes,
11) business development/marketing,
12) product safety/quality/system productivity,
13) reputation/trust.

Technological related uncertainty (number 1 above), fuelled by the rise of automation and artificial intelligence, is raising the challenge of how to adapt and realign the workforce to deliver the optimal human-machine partnership. Businesses in every sector, not just tech firms, are becoming increasingly data-driven, raising the threat of cyber attacks which pose both financial and reputational risks to most organizations. Selected issues related to the technological solutions in use and possible changes are discussed below.

3. Technological resilience including functional resilience and cyber resilience

3.1. Typical architecture of OT/IT/CT system

Below the role of the industrial automation and control systems (IACS) for the functional safety and cyber security is emphasized in context of converged technologies OT/IT/CT to be operated and managed in life cycle regarding general requirements of relevant international standards specified below. Some concepts for integrating functional safety and cyber security analyses with explanations are described in publications (Kanamaru, 2020; Kosmowski, 2013, 2020, 2021a; Kosmowski et al., 2019, 2022).

Typical ICT (information and communications tech) architecture consisting of OT/IT/CT systems and some elements of IACS is shown in Figure 1.

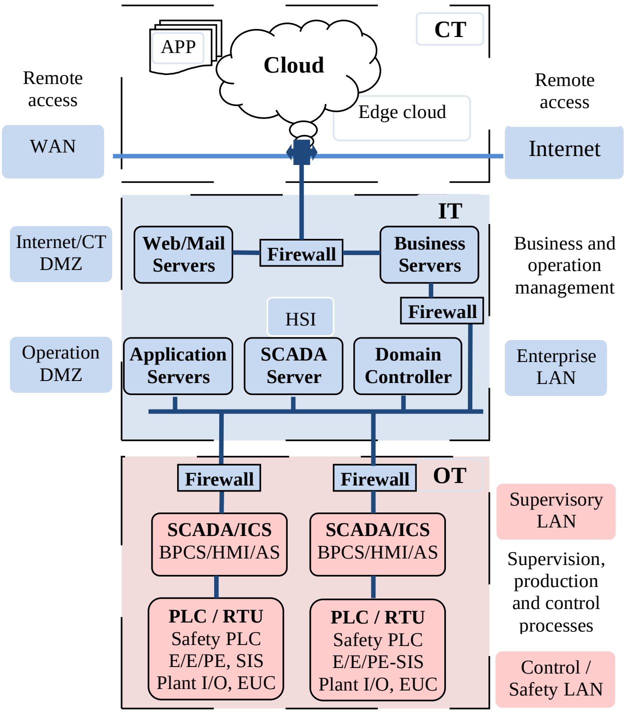

Figure 1. Typical ICT architecture consisting of OT/IT/CT systems and IACS.

At the bottom of OT area following elements and systems are located: control/safety local area network (LAN) input/output (I/O) elements, electrical / electronic / programmable electronic (E/E/PE) system, safety instrumented system (SIS), safety programmable logic controllers (PLC), basic process control system (BPCS), human machine interface (HMI), alarm system (AS), remote terminal units (RTU), supervisory control and data acquisition (SCADA) system.

At a higher system level, a human system interface (HSI) is distinguished that enables human operators to monitor and control various subsystems of OT. More details about such complex architecture including basic functional, safety and security requirements regarding selected international standards can be found in a publication (Kosmowski et al., 2019).

3.2. Functional resilience in relation to safety integrity levels

Functional safety concept and requirements are given in widely used in the process industry standards (IEC 61508, 2010; IEC 61511, 2016). The E/E/PE systems or SIS must be properly designed, with sufficient hardware fault tolerance (HFT) of subsystems, to perform successfully defined functions to ensure that relevant risks are reduced to fulfil specified criteria.

Allocation of requirements for defined safety functions and safety-related systems is illustrated in Figure 2. It starts with the hazard identification and the risk evaluation to determine required safety-integrity level (SIL) of the safety function (SF) to be implemented for the risk reduction. The risk acceptance criteria are to be defined for the individual risk or societal risk (IEC 61508, 2020, Kosmowski, 2013).

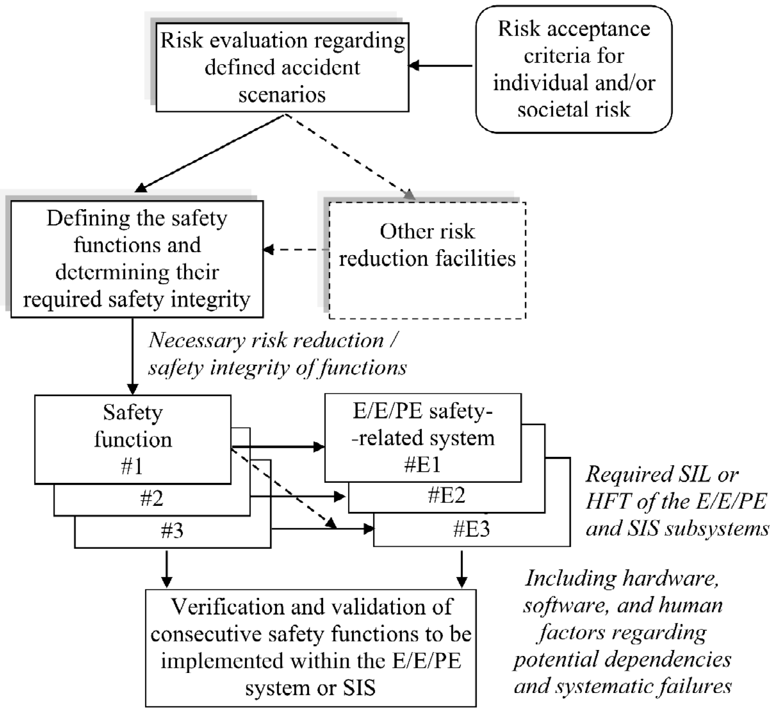
Risk evaluation regarding defined accident scenarios
Risk acceptance criteria for individual and/or societal risk
Defining the safety functions and determining their required safety integrity
Other risk reduction facilities
Necessary risk reduction / safety integrity of functions
Safety function #1
#2
#3
E/E/PE safety--related system #E1
#E2
#E3
Required SIL or HFT of the E/E/PE and SIS subsystems
Including hardware, software, and human factors regarding potential dependencies and systematic failures
Verification and validation of consecutive safety functions to be implemented within the E/E/PE system or SIS

Figure 2. Allocation of requirements for safety functions and safety-related systems.

If the societal risk is considered, the analyses can be generally oriented on three distinguished categories of losses, namely (IEC 61508, 2010; IEC 61511, 2016): health (H), environment (E) and/or material (M) damage, and then the safety integrity level required (SILr) for particular safety function, is determined as follows

$$\mathrm{SIL}_r = \max\,(\mathrm{SIL}_r^H, \mathrm{SIL}_r^E, \mathrm{SIL}_r^M) \qquad (1)$$

Consecutive safety functions are implemented in the safety related control system (SRCS), e.g., E/E/PE or SIS. The SIL to be achieved by designed SRCS of an architecture proposed is verified using appropriate probabilistic models (Kosmowski, 2013). The SRCS architecture (hardware and software) must be then verified as regards potential systematic failures and deteriorating contribution of human factors resulting in potential human errors of relevant types (Kosmowski, 2018). This issue is discussed in next subsection.

In some hazardous plants a single SRCS is not sufficient to reduce the risk as required and a more complex system must be designed according to a concept of defence in depths (DinD) using several protection layers. In Figure 3 typical protection layers in a process plant (IEC 61511, 2016; Kosmowski, 2013) are shown.

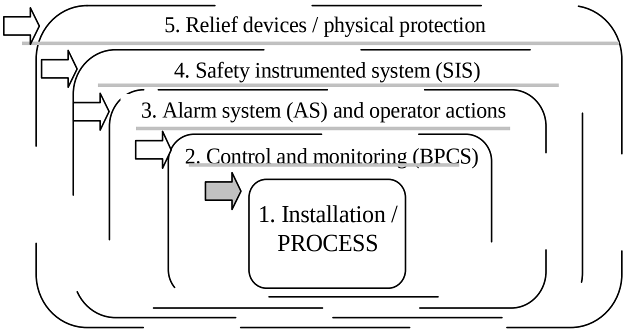
5. Relief devices / physical protection
4. Safety instrumented system (SIS)
3. Alarm system (AS) and operator actions
2. Control and monitoring (BPCS)
1. Installation / PROCESS

Figure 3. Typical protection layers in hazardous industrial installation.

The protection layers include: the basic process control system (BPCS), the alarm system (AS) and human-operator interactions, and the safety instrumented system (SIS). These protection layers should be physically and functionally independent, however, it is not always achievable in industrial practice.

They are denoted in Figure 4 respectively as:

- PL2 – basic process control system (BPCS),
- PL3 – operators supervising the process, installation and IACS who intervene when justified according to prescribed procedures and rules, using information from relevant interfaces, including the alarm system (AS),
- PL4 – safety instrumented system (SIS) performing an emergency shutdown (ESD) function when necessary.

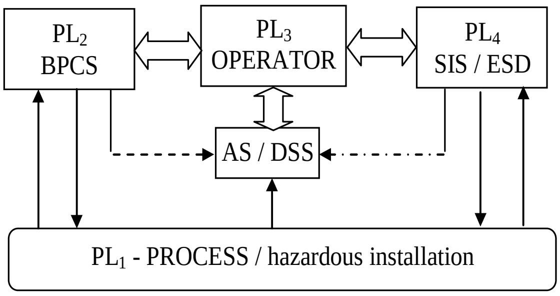

Figure 4. Human operator and alarm system (AS) as elements of the protection layers.

Required SIL of BPCS and SIS for given safety function is achieved using appropriate architectures of subsystems considering the probabilistic criteria (see Table 1) for verifying the SIL to be achieved by SIS (Kosmowski, 2013). The safety function can be also implemented in BPCS, but due to its complexity the safety integrity level achieved is usually not higher than SIL 1.

Table 1. Safety integrity levels and probabilistic criteria to be assigned to SRCS

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	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

A measure PFD_{avg} (probability of failure on demand average) is evaluated using probabilistic model of SRCS that operates in a low demand mode (LDM). A measure *PFH* (probability of danger failure per hour) is evaluated using another probabilistic model of SRCS that operates in a high or continuous mode (HCM). Examples of probabilistic modelling of such systems can be found in publications (Kosmowski, 2013; Kosmowski et al., 2022).

It is worth to mention that the functional safety evaluation framework concerning the hardware and software solutions of the SRCS, AS and safety related decision support system (DSS), with relevant interfaces within overall HIS, provide useful insights for contextual HRA human reliability analysis (Carey, 2001; Gersh et al., 2005; Kosmowski, 2018).

3.3. Cyber resilience in relation to the security levels

Cyber resilience is considered below in relation to the term of security of the industrial control systems (NIST SP 800-82r2, 2015). Cyber resilience means here a capability to reduce the occurrence and mitigate the effects of incidents arising from the disruption or impairment of the information technology (IT) and operational technology (OT) in technical systems that potentially can lead to dangerous situations and various losses (H, E, M) as explained above formula (1).

Vulnerability is defined as weakness in a system (hardware and software), system security procedures, internal controls, or implementation that could be exploited or triggered by a threat. Security is generally defined as a freedom from those conditions that can cause loss of assets with some unacceptable consequences (NIST 800-160v1, 2016; NIST 800-160v2, 2019).

Systems security engineering (SSE) is an engineering discipline of systems engineering (SE) that applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering specialties, and other contributing engineering specialties, to provide a fully integrated, system-level perspective of system security. Security requirement specifies the functional, assurance, and strength characteristics for a mechanism, system, or system element (see documents above).

The security-related risks shall be mitigated through a combined effort of the component suppliers, the machinery manufacturer, the system integrator, and the machinery end final user / the company owner (ENISA, 2016; IEC 62443, 2018; IACS Security, 2020). Generally, the responses to the security risks should be as follows (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 adopted by the user.

The IEC 62443 standard proposes an approach to deal systematically with the security-related issues of the IACS. Four security levels (SL) presented in Table 2 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.

Relevant *SL* number from 1 to 4 are to be assigned to consecutive seven foundational requirements (FRs) that are relevant in the domain analysed (IEC 62443, 2018):

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).

Thus, it is suggested in the dependability and security-related evaluations to apply a defined vector of relevant FRs from seven specified above. Such vector can be defined for a zone, conduit, component, or system. It contains in general the integer numbers characterizing SL from 1 to 4 (or 0 if not relevant) to be assigned to relevant FR (IEC 62443, 2018).

Table 2. Security levels to be assigned for IACS domains (IEC 63074, 2017; Kosmowski et al., 2019).

Security levels	Description
SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation
SL3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

A general format of the security assurance level (SAL) to be evaluated for a given domain is defined as a function of [FRs] (IEC 62443, 2018):

SAL(-X) ([FR,] domain)

$$= f\,[\text{IAC UC SI DC RDF TRE RA}] \qquad (2)$$

where*:* SAL(-X) security assurance level of an alternative format: SAL(-T) – target SAL, SAL(-A) – achieved SAL, and SAL(-C) = capabilities SAL to be assigned for given zone or domain.

Using formula (2) makes some problems in assigning SAL to the domain or zone of interest as an integer number from 1 to 4. To overcome this difficulty, a security indicator SI^{Do} for the domain (*Do*) was defined (Kosmowski et al., 2019) for assigning security levels SL_i for a set of relevant (Re) fundamental requirements (FRi) with appropriate weights w_i to be evaluated by experts. This indicator is a real number from the interval [1.0, 4.0] to be calculated from the following formula

$$SI^{Do} = \sum_{i \in \mathrm{Re}} w_i SL_i, \ \sum_i w_i = 1 \qquad (3)$$

Details of the method can be found in the publication (Kosmowski et al., 2022). In this section a macro criteria table is presented (Table 3) for final verifying of SIL achieved using defined safety function to be implemented in given SRCF in relation to the security indicator SI^{Do} achieved (or *SAL* known) for the domain of interest.

Table 3. Correlation between achieved SI^{Do}/*SAL* for domain and final SIL to be attributed to SRCS in safety critical installation.

Security indicator SI^{Do} / SAL	SIL verified according to IEC 61508*			
	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 constraints regarding S_{FF} and HFT of subsystems

Shaping strong resilience of the control systems in the context of OT/IT technologies described above will be successful only in companies of strong organizational culture that enable shaping safety and security culture and using the functional safety and cyber security solutions regarding appreciated in industrial practice approaches and standards. Security requirements for IT are specified in the international standards (ISO/IEC 27001, 2013; ISO/IEC 27005).

It is worth to mention that in probabilistic modelling of the SRCS including its redundant subsystems to verify SIL achieved, it is necessary to include potential influence of dependent failures, in particular potential common cause failure (CCF) using the β factor model. In evaluation of the β factor several influencing factors should be considered and scored on proposed scale (IEC 61508, 2010):

(1) separation / segregation,
(2) diversity / redundancy,
(3) complexity / design / application / maturity / experience,
(4) assessment / analysis and feedback of data,
(5) procedures / human interface,
(6) competence / training / safety culture,
(7) environmental control,
(8) environmental testing.

Factors of category (6) include competence, training, and safety culture. These issues will be discussed in next section in context of the human reliability analysis (HRA).

4. Human factors and resilience engineering

4.1. Human factors and systems cognitive engineering

The domain of systems engineering (SE, 2021) is traditionally focused on the technological aspects of the system design, such as hardware, software, including automation and control systems, while ignoring the fact that technical systems are designed and ultimately operated and maintained by humans to meet the mission or production goals.

The preliminary idea of resilience engineering (RE) can be found in some NASA reports dated on 2003 that tried to explain the influence of human factors on errors committed prior to and during accidents. Authors of publication (Holnagel et al., 2006) outlined interesting RE concepts and precepts.

Some researchers have expressed opinions, see publication (Pillay, 2017), that the RE and organisational resilience (OR) concepts could be inspirations for future research in area of reliability and safety management. Nowadays similar concepts are formulated known as cyber resilience (CR) for security management in complex computerized systems (WEF, 2019, McKinsey 2022b).

Resilience engineering definition is proposed (Pillay, 2017) as a sophisticated approach for managing organisational safety through the development of cognitive, behavioural, and cultural abilities to enable organisational members at all levels to actively anticipate, respond, monitor, and learn to operate close to the boundary of safe operations as part of normal work, by narrowing the gap between work as imagined and work as performed.

The goal of cognitive engineering (CE), or more generally cognitive systems engineering (CSE), is to develop advanced systems, training programs, and other products that support cognitive functions in decision-making, abnormal situation management, course-of-action selection, resource allocation and other information processing tasks (Bonaceto & Burns, 2005; Gersh et al., 2005).

The CE approaches are classified regarding their focus and application purpose. Following categories of the CE research areas are to be distinguished that concern the functional safety aspects (Kosmowski, 2018):

(1) analysis of system oriented human interactions,
(2) cognitive task analysis and identification of critical tasks,
(3) expected behavioural processes,
(4) cognitive processes required, and
(5) identification of erroneous diagnosis and following actions.

Each of these areas can be divided into several subareas. An approach outlined below is focused on area (5). Human diagnosis and following actions including potential errors are considered in the context of safety functions implemented using relevant systems: BPCS, AS, and/or SIS. Cognitive aspects of human operator behaviour are incorporated into the probabilistic model of system using Rasmussen's skill-rule-knowledge (SRK) framework (Rasmussen, 1983).

4.2. Human behaviour types

Some HRA methods are based on conceptual frameworks that include the human behaviour types or distinguished categories of human unsafe acts (Reason, 1990). Rasmussen (1983) proposes the distinction of three types of human behaviour. His appreciated conceptual framework assumes following cognitive levels of human behaviour:

- skill-based (S), highly practiced tasks that can be performed as more or less sub-conscious routines governed by stored patterns of behaviour,
- rule-based (R), performance of less familiar tasks in which a person follows some common-sense rules and previously developed procedures for given system, and
- knowledge-based (K), rough analysing a system state in more or less unknown situation when familiar patterns and rules cannot be applied directly, and actions that follow include information processing with the inclusion of diagnosis, planning, decision making, and actions directed towards reducing losses.

Figure 5 illustrates this concept that is useful in the analysis of human behaviour during abnormal situations or major accidents to identify potential human errors.

4.3. Cognitive aspects in human reliability analysis

Highly appreciated HRA method, developed for dealing with cognitive aspects in evaluating human error probability (*HEP*) for activity considered, is a HCR (human cognitive reliability), technique based on a model developed by Hannaman et al. (1984). *HEP* is treated in analysis as the probability of an event to be assigned within an event tree developed for defining potential accident scenarios (Kosmowski, 2018).

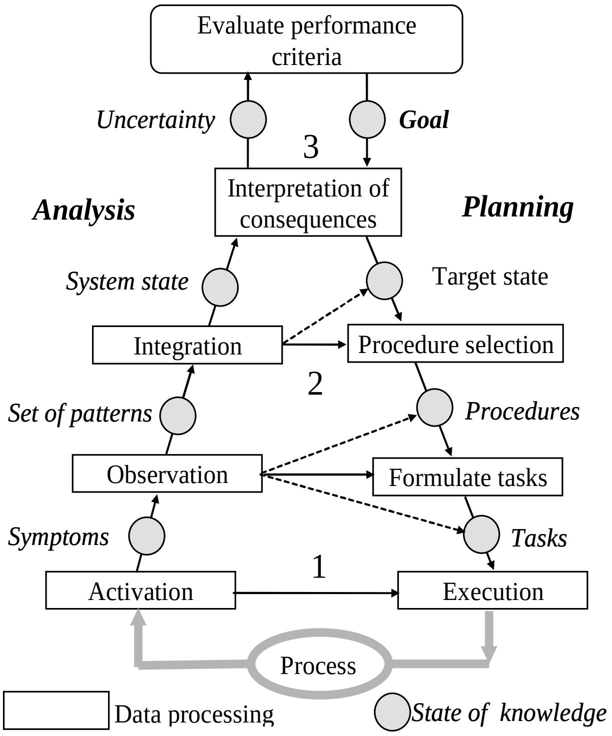

Figure 5. Information processing and actions undertaken by operators for human behaviour types (1 – skill, 2 – rules, 3 – knowledge).

Time-dependent *HEP* treated as an event of non-response in the situation considered, is calculated using the Weibull distribution from following formula (Hannaman et. al., 1984):

$$HEP^{X}(t) = \exp\left\{-\left[\frac{t/t_{0.5}-a}{c}\right]^{b}\right\} \tag{4}$$

where: *a, b, c* – are behaviour type coefficients specified below for behaviour type X (S, R, K) in given situation as explained below, and $t_{0.5}$ is the median value of time required to perform required task by a crew of human operators to be evaluated as follows

$$t_{0.5} = t_{0,5/nom}\prod_{i=1}^{3}(1+k_i) \qquad (5)$$

where:

k_1 – coefficient of operator experience: $k_1 = 0.22$ (expert, well-trained), $k_1 = 0$ (average knowledge training), or $k_1 = 0.44$ (novice, minimum training),

k_2 – coefficient of stress level: $k_2 = 0.44$ (situation of grave emergency), $k_2 = 0.28$ (situation of potential emergency), $k_2 = 0$ (normal activity, no emergency), or $k_2 = 0.28$ (low activity, low vigilance),

k_3 – coefficient for quality of operator/plant interface: $k_3 = – 0.22$ (excellent), $k_3 = 0$ (good), $k_3 = 0.44$ (fair), $k_3 = 0.78$ (poor), or $k_3 = 0.92$ (extremely poor).

The behaviour-type coefficients (*a*, *b*, *c*) in the formula (4) are to be evaluated as follows:

- (0.7, 1.2, 0.407) for skill-based behaviour (S),
- (0.6, 0.9, 0.601) for rule-based behaviour (R),
- (0.5, 0.8, 0.791) for knowledge-based (K).

If time window t_x allowable is relatively short for a dynamic process in an industrial installation during accident, then HEP^X evaluated according to formula (4) is high and can take in some cases a value of close to 1. It is in contrast with *HEP* = 0.1 being often suggested for assuming in many cases in the functional safety analysis according to the IEC 61511 standard (2016).

4.4. Human reliability analysis in context of accident scenarios

Human reliability analysis (HRA) methods are useful during the design and operation for assessing the contribution of potential human errors. These errors are treated as failure events in the logical and probabilistic model of given technical system, based on the accident scenarios identified and estimated human error probability (*HEP*) using relevant HRA method (Kosmowski, 2018).

Lately, it is emphasised that there is a need to develop for solving new engineering problems a next generation of HRA methods, such as described in previous subsection HCR method or CREAM (cognitive reliability and error analysis method) (Hollnagel, 1998). A cognitive basis for human reliability analysis is outlined in NUREG-2114 (Whaley et al., 2014).

Typical human errors in context of scenarios and their consequences are presented in Figure 6. HRA approaches are based on relevant task analysis technique (Embrey, 2000; Kirwan, 1994).

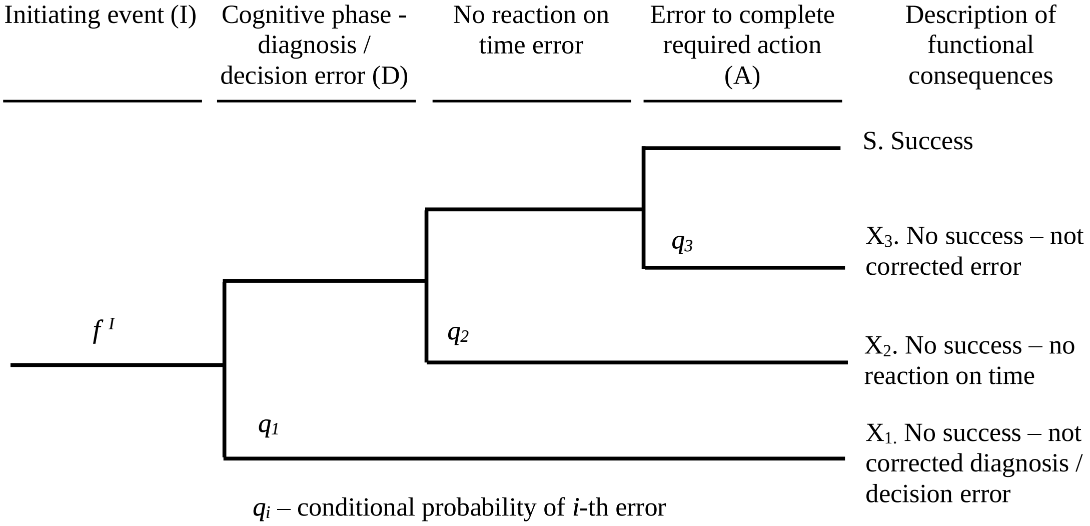
Initiating event (I)
Cognitive phase - diagnosis / decision error (D)
No reaction on time error
Error to complete required action (A)
Description of functional consequences
S. Success
X3. No success – not corrected error
X2. No success – no reaction on time
X1. No success – not corrected diagnosis / decision error
f I
q1
q2
q3
qi – conditional probability of i-th error

Figure 6. An event tree representing typical human errors and their consequences.

Till now mostly traditional, second generation HRA methods are used in PSA (probabilistic safety analysis) practice, such as a technique for human error rate prediction (THERP) (Swain & Guttmann, 1983), developed for the nuclear industry, applied also in various industrial sectors.

Other HRA methods, more often used in practice, are as follows: an accident sequence evaluation procedure (ASEP), a human error assessment and reduction technique (HEART), and a success likelihood index method (SLIM).

These HRA methods are characterized and evaluated in various papers, monographs, and reports (Adhikari et al., 2009; Bell & Holroyd, 2009). In a recent publication (IAEA, 2021) the role of human factors engineering in the control system design is emphasised.

Thus, different HRA methods can be applied for evaluating *HEP* regarding a set of *PSF*s, e.g., using a nonlinear relationship proposed in the SPAR-H (2005) method

$$HEP = \frac{NHEP \cdot PSF^{composite}}{NHEP(PSF^{composite} - 1) + 1} \qquad (6)$$

where: *NHEP* is a nominal *HEP*; the value of *NHEP* is suggested to be assumed as equal 0.01 for diagnosis (D), and 0.001 for action (A).

In the method SPAR-H eight performance shaping factors (PSF_i) are to be evaluated by the HRA analysts/experts:

(1) available time (for diagnosis and/or action),
(2) stressors,
(3) complexity,
(4) experience/training,
(5) procedures,
(6) ergonomics/HMI/HSI,
(7) fitness for duty, and
(8) work processes,

according to relevant tables developed for tasks of diagnosis (D) and/or action (A) in specified situations to be evaluated in given technical system.

4.5. Shaping safety and security culture for higher resilience of industrial plants

As it has been discussed in previous sections the organisational culture is a prerequisite of the safety culture and obviously also security culture to be shaped in life cycle (Kosmowski & Śliwiński, 2016). It is important for proactive risk management in a dynamic society (Rasmussen & Svedung, 2000), especially in uncertain business conditions and changing environment.

These cultures influence the human behaviour in performing various tasks at relevant levels of the organisation hierarchy and therefore are crucial for the organisational resilience of industrial plants and critical infrastructure systems (Rehak, 2020).

A management system concept has been developed consisting of defined processes of activity in given company (Kosmowski & Gołębiewski, 2019). They are based on relevant key performance indicators (KPIs) for an integrated dependability, safety, and security management in industrial company within a business continuity management (BCM) framework (ISO 22400, 2014; ISO/IEC 24762, 2008; Kosmowski, 2021b).

In such management system periodical audits are important to discover potential discrepancies in industrial company. An audit documentation was elaborated and has been used in industrial practice for a third-party audit in a refinery. The audit was directed for the design and operation phases of the safety-related ICS in relation to a set of criteria specified (Rogala & Kosmowski, 2012). The audit results with conclusions drawn were then discussed with the staff responsible for the dependability and functional safety to mitigate risks and improve relevant technical and organizational solutions.

Nowadays, shaping the cyber resilience requires special attention due to many emerging threats including intentional hacker attacks of relatively high frequency (WEF, 2019). It is a significant challenge because highly motivated hackers are using nowadays advanced methods and tools of artificial intelligence (AI), machine learning, and other technologies to launch increasingly sophisticated attacks on industrial installations in many countries (WEF, 2022).

5. Conclusion

In this chapter current issues that are on the road to strategic resilience of the process plants and critical infrastructure are considered regarding the functional safety and cybersecurity aspects based on selected publications and international standards specifying useful in industrial practice approaches, requirements, and criteria.

The resilience issue becomes crucial in the world of dynamic changes and substantial uncertainties involved. In such circumstances using traditional approaches for the dependability, safety and security related decision making, based mainly on statistical data and probabilistic models, are disputable. In such situation it rational, first of all, to shape resilience in the organisations and industrial companies considering carefully existing and emerging hazards and threats to propose countermeasures based on appropriate organisational and technological solutions.

As it was discussed the resilience can be defined generally as the ability of a system to succeed under varying and adverse conditions. Specifically, resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions.

The resilience engineering (RE) concepts and precepts published a pioneering work (Hollnagel et al. 2006) was an important step for further research to develop new methods and tools for both the system developers and specialists responsible for the maintenance and management of the system safety and security in a number of industries.

The next postulated step would be to concentrate on the cognitive resilience engineering (CRE) concepts and precepts for future implementation in practice because human factors are decisive for safety and security issues in socio-technical systems. An initial idea was outlined based to employ human cognitive reliability analysis methods such as HCR or CREAM to be combined with relevant techniques of cognitive task analysis.

The organisational culture is a prerequisite of the safety culture and obviously also security culture to be shaped in changing conditions. It is crucial for proactive risk management, especially in uncertain business conditions and changing environment. The holistic approach to building resilience advances the organization from a narrow focus on risk, controls, governance, and reporting to the longer-term strategic goals.

Nowadays, shaping the cyber resilience requires special attention due to many emerging threats including intentional attacks of relatively high frequency. It is a significant challenge because hackers are using at present advanced methods and tools of artificial intelligence (AI), machine learning, and other technologies to launch sophisticated attacks on industrial installations in many countries.

A process-based management system is proposed including periodic audits and multi-context evaluations using defined key performance indicators (KPIs). Such system will not be successful without a strong and creative leadership in given organisation/industrial company. It is obvious that a strong organisational resilience can not be reached without a high organisational culture that is a vital prerequisite of the safety and security culture to be created in a longer term in life cycle.

Some new methods and approaches should be conceptually developed to be directed towards integrating theoretical findings of the cognitive systems engineering (CSE), human factors engineering (HFE), cognitive reliability (CR), likely in a framework of cyber physical system (CPS). It requires further interdisciplinary research.

References

Adhikari, S. et al. 2009. *Human Reliability Analysis: A Review and Critique, Final report of the EPSRC funded project "Rethinking Human Reliability Analysis Methodologies"*. Manchester Business School Working Paper No 589.

Bonaceto, C., Burns, K. 2005. *Using Cognitive Engineering to Improve Systems Engineering*. MITRE Corporation, Bedford.

Bell, J., Holroyd, J. 2009. *Review of human reliability assessment methods*. Prepared by the Health and Safety Laboratory for the Health and Safety Executive.

BSI. 2018. *BSI Organizational Resilience Benchmark*. Report 2018.

Carey, M. 2001 *Proposed Framework for Addressing Human Factors in IEC 61508*. A study prepared by Amey VECTRA Ltd. for Health and Safety Executive (HSE), U.K. Research Report 373.

Dekker, S., Hollnagel, E., Woods, D. & Cook, R. 2008. *Resilience Engineering: New Directions for Measuring and Maintaining Safety in Complex Systems*. Lund University School of Aviation. Final Report.

Embrey, D. 2000. *Task Analysis Techniques*. Human Reliability Associates Ltd.

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

Gersh, J.R., McKneely, J.A., Remington, R.W. 2005. Cognitive engineering: understanding human interaction with complex systems. *John Hopkins Technical Digest* 26(4).

Hannaman, G.W., Spurgin, A.J. & Lukic, Y.D. 1984. Human cognitive reliability model for PRA analysis. Report NUS-4531, EPRI Project RP2170-3.

Hollnagel, E. 1998. Cognitive Reliability and Error Analysis Method. Elsevier Science Ltd.

Hollnagel, E., Woods, D., Leveson, N. 2006. *Resilience Engineering: Concepts and Precepts*. Aldershot. CRC Press, Taylor & Francis Ltd.

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 13 May 2022).

IAEA 2021. Human Factors Engineering Aspects of Instrumentation and Control System Design. Nuclear Energy Series No. NR-T-2.12.

IEC 61508. 2010. *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 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.

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

ISO 22316. 2017. *Security and resilience – Organizational resilience – Principles and attributes.* Geneva.

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

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

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.

Kanamaru, H. 2020. Requirements for IT/OT cooperation and in safe and secure IACS. *59th Annual Conference of Society of Instrument and Control Engineers of Japan,* 39–44.

Kirwan, B. 1994. *A Guide to Practical Human Reliability Assessment*. CRC Press, London.

Kosmowski, K.T. 2013. *Functional Safety and Reliability Analysis Methodology for Hazardous Industrial Plants*. Gdańsk University of Technology Publishers.

Kosmowski, K.T. 2018. Human factors and cognitive engineering in functional safety analysis. *Advanced Solutions in Diagnostics and Fault Tolerant Control*. Springer Int. Publishing AG, 434–448.

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. 2021a. 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. 2021b. Business continuity management framework for Industry 4.0 companies regarding dependability and security of ICT and ICS/SCADA system. K. Kołowrocki et al. (Eds.). *Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2021*. Gdynia Maritime University, Gdynia, 249–270.

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* 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* 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.

Kosmowski, K.T., Piesik, E., Piesik, J. & Śliwiński, M. 2022. Integrated functional safety and cybersecurity evaluation in a framework for the business continuity management. *Energies* 15, 3610–3631.

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.

McKinsey. 2022a. *From Risk Management to Strategic Resilience*. McKinsey & Company.

McKinsey. 2022b. *Cybersecurity Trends: Looking over the Horizon*. McKinsey & Company.

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

NIST SP 800-160v1. 2016. *Systems Security Engineering.* Vol.1: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.

NIST SP 800-160v2. 2019. *Systems Security Engineering.* Vol.2: A Systems Security Engineering Approach.

Pillay, M. 2017. Resilience engineering: an integrative review of fundamental concepts and directions for future research in safety management. *Open Journal of Safety Science and Technology* 7, 129–160.

Rasmussen, J. 1983. Skills, rules, knowledge; signals, signs and symbols and other distinctions on human performance models. *IEEE Transaction on Systems, Man and Cybernetics*, SMC-13/3.

Rasmussen, J., Svedung, I. 2000. *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, Karlstad.

Reason, J. 1990. *Human Error*. Cambridge University Press.

Rehak, D. 2020. Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic. *Safety Science* 123, 1–9.

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.

SPAR-H. 2005. *Human Reliability Analysis Method*. NUREG/CR-6883, INL/EXT-05-00509, US NRC.

Swain, A.D., Guttmann, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. NUREG/CR-1278. Washington: US NRC.

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

WEF. 2019. *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*. In collaboration with Boston Consulting Group. World Economic Forum, Cologny/Geneva, Switzerland.

Whaley, A.M., et al. 2016. *Cognitive Basis for Human Reliability Analysis*. NUREG-2114, US NRC.