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

Operational resilience regarding safety and security aspects of industrial automation and control systems

Keywords

resilience, sustainability, industrial automation and control system, functional safety, cybersecurity, business continuity management, human factors, organisational culture

Abstract

This chapter addresses selected issues concerning shaping resilience of the industrial automation and control systems (IACS). Such systems play nowadays a key role in safety and security of hazardous industrial installations and critical infrastructure networks due to a considerable attack surface. Productivity, safety, and security management is becoming now more and more challenging due to dynamic changes in business conditions, limited access to energy sources at accepted costs, adverse environment, pandemic consequences, difficulties in maintaining reliable and timely supply chains, etc. In situation of significant uncertainty and interrelated systems involved, a reasonable approach to achieve adopted goals is to elaborate a rational strategy of sustainable development to be combined with shaping resilience of relevant systems in life cycle. It concerns any organisation that governs for instance an industrial company and its manufacturing system, or a state institution responsible for critical infrastructure development. In this chapter shaping operational resilience of industrial control systems regarding basic functional safety and cybersecurity requirements is outlined.

1. Introduction

Shaping resilience of technical systems in context of sustainable development processes is becoming now more and more important due to dynamic changes in environment and deteriorating business conditions. In a publication by Kosmowski (Kosmowski, 2022) two main areas of strategic resilience shaping in industrial companies are distinguished: (I) the resilience of business processes that is evaluated and supported using a methodology of the business continuity management (BCM), and (II) the resilience of safety and security-related technologies to limit scale of potential losses and mitigate relevant risks. Some topics of these two areas have been discussed in that publication in relation to selected references including reports and standards. In area (II) shaping resilience of industrial automation and control systems (IACS) was emphasized including the requirements imposed on solutions of the functional safety (FS) and cybersecurity (CS) to be designed according to a defense in depth (DinD) concept in the context of defined protection layers.

The safety and security of IACS within the information communication technology (ICT), are often considered regarding converged systems including OT-IT-CT (operational technology-information technology-cloud technology). The IACS plays nowadays a key role in safety and security of distributed hazardous industrial installations and critical infrastructure networks due to a considerable hacker attack surface. Productivity, safety, and security management is becoming now more and more challenging due to dynamic changes in deteriorating business conditions, limited access to energy sources at accepted costs, adverse environment, pandemic consequences, difficulties in

Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2023.

DOI: 10.26408/srsp-2023-08.

maintaining reliable and timely supply chains, etc.
It becomes understandable that the analyses concerning strategic resilience, as outlined in a publication by Kosmowski (Kosmowski, 2022), including the operational resilience (OR) and technological resilience (TR) should be performed in context of sustainable development of given system considering dynamic changes of external conditions.
As regards the operational resilience, the industrial systems, including smart manufacturing systems, 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 of products.
To shape the technological resilience, the firms should invest in secure, and flexible infrastructure to effectively avoid consequences of cyberthreats and breakdowns causing losses. They should maintain and make use of high-quality data gathered, in a way that respect privacy and confidentiality to be compliant with company marketing strategy and regulatory requirements.
It concerns especially the ICT systems and networks that include converged operational technology (OT), information technology (IT), and cloud technology (CT), respecting the reliability, safety, and security requirements (Flaus, 2019; Kosmowski, 2021).
In this chapter the safety-related control systems, such as the E/E/PE (electric / electronic / programmable electronic) systems (IEC 61508, 2010) and SIS (safety instrumented systems) (IEC 61511, 2016) are of special interest as an important part of IACS.
The security-related issues of functional safety solutions, focused on the SIS in the oil and gas industry, including the cybersecurity aspects have been investigated by Grøtan et al. (Grøtan et al., 2020). It was an interesting attempt to integrate mentioned functional safety standards with a cybersecurity standard concerning the IACS (IEC 62443, 2018). Some other proposals in this research area have been published, for instance in the following publications (Kosmowski, 2020, 2021, 2022; Kosmowski et al., 2019, 2022).
The main objective of this chapter is to outline the approach to shape the operational resilience in sustainable development of the industrial systems in life cycle. This approach concentrates on the industrial automation and control systems regarding the design solutions of functional safety and cybersecurity.
The automation and control solutions used in the computer systems and networks significantly influence the reliability, functional safety, and cybersecurity of any technical system, particularly in Industry 4.0. New research challenges concern advanced solutions to be applied in Industry 5.0. They should include the technical and organizational aspects.
This chapter is organized as follows. In Section 2 some publications are reviewed concerning sustainability development, and the challenges in shaping resilience of industrial systems and critical infrastructure are discussed. Section 3 is devoted to the sustainable development and resilience issues presented in some reports, legal acts, and standards.
In Section 4 some conceptual frameworks for the operational resilience analysis of industrial systems are reviewed, including the internet of things (IoT) and the industrial internet of things (IIoT) in relation to the cyber physical systems (CPS) concept, and the ISA 95 model. The CPS framework including cognitive realm was indicated as interesting for the resilience analysis combined with hierarchical ISA 95 model. Two categories of human factors (A) and (B) are distinguished that potentially influence the resilience.
Section 5 describes an approach for the operational resilience analysis regarding functional safety and cybersecurity requirements in the risk criteria context. It includes determining and verifying of the safety integrity level (SIL) of defined safety functions and the security assurance level (SAL) of relevant domains. The issue of the alarm system integrity in context of human reliability analysis (HRA) and evaluation of the human error probability (HEP) is also discussed.
The final part of this chapter is devoted to the research challenges concerning resilience of the industrial automation and control systems. The chapter is ended with conclusions and proposals of research directions.

2. Challenges in shaping resilience of industrial systems and critical infrastructure

2.1. Resilience concepts and resilience engineering

In this Section selected publications are reviewed concerning the resilience concepts focused on issues of the reliability, safety, and security of industrial control systems. The relation of the oper-

ational resilience (OR) and business continuity management (BCM) is also discussed.

Interesting resilience engineering (RE) concepts and precepts were proposed by the authors of a pioneering publication (Hollnagel et al. 2006). Their first ideas have helped in developing innovative methods and tools for both the system developers and the staff responsible for the maintenance and management of system safety, in a number of industries. A review of fundamental concepts and directions of the resilience engineering useful for planning of future research concerning the safety management can be found in a publication (Pillay, 2017).

Riegel (Riegel, 2013) has dealt with resilient control systems and proposed some metrics useful for defining a mission impact. He explained that the resilience describes how the systems operate at an acceptable level of normalcy despite disturbances or threats. He also considered some cognitive aspects of the cyber-physical interdependencies inherent in critical infrastructure systems and explained how the resilience concept differs from the reliability in evaluation and mitigating risks.

He proposed following definition of a resilient control system: *A resilient control system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature*. The resilient control system (RCS) term was considered as a new control system design paradigm that encompasses issues of cybersecurity, physical security, economic efficiency, dynamic stability, and a process compliancy in complex systems.

In several publications some issues have been raised how to understand relations between the sustainable development and resilience in a governance process in life cycle. For instance, in a publication (Redman, 2014) the author asked a question *Should sustainability and resilience issues be combined or remain distinct pursuits?* He claims that it has become common for sustainability science and resilience theory to be treated as complementary approaches. Occasionally, the terms have been used even interchangeably.

However, it should be emphasized that although these two approaches share some working principles and objectives, they are based on distinct assumptions about the development and operation of systems and how to best guide these systems into the future.

Häring et al. (Häring et al., 2016) argue that a resilience engineering can substantially contribute to improving safety and security as well as the adaptive capabilities of complex socio-technical systems when they face adverse and potentially disruptive events. Those capabilities, which can be summarized as resilience, should be a key characteristic of sustainability. The authors add, citing several references, that in our modern world depending on complex, interdependent, coupled networks of infrastructure, sustainable development is only achievable, if we learn to design and optimize our systems in a resilient way.

They propose to define the resilience of such systems as their capability to successfully:

- prepare for,
- prevent,
- protect from,
- respond to, and
- recover from

minor up to larger, from creeping up to sudden, known up to completely unexampled disruptions. Such events should be considered in the societal and technical contexts.

Hickford et al. (Hickford et al., 2018) emphasize that resilience and emerging concept of resilience engineering that concerns especially the critical infrastructure systems are among the main inquiries of those managing complex systems. However, the disparate nature of resilience engineering development in various academic institutions and industrial companies has resulted in a diversity of definitions and characterizations.

This paper outlines some existing methodologies treated within implementation and monitoring of engineering resilience solutions. Current practices including existing approaches and metrics, and an insight into the opportunities and potential barriers associated with these methodologies and practices are also discussed.

The authors conclude that the field of resilience engineering, rather still in its infancy, presents significant opportunities to get things right, particularly in situations where coordinated planning and decision-making for infrastructure systems is becoming more common. They express opinion that further research works should be carried out to identify best-practices in infrastructure planning, design, operation, and governance. Methodological development is needed that includes defining metrics useful in practice for verification of implemented resilience solutions.

It is worth to mention that in the reviewed public-

cation as above (Häring et al., 2016), some issues of the resilience are discussed related to the business continuity management (BCM) concept regarding the influence of human factors in organizational and social context. Similar issues have been described in publications by Kosmowski (Kosmowski, 2022) and Kosmowski et al. (Kosmowski et al., 2022) that are focused on the information communication technology (ICT) and the industrial automation and control system (IACS). Below the operational resilience issue versus business continuity will be discussed.

2.2. Sustainable development and resilience

In a publication of the Word Economic Forum (WEF, 2019) it is emphasized that digitalization is driving growth and innovation in the electricity industry and has tremendous potential to deliver new values for shareholders, customers, and environment. However, new technologies and business models affecting the operating assets present both opportunities and risk. Cyber risk is considered often as the business risk. In the electricity industry, cyber risk is also an ecosystem-wide risk. Shaping cyber resilience is a challenge for all organizations, but it is of particular importance for the electricity ecosystem (WEF, 2019). Some questions for the board were specified in that publication:

- Are cyber risks and associated implications evaluated, embedded, and appropriately managed in all aspects of the business?
- Are cyber risk and associated risk management activities discussed and planned for when starting a new initiative?
- Does management ensure that appropriate technical controls (e.g., limited access controls, segmentation, and defense in depth) are in place and properly implemented?
- How does management communicate the cyber risks, the importance of organization and ecosystem-wide cyber resilience, and the relevant cyber risk management policies to all personnel?
- Are all personnel aware of how cyber resilience impacts their role within the organization? Is there cross-functional and cross-departmental ownership for cyber risk management?
- What mechanisms are in place to train personnel on cyber resilience and raise awareness about the need to embed cyber resilience in all aspects of the organization?
- How is the effectiveness of these mechanisms monitored and measured?

There are 10 cyber resilience principles proposed by the Forum (WEF, 2019) for General Board and 7 for Electricity Board. For instance, the principle EI1 (Cyber resilience governance) states that the electricity board requires management to implement comprehensive cybersecurity governance, which governs information technology (IT), operational technology (OT), physical security and digital transformation, to ensure interoperability within the organization and to drive alignment across the ecosystem.

Bouloiz (Bouloiz, 2020) argues that resilience, which is the ability to withstand shock and maintain critical function, has been recognized as an important approach to keep a firm operating in varying conditions, even if these conditions are excepted or not. With the objective to further enhancing the performance of companies and be a part of sustainable development, he suggests that it is necessary to study this performance through the resilience perspective to manage more effectively potential disturbances.

He proposes a resilience engineering model for including the principles of sustainable development to manage disruptive events and maintain a resilient performance. This model distinguishing three interrelated modes of resilience. Each resilience mode has a performance management function which, to be successful, requires the establishment of barriers called performance barriers that integrate the three components of sustainable development.

In the publication (Grøtan et al., 2020) a need was identified for additional measures for countering unexpected and surprising events from the complex security threats. The authors explore how the resilience concept can be the foundation for additional approaches and measures within elaborated earlier a functional safety methodology named *SecureSafety* (SeSa). They sketched out a scientific roadmap to advance on a path that in the end could reinforce the SeSa methodology with a trustworthy cyber resilience component in the context of converged OT-IT technologies and the safety-related control system architecture.

Kanamaru (Kanamaru, 2020) discusses the safety and security issues concerning the converged IT-OT systems and networks in context of functionality of the industrial automation control system

(IACS). He emphasized that the safety instrumented system (SIS), designed regarding requirements given in a standard IEC 61511 (IEC, 2016), has a critical role in protecting industrial plants.
The author of that paper suggests that the security-related aspects should be considered regarding the standard IEC TR 63069 (IEC, 2019). This standard proposes a framework for integrated functional safety and cybersecurity analysis. It should include, in addition, such aspect as the recovery planning, the converged IT-OT systems cooperation during an accident response. A very important issue is the influence analysis of human factors in context of the design of SCADA system, and security operations center (SOC). Also, a system for the security information and event management (SIEM) should be considered and organizational aspects of a team of maintainers.
He concludes that the most effective counter measure to control damage of attack is to quickly restore industrial plants and social infrastructure services from a down state. For this purpose, SOC, the operator, and the maintainer should work quickly to investigate the cause of abnormality, and then to plan recovery, and reset devices by utilizing IT-OT cooperation functions.
It is worth to mention that such activities are typical in the business continuity management (BCM) framework to be developed for given industrial plant (Kosmowski et al., 2022).

2.3. Current issues of resilience research concerning interrelated systems

Cantelmi et al. (Cantelmi et al., 2021) provided a synthesis of literature on qualitative methods developed in resilience research concerning the critical infrastructure (CI) systems, detailing lessons learned from such approaches to shed lights on best practices and identify possible future research directions. The authors of that article have explained that the critical infrastructure systems contribute to producing and distributing essential goods or services. Examples are the energy systems and electric grid including power transmission systems, nuclear power plants, water treatment and distribution infrastructures, wastewater treatment installations, transportation systems, computer systems and communication networks, etc.
The literature review indicates that there a focus is on identifying cyber vulnerabilities and preventing cyber-attacks, but much less attention to mitigate their effects by improving cyber resilience. They propose in related research to widen the cybersecurity concept to the cyber resilience. It requires an evolution of traditional risk management concepts, calling for a greater emphasis on shared responsibility in given organization, leadership, and more involvement of humans in context of using various resources.
They express opinion that qualitative research can play an important role to prioritize activities and identify threats by means of dedicate surveys that can increase the level and quality of information security to next maturity levels. In current uncertain and turbulent world, future research on the resilience of CI should prioritize integration to support the survivability and development of future organizations, communities, cities, and regions, towards next staging areas of evolution and adaptations in dynamic environment.
Dreesbeimdiek et al. (Dreesbeimdiek et al., 2022) describe a systemic (system-of-systems) approach to resilience. Shaping resilience is understood as a continuous process. The authors emphasize that due to multi-disciplinary conceptual developments, varying definitions of resilience have emerged that primarily differ in the process of reaching positive outcomes when facing adverse events. The resilience properties usually considered include adaptability, robustness, agility, and flexibility.
It was explained in that publication, based on some references, that in ecological resilience, systems respond to challenges through adaptation allowing for many possible desirable, emerging states. But, in the resilience engineering concept the systems absorb the shock and should recover as quickly as possible to return to the original functional status. The authors distinguish four system properties, five resilience capacities, and a variety of system activities.
In this conceptual paper, an integrative resilience framework is proposed, which moves beyond simplistic linear models towards adaptive and collaborative strategies to enable social and economic institutions to deal effectively with expected and unexpected changes. Main domains considered include economy, health, environment, and communities. The authors propose, as a next step of research, the identification of metrics that capture not only the performance of the individual subsystems but also of their interfaces.

A concept of *zero trust* has gained significant traction in the cybersecurity realm in protecting networks and increase security across organizations (WEF, 2022). A growing popularity of this security model can be attributed to the shift to hybrid working practices that call for a more secure work environment whether on- or off-premises.

Most cybersecurity challenges arise with the adoption of digitalization. New threat landscape introduced by multi-cloud hosting, the industrial internet of things (IIoT), mobility, remote working and other developments have caused that trust can no longer be implicitly assumed in an internal corporate network.

In contrast to a perimeter-based security model that considers anything from inside the corporate network to be secure and trustworthy, *zero trust* assumes that no user or device can be inherently trusted. Threats can be both external and internal. For organizations to effectively adopt *zero trust* a set of guiding principles is proposed:

- establish no trust by default,
- ensure visibility,
- apply trust with continuous verification,
- use *least privilege*,
- ensure the best possible end-user experience.

The concept of *zero trust* has mostly been applied within the information technology (IT) area. As the IT and OT (operational technology) systems converge across industries, keeping both secure is a challenge in the age of digitalization. Even though certain *zero trust* practices (e.g., network segmentation and multifactor authentication) can be adopted from the IT environment and translated into the OT context, it is important to understand that the OT systems were not designed with cybersecurity in mind.

As innovation continues to transform the industrial environment from the perspective of the IT and OT environment, emerging technologies could be employed to enable novel cyber capacities and improve existing ones.

Technologies such as biometrics and artificial intelligence (AI) can play nowadays a key role in supporting some of the foundational principles of *zero trust*. For instance, facial, fingerprint and voice recognition could be used to identify users, verify access, and detect intrusions. AI could, among other things, automate the detection of threats and abnormal behavior in real time. In the long run, this would enable organizations to take preventive rather than reactive measures.

Resilience has become nowadays a mantra across the business world, and the operational resilience has emerged as a key corporate objective in the post-COVID era (Noggin, 2022). Gartner understands the operational resilience as initiatives that expand business continuity management programs focusing on the impacts of connected risk appetite, and tolerance levels for disruption of product or service delivery to internal and external stakeholders, e.g., employees, customers, citizens, and partners.

The resilience-related initiatives in question coordinate managing the risk assessments, risk monitoring, and execution of controls that impact workforce, processes, facilities, technology, and third parties across the following risk domains used in the business delivery and value realization process (Noggin, 2022):

- security (cyber and physical),
- safety,
- privacy,
- continuity of operations,
- reliability.

Even with the rise in importance of operational resilience, business continuity practitioners will remain responsible for the management of prioritized activities, i.e., those activities that make critical products and services happen. These activities are discovered during a business impact analysis (BIA) process.

Business continuity focuses on getting processes back up and running in an agreed timescale, with the recovery time objective (RTO) focusing on the time it takes to get a process back up and running following a disruption. Operational resilience measures should focus on getting a process up and running before that process causes an intolerable harm to the business, its customers, or the market.

Thus, various resilience concepts have been distinguished in the literature. They concern also macro economy aspects and economy in particular organization (BSI, 2018; McKinsey, 2022a). Some resilience examples are as follows (Kosmowski, 2022):

- financial resilience,
- operational resilience,
- technological resilience,
- organizational resilience,
- reputational resilience,
- business-model resilience.

It becomes clear that in situation of significant un-

certainty and converged systems involved, a reasonable approach to achieve adopted goals is to elaborate a rational strategy of sustainable development combined with appropriate shaping resilience in organizations and industrial companies. It concerns particularly the engineering resilience and operational resilience focused on functional safety and cybersecurity aspects. The rationale is to develop an approach based on forward and backward reasoning in context of goals that could be modified in time when external conditions would change.

3. Sustainable development and resilience issues in reports, legal acts, and standards

3.1. Some concepts and definitions

As suggested in the international standard ISO 37101 (2016) a sustainable development in communities meets the environmental, social, and economic needs of the present without compromising the ability of future generations to meet their own needs.

According to the Cambridge Dictionary a community is understood as the people living in one particular area or people who are considered as a unit because of their common interests, social group, or nationality, in particular the people living in one particular area or people who are treated as a group because of their common interests, social status, or nationality.

In a general sense, it can be an international community. In a narrow sense it can be an organization understood as a group of people who work together in a coordinated way for shared purposes, for instance an institution or industrial company.

Resilience is defined in this standard as an adaptive capacity of an organization in a complex and changing environment to avoid abnormal or crisis situations that would not enable achieving goals that have been set in a sustainable development process.

As it is known, any international standard is being developed by a group of experts that represent specific scientific disciplines and/or experience from professional practice. Final version of the standard before publishing is voted by given technical committee for acceptance, preferably by consensus. In Section 5 of this chapter some standards will be specified concerning directly or indirectly the resilience of safety-related control systems.

If a standard is devoted to the engineering issues in given domain, it is often considered as an example of good engineering practice providing minimal requirements for development of specific technology and/or a framework for evaluations to support decision making in design and/or operation. Using standards is generally not obligatory, but standards can be mentioned in the domain regulation (e.g., in specific directive of EU), as so-called harmonized standards for obligatory using, especially in cases of safety-related technologies and systems.

New interdisciplinary problems to be tackled require a systemic view regarding concepts and models elaborated in relevant domains, particularly a consensus knowledge available. Obviously, it is also important in research area concerning the engineering resilience and the operational resilience of interrelated technical systems. An approach will be outlined below (in Section 5) concerning operational resilience of converged OT and IT systems regarding selected aspects of functional safety and cyber security.

3.2. Sustainable development and engineering resilience

When considering humans and nature it is important to consider a macrosystem regarding socio-ecological aspects. ***Resilience*** related reflections and seeking its rational solution lead inevitably to the systems' perspective and a ***sustainable development*** issue. Thus, the resilience idea is related to some crucial concepts such as: human well-being, environmental changes, safety, new objectives and their achievability, adaptability, and transformability costs etc. (ESDN, 2022).

To achieve such new objectives an ***adaptive governance*** is needed that unites the systemic management of natural resources and various institutional and financial resources using best available and innovative technologies. Relevant processes to be initiated are created regarding the following principles: polycentric and multi-layered institutions, purposeful participation and collaboration, self-organization in networks with clear leadership and responsibility, effective audits, and learning and introducing innovation (ESDN, 2022).

Resilience is being explained simply as the ability of a system to absorb disturbances and still retain its basic function and structure. Resilience is de-

fined also as the ability of a system to succeed under varying and adverse conditions. Specifically, *resilience is an intrinsic ability of given 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).

Following resilience categories have been distinguished and characterized by Pisano (Pisano, 2012):

- ecological resilience,
- socio-ecological resilience,
- engineering resilience.

The first concept is mainly linked to an ecosystem, even though it influences also social changes related to the ability of human communities to withstand external disturbances and shocks for existing social infrastructure. The second concept, so-called socio-ecological resilience, has been suggested as best suited for considering governance issues.

The third one – engineering resilience – has been considered by some researchers as too narrow for the governance because it *focuses on maintaining efficiency of function, constancy of the system, and relatively predictable world near a single steady state* (ESDN, 2012).

Lately, a regulation of the Recovery and Resilience Facility (RRF) has been proposed in the European Union (Regulation, 2021) to be treated as a temporary instrument to tackle resilience problems based on experience acquired in response to economic and societal consequences of the COVID-19 pandemic. The discussions were directed to raise funds to support EU Member States in implementing reforms that align with the EU's strategic priorities and transitions required. The RRF is structured around 6 pillars:

- green transition,
- digital transformation,
- smart, sustainable, and inclusive growth,
- social & territorial cohesion,
- health, economic, social, and institutional resilience, and
- policies for the next generation.

An important pilar of the RRF to be considered and appropriately shaped in time is the digital transformation. It can transform society according to values of inclusion and cohesion. Some challenges related to digitization are the lack of technology required and sufficient skills of specialists in area of advanced information and communication technologies.

The RRF is conceptually related to the sustainable development strategy distinguishing three dimensions (ESE), namely:

- economy (E),
- society (S), and
- the environment (E).

These dimensions can be also analyzed in a framework of resilience evaluation. Crucial meaning for solving existing problems and effective governance of various risks has the economic resilience to be shaped within sustainable development strategy in realization.

As it has been mentioned in this chapter the multidisciplinary knowledge-based systemic approaches are needed to deal with coordinated and sustainable transitions, and the contribution of good governance is crucial. Good governance means to retain oversight over relevant policies and activities that are going on in different sectors and to coordinate and finding synergies whenever it is possible.

3.3. Digital transformation and resilience related acts and directives

The conditions of digital transformation influencing resilience and cybersecurity in sustainable development will be discussed on example of the European Union (EU). Lately, following cybersecurity and resilience related directives and acts elaborated in the EU have been published:

- the NIS 2 Directive,
- the European Cyber Resilience Act,
- the Digital Operational Resilience Act (DORA) for the financial sector,
- the Critical Entities Resilience Directive (CER).

Basic explanations can be found on pages https://digital-strategy.ec.europa.eu/ where the rationale towards the strategy for stronger EU capabilities for effective operational cooperation, solidarity and resilience is presented. Some remarks concerning the NIS 2 Directive and the DORA act are given below.

According to the NIS 2 Directive the cybersecurity risk-management measures should be proportionate to the degree of the essential or important entity's exposure to risks and to the societal and economic impact that an incident would have. A proactive approach to identifying cyber threats

should enable an effective cybersecurity risk management. It will enable the competent authorities effective preventing cyber threats from materializing into incidents that may cause considerable material or non-material damage. For that purpose, the notification of cyber threats is of key importance.
The security of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or of the services offered by, or accessible via, those network and information systems.
The risk is defined in this directive as a potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident. Vulnerability is understood as a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat.
The Digital Operational Resilience Act (DORA) seeks to align the approach to managing ICT and cyber risk in the financial sector across all EU member states. This ICT risk management framework template can be used by financial entities to document compliance with chapter II (ICT Risk Management) of the DORA (EU Regulation 2022/2554). It comprises the following sections:

- governance and organization,
- ICT Risk Management Framework,
- ICT systems, protocols and tools,
- identification,
- protection and prevention,
- detection,
- response and recovery,
- backup policies and procedures, restoration and recovery procedures and methods,
- learning and evolving, and
- communication.

The objective of DORA regulation is to increase the level of harmonization of various digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in comparison to those laid down in the current Union financial services law.
The digital operational resilience is understood as the ability of a financial entity to build, assure, and review its operational integrity and reliability by ensuring, either directly or indirectly using services provided by ICT third-party service providers. It includes a full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, regarding throughout disruptions.
The ICT risk means any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialized, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.
The information asset means a collection of information, either tangible or intangible, that is worth protecting. The ICT asset can be a software or hardware asset in the network and information systems used by the financial entity.
In accordance with their ICT risk management framework, financial entities shall minimize the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools. They shall provide complete and updated information on ICT risk and on their ICT risk management framework to the competent authorities upon their request.
It is worth to mention that the basic requirements as described above are focused on general resilience aspects of the ICT regarding the evaluation of relevant risks. Basic solutions of ICT are shortly discussed below aimed at characterizing frameworks useful for dealing with resilience of industrial automation and control systems (IACS) including human factors.

4. Frameworks for operational resilience analysis of industrial systems

4.1. Cyber physical systems and issue of cognitive realm

Cyber-physical systems (CPS) are often considered as smart systems that include engineered interacting networks of physical and computational components. CPS and related systems, such as the internet of things (IoT) and the industrial internet of things (IIoT), are widely recognized as having great potential to enable innovative applications in multiple economic sectors of the worldwide economy (NIST SP 1500-201, 2017; NIST SP 1900-202, 2019).

Those highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, traffic flow management, smart manufacturing, smart cities and rural development, water and energy supply and use, also including some aspects of communication and emergency response, defense, and homeland security, etc.

The combination of the cyber and physical aspects, and their connectedness, is essential to CPS that generally includes the sensing, computation, and actuation subsystems. CPS involve traditional information technology (IT) as in the passage of data from sensors to the processing of those data in computation, and traditional operational technology (OT) including automation and control systems. The combination of IT and OT systems along with associated timing constraints is a particularly new feature of CPS. Nowadays, the OT and IT systems can cooperate with the cloud technology (CT) (Kosmowski et al., 2019).

Timing and reliability aspects should be a central concern in designing architecture and operation of complex CPS. Also, the safety and security aspects of the CPS operation require special attention of the designer, integrator, and operator.

CPS are characterized by their interaction with their operating environment typically changing one or more of the observed properties, thus providing closed loop control. The CPS environment typically includes humans. The architecture must support a variety of modes of human interaction with CPS to include human as a CPS controller or partner in decision making.

CPS systems can be designed to control combined organizational and physical processes, and therefore specifically address tight human-machine interaction, mostly not addressed in IoT. CPS can encompass both open-loop and closed-loop control systems, while IoT usually focuses on the open-loop systems (NIST SP 1900-202, 2019).

Thus, the IoT concept emphasizes the networking and is aimed at interconnecting all the things in the physical world, thus it is *an open network platform and infrastructure*. The CPS emphasizes the information exchange and feedback, where the system should give feedback and control the physical world in addition to sensing the physical world, therefore forming *a closed loop system with supporting infrastructure*.

Therefore, most CPS definitions include the *system interactions with humans*, including human-in-the-loop (HIL) solutions, while IoT definitions emphasize system-to-system interactions and a level of automation to minimize human interventions.

Generally, the CPS concept comprises or can be integrated with:

- industrial automation and control system (IACS),
- converged technologies OT, IT, and CT,
- critical infrastructures (CI),
- IoT / IIoT solutions, and
- embedded systems (ES).

Thus, the cyber-physical system integrates computing, communication, and storage capabilities with monitoring and/or control of entities in the physical world, and must do so dependably, safety, securely, efficiently, and real-time in many industrial applications (Leitão et al., 2016).

Deploying CPS concept in practice need a methodology to ensure reliability, interoperability, managing evolution, and safety to limit probability and consequences of abnormal or emergency situations to mitigate of defined risks. It is challenging, especially in large scale CPS such as industrial distributed installations, smart grid, smart city, when some of subsystems and networks are designed by different manufacturers and deployed by various integrators.

One of the more important research challenges concerning CPS in modelling is human in the loop (HIL) regarding cognitive aspects of human behavior at relevant levels of the system hierarchy. This issue is discussed below in context of an extended ISA 95 framework.

4.2. Extended ISA 95 framework regarding human cognitive behavior

A typical ICT architecture including converged technologies OT-IT-CT, the IACS components and categories of human activity is shown in Figure 1. Some concepts for integrating functional safety and cyber security analyses are described in publications (Kanamaru, 2020; Kosmowski, 2021a; 2022; Kosmowski et al., 2019, 2022).

At the bottom of OT area following elements and systems are located: the control / safety local area network (LAN), input/output (I/O) elements, the 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 the subsystems of OT. More details about such complex architecture including some basic functional, safety and security requirements regarding selected international standards can be found in a publication (Kosmowski et al., 2019).

In the right side of this figure two blocks represent distinguished categories of human activities within an industrial company. The upper block (A) concerns the business and a long-term operation management. It includes, for instance, the business continuity management (BCM) strategy in relation to functionality of the enterprise resource planning (ERP) system and manufacturing execution system (MES). It corresponds to the levels 3 and 4 distinguished in the ISA 95 reference model (Kosmowski et al., 2019).

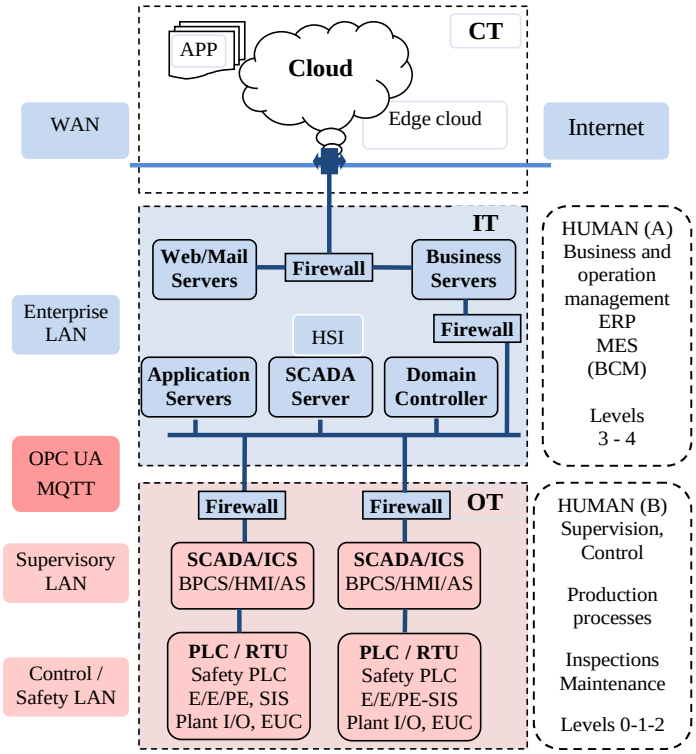

Figure 1. Typical ICT / OT-IT-CT architecture in relation to categories of human activity.

The lower block (B) concerns the supervision and control of production processes including periodical inspections and maintenance according to a strategy developed regarding current state of equipment and predictive models. It corresponds to the levels 0, 1 and 2 distinguished in the ISA 95 reference model (Kosmowski et al., 2019). These two blocks represent cognitive realm of human behaviors at relevant levels of the system model. The time window for human reaction in abnormal situation is an important factor influencing correct diagnosis and action. If this time is too short then the human error probability (HEP) can be high, close to 1 (Kosmowski, 2022). Such situation can deteriorate the system resilience depending on the design solution of safety-related control system designed, for instance to fulfil requirements of functional safety standards (IEC 61508, 2010; IEC 61511, 2016). Selected issues of human reliability analysis (HRA) including cognitive aspects will be discussed later in context of functional safety analysis of the control system and SCADA interface.

5. Operational resilience regarding functional safety and cybersecurity requirements

5.1. Determining and verifying SIL of safety functions in life cycle

The functional safety is defined as a part of general safety of an industrial plant or critical installation, which depends on a proper response of the safety-related control system (SRCS) during an abnormal situation or accident to avoid or limit

consequences and mitigate risks. The functional safety methodology has been formulated in a generic standard IEC 61508 (2010) and is used in the design and operation of the electric / electronic / programmable electronic (E/E/PE) systems in life cycle. Different names of the SRCS are used in various industrial sectors, for example, the safety instrumented system (SIS) in case of the process industry sector (IEC 61511, 2016). Such systems are designed to implement defined safety functions to ensure that the risk evaluated is reduced to specified tolerable level in entire life cycle.

The safety integrity level required (SIL_r), to be assigned to given safety function, is determined based on the results of the risk analysis to reduce sufficiently the risk of potential losses. Three categories of losses (l) are usually distinguished: health (H), environment (E) or material (M). The SIL_r^l is determined for particular safety function and relevant categories of losses and then resulting SIL_r (SIL required) is determined as follows

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

Resulting level of SIL_r (1, 2, 3 or 4) indicates a necessary risk reduction (RR). For instance, if $SIL_r = 3$ then RR will be at least 1000.

The safety integrity (SI) 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 system, in which defined safety function is to be implemented, two probabilistic criteria are defined as presented in Table 1 for four categories of the safety integrity level (SIL), namely:

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

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

Typical hardware architecture of the E/E/PE system, shown in Figure 2, consists of three subsystems: (A) sensors and input devices (transducers, converters etc.), (B) logic device (e.g., safety PLC or safety relay modules), and (C) actuators.

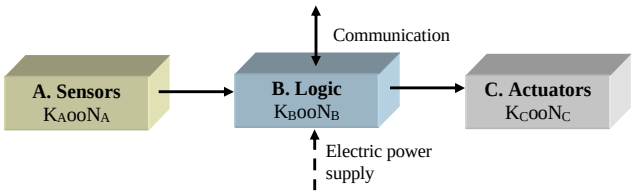

Figure 2. Typical architecture of the E/E/PE system or SIS.

The subsystems shown in Figure 2 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 regarding the value of a safe failure fracture (S_{FF}).

Designing the architecture of entire SRCS is considered as satisfactory, if verified SIL (using a probabilistic model) is at least as high as SIL_r ($SIL \geq SIL_r$). Details of determining and verifications of the safety integrity level can be found in publications (Kosmowski, 2022; Kosmowski et al., 2022).

5.2. Determining and verifying SAL of IACS domain

Figure 3 presents the requirement trads for the OT and IT domains. In case of OT an AIC (availability, integrity, and confidentiality) triad is often proposed for prioritizing basic safety and security requirements, as opposed to a triad CIA (confidentiality, integrity, and availability) being assigned to IT network. A strategy should be carefully elaborated for the life cycle that includes inspection, testing, preventive maintenance plans and incident management procedures (Kosmowski et al., 2019).

The security-related risks shall be mitigated through a combined effort of the component suppliers, the machinery manufacturer, the sys-tem integrator, and the machinery end final user / the company owner (ENISA, 2016; IEC 62443, 2018; IACS Security, 2020; Ladkin, 2019). Generally, the responses to the security risks should be as fol-

lows (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.

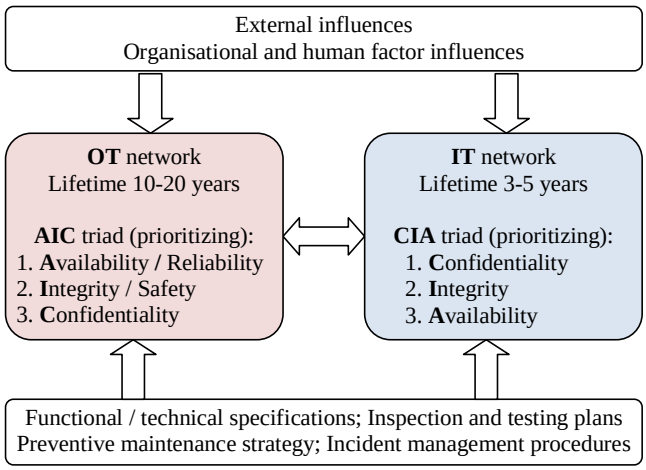

Figure 3. Triads of basic requirements for the OT and IT networks.

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.

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

Relevant SL number from 1 to 4 are to be assigned to consecutive seven foundational requirements (FRs) that are relevant in the domain analyzed (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).

An approach to assign the resulting security assurance level (SAL) for given domain based on FRs evaluated by experts is described in publications (Kosmowski, 2022).

Details of the method can be found in the publication (Kosmowski et al., 2022). In this chapter 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.

Shaping sufficiently strong resilience of the industrial control systems in the architectural and functionality context of IT and OT networks will be successful only in companies with good organizational culture. High reliability organisation will undoubtedly allow to shape strong safety and security culture. It is a prerequisite of advanced functional safety and cyber security solutions to reduce effectively risks. General security-related requirements concerning the IT systems and networks are specified in the international standards (ISO/IEC 27001, 2013; ISO/IEC 27005, 2018).

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

5.3. Operational resilience regarding human reliability and alarm system design

Appreciated HRA method, developed for dealing with cognitive aspects in evaluating human error probability (HEP) for defined activity, is a HCR

(human cognitive reliability) technique based on a probabilistic model developed by Hannaman et al. (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, 2023).
Three types of human behavior types are distinguished (Kosmowski, 2022), according to Rasmussen's conceptual model:

- skill based (S),
- rule based (R), and
- knowledge-based (K).

Time-dependent ***HEP***, treated as an event of non-response or human error in the situation considered, is calculated from the Weibull distribution from following formula:

$$HEP^{x}(t) = \exp\left\{-\left[\frac{\frac{t}{t_{0.5}} - a}{c}\right]^{b}\right\} \quad (2)$$

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 human operators. If median value $t_{0.5}$ is short, e.g., below 1 min., then ***HEP*** is high, and cab be close to 1.
Different HRA method 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:

$$HEP = \frac{NHEP \cdot PSF^{\text{composite}}}{NHEP\left(PSF^{\text{composite}} - 1\right) + 1} \quad (3)$$

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.
Described above models can be applied in analyses of operational resilience of the OT and IT networks when reactions of persons, responsible for functioning of these networks, are required, to diagnose correctly abnormal situation and to undertake action to shorten outage time of industrial installation. Similar models could be also used within the business continuity management (BCM) as suggested in the publication (Kosmowski et. al., 2022).
Correct reaction of operators in abnormal situation or emergency depends on the alarm system (AS) design. Three cases can be considered (EEMUA, 2007):
(1) AS is designed as not safety-related (within BPCS treated as not safety-related),
(2) AS is designed as safety-related for the safety integrity level SIL1,
(3) AS is designed as safety-related for the safety integrity level SIL2 or higher.

If the risk for given industrial installation is high, then AS must be designed as separated from BPCS. To obtain high operational resilience of such system, in its designing ***HEP*** should be evaluated. In case (3) of AS solution it is not recommended to assume ***HEP*** below 10^{-2} for any operator action, even if there is multiple alarming and task is relatively simple (EEMUA, 2008).

5.4. Research, standards, and challenges

As it has been discussed above, the resilience-oriented analyses include conventional reliability, safety and security-related evaluations in life cycle based on the hazards and threats identifying and assessing of risks regarding criteria determined.
These issues are also important in the domain of performability engineering that has been stimulated by Misra for many years (Misra, 2021). A review of many sustainability and resilience-related publications in an article (Mayar et al., 2022) shows a range of new challenges to undertake in research. It is important also for interdependent infrastructure systems (Naderpajouh et al., 2017). Key performance indicators (KPIs) for manufacturing operations management in context integration of automation systems are proposed in a standard (ISO 22400, 2014). Security and resil-

ience-related requirements are proposed in international standards (ISO/DIS 22301, 2019; ISO 22316, 2017; ISO/IEC 24762, 2008).

This chapter deals mainly with operational resilience of the industrial automation and control systems (IACS). Operational resilience is treated as a part of engineering resilience. A framework is proposed based on a general concept of cyber physical systems (CPS) including human in the loop (HIL) aspects regarding appreciated concepts, models and standards concerning the functional safety and cyber security IACS. Basic concepts of requirements concerning IACS are described in publications (SE, 2001; NIST SP 800-82, 2015; NIST SP 800-160, 2016, 2019).

It is crucial for further research to include new concepts from publications in the area and appreciated reports and international standards used already in industrial practice. The synergy of researchers' and specialists' efforts developing new technologies regarding standards developed by researchers and practitioners (in a consensus way) is crucial for reaching common success. Obviously, the persons involved should have feedback from the producers of innovative technologies and practitioners expecting better support in operation of manufacturing systems, and the safety and security-related systems.

Thus, human factors and organizational factors are crucial to shape operational resilience. In the approach outlined in this chapter they are symbolically denoted as HIL within cyber physical system. Two categories of HUMAN activities (A) and (B) are distinguished in Figure 1. Those are supervised in industrial companies respectively by the Chief Information Officer (CIO) and Chief Technology Officer (CTO).

Category (B), including cognitive aspects of human behavior in human reliability analysis, has been discussed above in Item 5.3 Category (A) concern cognitive aspects in management processes at higher levels of the system model in CPS. They include the logistic related activities and supporting technologies (Katina, 2016) and blockchain-enabled resilience within an integrated approach for disaster supply chain and logistics management (Katina & Gheorghe, 2023).

Proactive risk management approaches in a dynamic industrial society have been investigated by Rasmussen and Svedung (2000).

6. Conclusion

Various definitions of resilience in the context of sustainable development have been formulated in the literature and several definitions of operational resilience. The operational resilience concept has been discussed in this chapter with explanations regarding selected scientific publications, reports issued by some research institutions and related international standards.

Gartner defines the operational resilience as initiatives that expand business continuity management (BCM) programs focusing on the impacts of connected risk appetite, and tolerance levels for disruption of product or service delivery to internal and external stakeholders, e.g., employees, customers, citizens, and partners.

Another definition of operational resilience is focused on the industrial systems, including smart manufacturing systems. They 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 requirements of products.

The main objective of this chapter was to outline an approach for shaping the operational resilience in sustainable development of the industrial systems in life cycle. This approach concentrates on the industrial automation and control systems (IACS) regarding the design solutions of functional safety and cybersecurity. Nowadays, industrial control systems play a crucial role in all technical systems significantly influencing their reliability, safety, and cybersecurity.

It includes determining and verifying the safety integrity level (SIL) of defined safety functions and the security assurance level (SAL) of domains in computer systems and networks. The issue of the alarm system integrity in context of human reliability analysis (HRA) is also discussed. New research challenges concerning resilience of the industrial automation and control systems have been also discussed.

A proactive resilience-based approach has significant advantage if compared with conventional safety and security methodology based mainly on probabilistic modelling for evaluation of risks. It can be also useful for the business continuity management (BCM) that focuses mainly on getting processes back up and running in an agreed timescale regarding, e.g., the recovery time objective (RTO).

Operational resilience measures should be focused on getting a process up and running before that process causes an intolerable harm to the business, its customers, or the market. Thus, it is an extension of conventional BCM methodology.
Next research works to be undertaken, related to the topics of this chapter, could include:

- models of CPS regarding cognitive aspects of human behavior (see categories HUMAN A and B in Figure 1 at relevant levels of the system) regarding the cognitive resilience engineering (CRE) concepts and precepts,
- evaluation of human factors from the CPS perspective regarding HIL (human in the loop) and reliability analysis methods in the IACS context including required behavior of human operators who use interfaces HMI, HSI and AS, and advanced AI algorithms within decision support systems (DSS),
- benefits and risks of applying machine learning (ML) methods and AI methods in area of safety and security of industrial systems and critical infrastructure (Industry 5.0),
- benefits and risks using cloud technology (CT) and advanced OPC UA protocols within converged IT and OT systems and networks.

References

Bouloiz, H. 2020. Sustainable performance management using resilience engineering. *International Journal of Engineering Business Management* 12, 1–12.

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

Cantelmi, R., Di Gravio, G., Patriarca, R. 2021. Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions* 41, 341–376.

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.

Dreesbeimdiek, K.M., von Behr, C.M., Brayne, C., Clarkson, P.J. 2022. Towards a contemporary design framework for systems-of-systems resilience. *International Design Conference. Design 2022*. Cambridge University Press

EEMUA. 2007. Publication 191: *Alarm Systems, A Guide to Design, Management and Procurement* (Edition 2). London: The Engineering Equipment and Materials Users' Association.

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

ESDN. 2012. Resilience and sustainable development: Theory of resilience, systems thinking and adaptative governance. *ESDN Quarterly Report* 26.

ESDN. 2022. European recovery and resilience mechanisms – challenges in systemic approaches in sustainable development. *ESDN Report*, May 2022, ESDN Office, Vienna.

Flaus, J.M. 2019. *Cybersecurity of Industrial Systems*. ISTE Ltd and John Wiley & Sons, Inc.

Grøtan, T.O, Petersen, S., Myklebust, T. & Hanssen, G.K. 2020. SecureSafety; state-of-the-art and remaining challenges. P. Baraldi, et al. (Eds.). *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference* Research Publishing, Singapore.

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

Häring, I., Scharte, B., Stolz, A., Leismann, T., Hiermaier, S. 2016. *Resilience Engineering and Quantification for Sustainable Systems Development and Assessment: Socio-technical Systems and Critical Infrastructure. A part of the IRGC Resource Guide on Resilience*, www.irgc.org/riskgovernance/resilience/ (accessed 30 Jun 2023).

Hickford, A.J., Blainey, S.P., Hortelano, A.O., Pant, R. 2018. Resilience engineering: theory and practice in interdependent infrastructure systems. *Environment Systems and Decisions* 38, 278–291.

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

Hollnagel, E., Woods, D., Leveson, N. 2006. *Resilience Engineering: Concepts and Precepts*. 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*, www.isa.org/ISAGCA (accessed 30 Jun 2023).

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 63069. 2019. *Industrial Process Measurements, Control and Automation – Framework for Functional Safety and Security*. 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*. International Organization for Standardization. Geneva.

ISO 22316. 2017. *Security and resilience – Organizational resilience – Principles and attributes.* International Organization for Standardization. Geneva.

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

ISO 37101. 2016. *Sustainable development in communities – Management system for sustainable development – Requirements with guidance for use.* International Organization for Standardization. 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.

Katina, P.F., Keating, Ch.B. Gheorghe, A.V. 2016. Cyber-Physical Systems: Complex System Governance as an Integrating Construct. *Proceedings of the 2016 Industrial and Systems Engineering Research Conference* H. Yang, et al. (Eds.).

Katina, P.F., Gheorghe, A.V. 2023. *Blockchain-Enabled Resilience, An Integrated Approach for Disaster Supply Chain and Logistics Management.* CRC Press, Taylor & Francis Group.

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. 2022. Towards strategic resilience of process plants and critical infrastructure regarding functional safety and cybersecurity requirements. K. Kołowrocki et al. (Eds.). *Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2022*. Gdynia Maritime University, Gdynia, 117–132.

Kosmowski, K.T. 2023. Functional safety management in hazardous process installations regarding the role of human operators interacting with the control and alarm system. *In: Intelligent and Safe Computer Systems in Control and Diagnostics* Z. Kowalczuk (Ed.). Springer, Lecture Notes in Networks and Systems, 545, 85–99.

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.

Ladkin, P.B. 2019. IEC TRC 63069, Security environments and security risk analysis. *ResearchGate*, www.researchgate.net/publication (accessed 30 Jun 2023).

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.

Mayar, K., Carmichael, D.G., Shen, X. 2022. Resilience and systems – A review. *Sustainability* 14, 8327.

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

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

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

Naderpajouh, N., Yu, D., Aldrich, D.P., Linkov, I. 2017. *Towards an Operational Paradigm for Engineering Resilience of Interdependent Infrastructure Systems. Agenda Setting Scoping Studies Summary Report. The Resilience Shift.*

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.

NIST SP 1500-201. 2017. *Framework for Cyber-Physical Systems*: Vol. 1, Overview.

NIST SP 1900-202. 2019. *Cyber-Physical Systems and Internet of Things.*

Noggin. 2022. Operational Resilience Versus Business Continuity: What's the difference? www.noggin.io (accessed 30 Jun 2023).

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.

Pisano, U. 2012. Resilience and Sustainable Development: Theory of resilience, systems thinking and adaptive governance. *ESDN Quarterly Report No 26.* European Sustainable Development Network (ESDN).

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

Redman, Ch.L. 2014. Should sustainability and resilience be combined or remain distinct pursuits? *Ecology and Society* 19(2), 37.

Regulation. 2021. Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility. Document 32021R0241.

Rieger, C.G. 2013. *Resilient Control Systems – Practical Metrics Basis for Defining Mission Impact.* DOE Idaho Operations Office Contract DE-AC07-05ID14517, Instrumentation, Control, and Intelligent Systems (lCIS) Distinctive Signature of Idaho National Laboratory.

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.

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

WEF. 2022. *The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment.* Community Paper. World Economic Forum, Cologny, Geneva.