Advances in Reliability, Safety and Security, Part 7 – Kołowrocki, Magryta-Mut (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-19-7 (printed), ISBN 978-83-68136-06-7 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Operational Resilience Of Industrial Plants And Interdependent Infrastructure Systems

Kazimierz T. Kosmowski

Polish Safety and Reliability Association, Gdansk, Poland

Abstract

This paper addresses selected issues and research challenges concerning the resilience, in particular the operational resilience, of industrial plants and interdependent infrastructure systems. Such plants and systems are being designed and operated regarding relevant regulations and standards to meet the reliability, quality and productivity, safety and security requirements and the risk criteria. Due to their complexity as well as changing and uncertain operational conditions they should be, first of all, characterized by a high resilience to be governed in entire life cycle. It requires sustainable solutions that include technical and organizational aspects remembering that new hazards can emerge in time and related risks. The problem is considered in the light of selected literature concerning the systems engineering, performability engineering, business continuity management and the resilience engineering in relation to the concept of sustainable systems development. Operational resilience is discussed versus business continuity. A focus is on the operational resilience of converged operational technology (OT), information technology (IT) and cloud technology (CT). The operational resilience analysis of the industrial automation and control system (IACS) in life cycle is directed on the safety-related control systems (SRCS) regarding the functional safety and cybersecurity aspects.

Keywords: operational resilience, resilience engineering, industrial plants, business continuity management, control systems, functional safety, cybersecurity, interdependent infrastructure systems

1. Introduction

Shaping resilience of technical systems in the 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 (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 in-formation 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 maintaining reliable and timely supply chains, etc.

The main objective of this paper 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.

2. Towards strategic resilience

2.1. Sustainable development and resilience issues

Many papers and reports have been published over last decades concerning concepts and research challenges of sustainable development and resilience. However, there are still open questions how to proceed in practice to support decision making in solving the resilience problems in complex systems, especially those that are interdependent.

Lately, a holistic view on resilience issues has been proposed with examples of relevant attributes and principles (in parentheses), for instance in a publication by Naderpajouh et al. (2017):

- social resilience (leadership, linking social capital, cultural norms, autonomy, cohesion and social ties),
- social-ecological resilience (monitoring, learning, feedback, adaptivity, participation, diversity), and
- engineering resilience (monitoring, anticipation, planning, response, robustness, redundancy, adapting).

There is an increasing research interest to include within the resilience engineering concept the resilience issue of interdependent systems (Hickford et. al, 2018). It is especially justified in cases of complex industrial plants and critical infrastructure systems (Kosmowski, 2022, 2023).

As it is stated in the international standard ISO 37101 (2016) a sustainable development in communities meets the environmental, social, and economic needs of the present and near future without compromising the ability of future generations to meet their own needs. In a general sense, it can be a regional or given state community. In a narrow sense it could be an organization understood as a group of people who work together in a coordinated way for shared purposes, for instance in given 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 a crisis situation that would not enable achieving goals set in a sustainable development process.

The organizational resilience is defined in an international standard ISO 22316 (2017) as the ability of an organization to adapt in a changing environment to enable it to deliver its planned objectives and to survive in in the future and to prosper on competitive markets. More resilient organizations are able to anticipate and respond to hazards, threats, and opportunities, arising from sudden or gradual changes in their internal and external context including business environment. It is stated that enhancing resilience should be a strategic organizational goal and an outcome of good business practice to effectively manage resources, eliminate hazards and mitigate risks evaluated periodically or in situation of rapid internal and external changes.

In a recent publication (McKinsey, 2022a) the idea of a new approach is outlined how to move efforts from the risk management to shaping a strategic organizational resilience. It also concerns the cybersecurity trends that require looking over the horizon (McKinsey, 2022b). The core resilience areas have been categorized as follows (McKinsey, 2022a):

- Financial resilience. Institutions must balance short- and longer-term financial aims. Resilient companies can achieve superior margins by increasing revenue more than controlling costs.
- 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, planned productivity, safety, and security.
- 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 and international standards.
- Organizational resilience. Resilient firms should attract and develop talent in areas critical to their future growth and the ability of an organization to adapt in a changing environment and crisis situations.
- 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 issues.
- Business-model resilience. Resilient organizations develop business models that can adapt to significant shifts in customer demand, technological changes, as well as the legal and regulatory terrains.

Generally, two kinds of strategic resilience can be distinguished (Kosmowski, 2022, 2023):

(I) Resilience of business processes to be evaluated using, e.g., the business continuity management (BCM) methodology and others, and

(II) Resilience of the safety and security-related technologies to be managed in life cycle of the system considered.

In area (II) the resilience of industrial automation and control systems (IACS) is considered. It includes the requirements imposed on solutions of the functional safety (FS) and cybersecurity (CS) that are designed regarding the defense in depth (DinD) concept using defined protection layers.

A holistic approach to shaping resilience creates undoubtedly the advances in the organization, ranging from focusing on the risk, controls, governance, and reporting to a strategic view in anticipated conditions of changing environment. An important issue of holistic approach involves developing the crisis scenarios to test for resilience in potential downturns and outages, similarly as it is analyzed applying the business continuity management (BCM) model (Kosmowski et al., 2022). These issues are outlined below and will be discussed more comprehensively during the workshop.

2.2. Resilience engineering and operational resilience

The 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. A review of fundamental concepts and development directions of the resilience engineering, useful for future research in area of safety and security governing can be found in a publication by Pillay (2017).

Resilience can be generally defined as the ability of a system to succeed under varying and adverse conditions. Specifically, the resilience is defined as 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).

In Figure 1 the resilience capacity is divided into its constituent elements. These include: anticipation capacity, preventive capacity, absorptive capacity, protection capacity, reaction capacity, restorative capacity, and adaptive capacity. These capacity should be govern in life cycle based on results of audits performed periodically according to a strategy and objectives of given organization regarding business and environmental conditions changing in time.

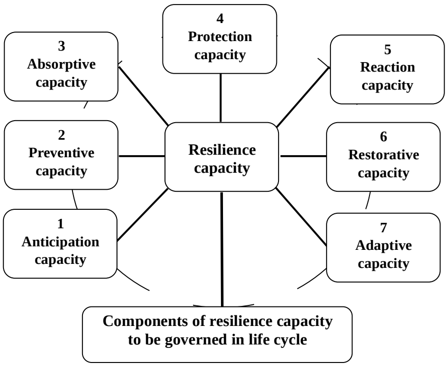

Fig. 1. Resilience capacity and its constituent elements.

It is necessary to consider a spectrum of potential situations, from minor up to larger disruptions, including creeping situations or sudden events leading to a major accident with serious consequences. Such hazardous events lead to crisis that should be considered both in the societal and technical contexts (Häring et al., 2016). A systemic approach is necessary to deal with such situations in life cycle in changing conditions (Kosmowski, 2023).

3. Operational resilience

3.1. Operational resilience versus business continuity

Proposed business continuity management (BCM) framework comprising the business continuity plan (BCP) in an industrial company is presented in Figure 2. On left site of this figure some important stages of the BCP development are specified regarding suggestions of the ISO/IEC 24762 (2008) standard:

(1) Conducting a business impact analysis (BIA) and preliminary risk assessment regarding identified hazards / threats.
(2) Establishing business recovery priorities, timescales for recovery, and related requirements.
(3) Business continuity strategy formulation (options for meeting priorities including technical and organizational aspects),
(4) Business continuity plan development (organization, responsibilities, logistics, and detailed action task lists),
(5) Business continuity plan testing for verification of strategy and plan elaborated,
(6) Ensuring business continuity awareness (for all staff),
(7) Ongoing business continuity plan updating including maintenance activity.

The BCP includes the company business requirements and an agreement with the service providers. The recovery procedures (RP) should be developed for expected abnormal situations, major failure events, together with so-called disaster recovery plan (DRP) for cases of potential disruptions and major accidents.

In the middle of Figure 2 a BCM system is presented to deal with the dependability, safety, and security aspects. The management activities are based on knowledge acquired (from relevant domains), current information, evidence, and results of probabilistic modelling and evaluation of risks in context of criteria. The analyses and evaluations include relevant domain key performance indicators (KPIs).

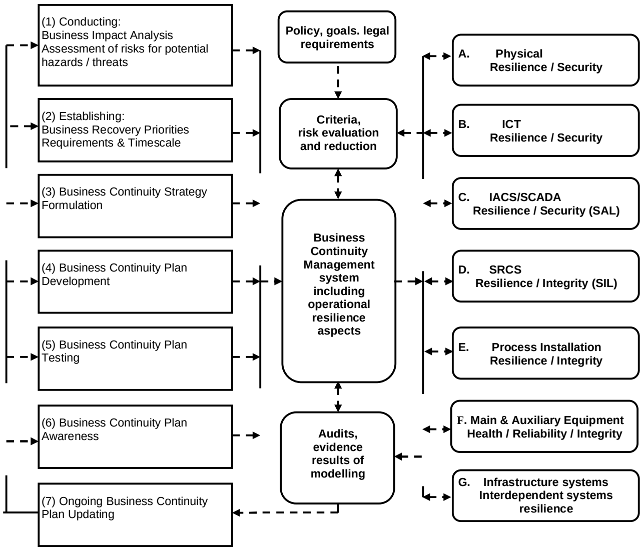
(1) Conducting:
Business Impact Analysis
Assessment of risks for potential hazards / threats
(2) Establishing:
Business Recovery Priorities
Requirements & Timescale
(3) Business Continuity Strategy Formulation
(4) Business Continuity Plan Development
(5) Business Continuity Plan Testing
(6) Business Continuity Plan Awareness
(7) Ongoing Business Continuity Plan Updating
Policy, goals. legal requirements
Criteria, risk evaluation and reduction
Business Continuity Management system including operational resilience aspects
Audits, evidence results of modelling
A. Physical Resilience / Security
B. ICT Resilience / Security
C. IACS/SCADA Resilience / Security (SAL)
D. SRCS Resilience / Integrity (SIL)
E. Process Installation Resilience / Integrity
F. Main & Auxiliary Equipment Health / Reliability / Integrity
G. Infrastructure systems Interdependent systems resilience

Fig. 2. Proposed framework for BCM including resilience aspects.

On the right site of Figure 2 seven areas are proposed in a process of BCM including resilience aspects that requires considering relevant technical and organizational solutions:

A. Physical resilience of security-related resources / assets.
B. Information and communication technology (ICT) resilience and its security in life cycle.
C. Industrial Automation and Control System (IACS) including Supervisory Control and Data Acquisition (SCADA) system to be adequately resilient and secure at required security assurance level (SAL).
D. Safety-related control systems (SRCS) to be designed and operated according to functional safety concept at required safety integrity level (SIL).
E. Industrial installations and processes with required physical integrity and protections.
F. Equipment (main and auxiliary) health / reliability / integrity to be adequately maintained according to a strategy developed to achieve a high overall equipment effectiveness (OEE).
G. Infrastructure systems (delivery of materials and energy needed for production processes) resilience regarding potential their interdependency.

Expected outcomes of an effective BCM program including resilience aspects to be implemented are as follows:

- key products and services are identified and protected to ensure required quality and effectiveness,
- an incident management capability is enabled to provide the effective response,

- a company understands more its relationships with cooperating companies, regulators and authorities as well as the emergency services,
- the staff is better trained to respond effectively to incidents or disruptions through appropriate training and exercising,
- requirements of stakeholders and shareholders are better understood and able to be delivered,
- the staff receives adequate support and communications during potential disruption events,
- the company's supply chain is better secured,
- the organization's reputation is protected and remains compliant with its legal and regulatory obligations.

It is important, from theoretical and practical point of view, to understand differences between the operational resilience versus business continuity. The fields of business continuity and operational resilience, despite their overlaps, are distinct (Noggin, 2023). Practitioners would do well to acknowledge existing differences rather than to risk undermining the viability of their resilience aims. Some sectoral definitions of operational resilience extend the purview of this field beyond that of business continuity and disaster recovery.

Gartner treats the operational resilience initiatives (Noggin, 2023) as those expanding the business continuity management programs to focus more on the impacts, 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 the management of 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, such as: security (cyber and physical), safety, privacy, continuity of operations, and reliability.

Organizations, for instance due to the pandemic or global and regional supply chains problems, have been trying to manage a significantly different operating environment. That's fundamentally changed the way businesses interact with technology, customers, and their own employees. Also climate change, for its part, is set to test infrastructural resilience to physical risks while disrupting operations through changes in market sentiment and economic models. These factors make operational resilience more important than ever. It is obvious that the organizations have to prevent disruption, but they must also adapt to change (Noggin, 2023).

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 to be delivered. These activities are discovered during the BIA process (see Figure 2). In fact, business continuity focuses on getting processes back up and running in an agreed timescale, e.g., regarding the Recovery Time Objective (RTO) required. The operational resilience measures should focus more on getting the process up and running before that process causes intolerable harm to the business, its customers, or the market. Proposed steps to achieving operational resilience are as follows (Noggin, 2023):

(1) Identify critical products and services.
(2) Set impact tolerances.
(3) Conduct end-to-end mapping and identify interconnections.
(4) Perform scenario testing of plausible scenarios.
(5) Integrate Third-Party Risk Management (TPRM) into resilience initiatives.

3.2. Context of digital transformation and resilience related directives and acts

The conditions of digital transformation influencing resilience and cybersecurity will be discussed on example of the European Union (EU) and in consequence its member states. Lately, following cyber-security and resilience related directives and acts elaborated in the EU have been published:

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

Basic explanations can be found under the Internet address 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 exposure to risks of an essential (or important entity), including 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 nonmaterial 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. Vulnerability is understood as a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat. 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.

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 potential disruptions.

4. Systemic operational resilience analysis of industrial installations and interdependent infrastructure systems

4.1. Typical architecture of converged OT-IT-CT systems and IACS

Typical architecture of the information and communications technology (ICT) is shown in Figure 3. It comprises the computer systems and networks of the operational technology (OT), information technology (IT) and the cloud technology (CT) for data processing, transferring and storage including technology for the edge computing. The information diodes for securing the computer networks should be adequately designed using relevant solution for the Demilitarized Zones (DMZ) distinguished.

At the bottom of the OT area following elements and systems are located: a local area network (LAN), the input/output (I/O) elements, equipment under control (EUC), the electrical / electronic / programmable electronic (E/E/PE) system or safety instrumented system (SIS), the safety programmable logic controllers (PLC), a basic process control system (BPCS), a human machine interface (HMI), an alarm system (AS), the remote terminal units (RTU). At this level the industrial automation and control system (IACS) is also designed including local supervisory control and data acquisition (SCADA) system to enable supervision by the human operators of controlled processes, especially in abnormal situations.

At higher in hierarchy IT system level a human system interface (HSI) is distinguished that enables the human operators to monitor and control the OT subsystems within a SCADA sever. At this level various severs are placed that enable management of assets in realization of the business plans as well as the supervision and control of the production processes. The IT computer systems communicate with the wide area network (WAN) and Internet. Some relatively new protocols for communication are proposed to be implemented: Open Platform Communication Unified Architecture (OPC UA) or MQ Telemetry Transport (MQTT), although there are still some cybersecurity problems to be solved when the CT is of interest including the edge computing solution.

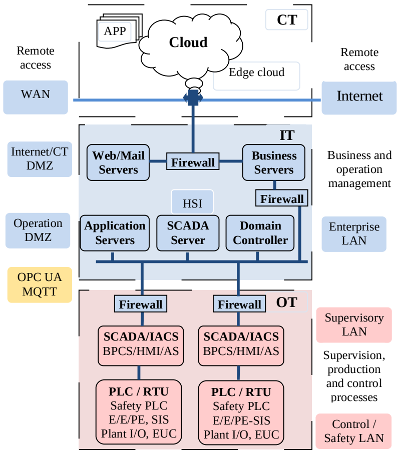

Fig. 3. Typical ICT architecture comprising converged OT/IT/CT systems and IACS.

More details about complex computer architectures in the industry to be designed regarding the functional safety concept and cybersecurity requirements for the IACS according to relevant international standards can be found in publications (Kosmowski, 2020, 2021, 2022. 2023).

4.2. Resilience oriented analysis of interdependent digital infrastructure systems

The digital transformation has a profound impact on the computer networks and control environment. Improvements in cost and performance have encouraged the evolution of the IACS by utilizing the IT and OT capabilities in existing systems, resulting in so called “smart systems”, such as the smart electric grid, smart transportation, smart buildings, etc. in the Industry 4.0 and 5.0 solutions. Technological advances have made it possible that IACS have great flexibility, scalability, and connectivity within converged IT and OT system at all its levels (IEC 62443, 2018; IACS Security, 2020).

Integrated functional safety and cybersecurity aspects are treated as a part of the resilience analysis (Kosmowski, 2023). As it was discussed in that publication, four security level (SL) categories are distinguished and defined in the standard IEC 62443 (2018). They have been discussed in publications by Kosmowski (2021, 2022, 2023) in the context of functional safety concept described in the standards (IEC 61508, 2010; IEC 61511, 2016; IEC 63069, 2019) in which four safety integrity levels (SILs) are also distinguished. So, the problem was encountered how to treat these issues in an integrated way in functional safety analysis regarding cybersecurity aspects of the industrial computer network. The correlation between SIL and security assurance level (SAL) was proposed in publications (Kosmowski, 2020, 2022). Similar correlation have been proposed for the SRCS of manufacturing systems, remembering that in the machinery sector the highest SIL to be assigned to the safety-related systems is SIL 3.

Proposed correlations between defined security index (SI) to be assigned to the domain (Do) SI^{Do} or SAL and final SIL attributing to given SRCS in industrial installation are presented in Table 1. It was assumed that SIL has been verified according to IEC 61508 based on results of probabilistic modelling, including a common cause failure (CCF), human factors and so called architectural constrains for known a safe failure fraction (S_{FF}) and the hardware fault tolerance (HFT) of subsystems in the SRCS considered (Kosmowski et al., 2022).

Table 1. Proposed correlation between SI^{Do} or SAL for given domain and final SIL to be attributed to the SRCS.

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

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

Following issues should be carefully considered in the design and operation process of resilient digital systems:

- System architecture - to design the system architecture with inbuilt resilience, which will be more adjusted to safeguard, using redundant safety systems and defence in depth (D-in-D) solutions.
- System version/update management (patching of software) - to keep the system up to date with the latest version and remove the obsolescent components.
- Regular maintenance and backup – to maintain the system regularly and improve its ability to recover from any abnormal situation or breakdown.
- Dedicated support and resource – to retain standards against pressures of cost, constrained resourcing, and workflow; it is especially important in cases of the safety and security related systems within converged OT-IT-CT systems.

4.3. Operational resilience governance on example of safety-related control systems

A hierarchy of decisions to be undertaken proactively, based on information flow in the context of documentation and activity using a process based management system, is presented in Figure 4. The strategic decisions concerning governance of the operational resilience are elaborated at level 1 taking into account opinions of interested stakeholders and shareholders (Kosmowski & Gołębiewski, 2019). These decisions are carefully considered at a tactic level 2 in relevant processes distinguished in the management system that is designed to include the resilience aspects of given industrial installation regarding interdependent infrastructure systems. Resulting plans of activities are executed at level 1 according to preprepared procedures and instructions that should be periodically verified in entire life cycle.

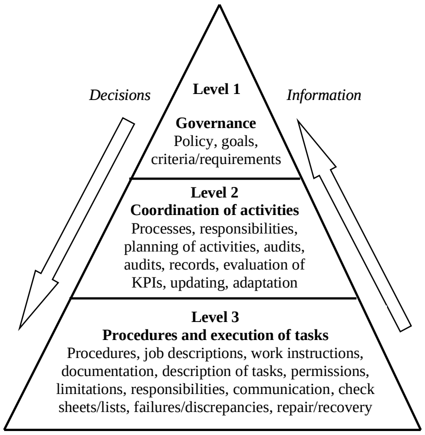
Decisions
Information
Level 1
Governance
Policy, goals,
criteria/requirements
Level 2
Coordination of activities
Processes, responsibilities,
planning of activities, audits,
audits, records, evaluation of
KPIs, updating, adaptation
Level 3
Procedures and execution of tasks
Procedures, job descriptions, work instructions,
documentation, description of tasks, permissions,
limitations, responsibilities, communication, check
sheets/lists, failures/discrepancies, repair/recovery

Fig. 4. Hierarchy of activities for systemic governance of resilience.

According to basic requirements of a quality management (QM) standard ISO 9000 (2015) to each process (see level 2) the owner (a competent specialist responsible for given process, e.g. coordinating of functional safety, cyber security and operational resilience aspects) has to be assigned. The framework for BCM including resilience aspects shown in Figure 2 seems to be useful for distinguishing processes and procedures in systemic resilience management systems including the reliability, quality, productivity, safety, and security aspects. In development of such process, mentioned above functional safety and cybersecurity-related standards as well as the standards ISO/IEC 27001 (2022) and ISO/IEC 27005 (2022). Distinguishing the processes and procedures in a QM system depend on size of company, e.g. small or medium enterprise (SME) or a large distributed company, eventually an international consortium. All of them have to follow state regulations, EU directives and good engineering practices in area of safety and cybersecurity. Mentioned above standards are useful for preparing relevant checklists.

Given process within quality management system is coordinated based on current information, audits, and evaluation of various factors and/or indicators, including a set of key performance indicators (KPIs). For proactive safety management of the safety-related control systems (SRCS) such KPIs should be evaluated in life cycle. In publication (Kosmowski & Gołębiewski, 2019) several categories of KPIs have been distinguished. Following KPIs for the safety-related systems have been proposed regarding scope of functional safety standards:

Basic process control system (BPCS):

- Mean time to failure (MTTF),
- Mean time to repair / restoration (MTTR),
- Mean time to spurious operation failure (MTTFS) of subsystems,

Alarm system (AS):

- Alarming rates in normal operation per day (maximum and average),
- Number of alarms following an upset situation per hour,
- Number of alarms following an upset situation per 10 minutes,
- Percentage of hours containing more than 30 alarms.

Safety Instrumented System (SIS):

- The number of demands on the SIS,
- The time intervals of partial and overall testing of redundant SIS,
- The number of failures of channels on tests in redundant SIS per month and year,
- Spurious operation rate of the SIS channels per month and SIS in year,
- Safe failure fraction (S_{FF}) for a channel of subsystem in the safety-related system.

The safety integrity level (SIL) is determined for consecutive safety functions based on results of the risk evaluation (Kosmowski, 2020, 2021). The SIL is then verified for the SRCS in which given safety function is implemented, based on the results of the probabilistic modelling of safety-related systems for relevant operation mode: high demand/continuous mode (HDM) or low demand mode (LDM).

5. Conclusions

Governing the operational resilience should be focused on getting a process up and running before abnormal situation causes an intolerable harm to the business, its customers, or the market. Thus, it should be considered as an extension of conventional business continuity management. Resilience capacity and its constituent elements have been discussed regarding the resilience engineering concept. The operational resilience research issues are discussed on example of converged technologies and communication networks: the operational technology (OT), information technology (IT) and cloud technology (CT). Importance of the industrial automation and control system (IACS) and the safety-related control systems (SRCS) is emphasized. The operational resilience governing are discussed on example of the functional safety and cybersecurity management in life cycle. The OT-IT-CT comprising the computer systems and networks are considered as interdependent infrastructure systems.

It is suggested to undertake additional research works related to the workshop that could include:

- Operational resilience models oriented on the cyber physical systems (CPS) regarding cognitive aspects of human behavior and the cognitive resilience engineering (CRE) concepts and precepts,
- Evaluation of human factors from the CPS perspective regarding HIL (human in the loop) and human reliability analysis methods in context of human system interfaces (HSI) including the alarm system (AS) concept using AI algorithms within the decision support system (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 for Industry 5.0 solutions,
- Benefits and risks of applying OPC UA protocols and other advanced protocols within distributed OT-IT-IT systems and networks,
- Categorizing and governing the operational resilience of interrelated defense in depth (DinD) systems.

Acknowledgements

The study outlined in this paper has been elaborated within individual research activity supported by the Polish Safety and Reliability Association as organizer of the SSARS conferences.

References

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

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 https://doi.org/10.1017/pds.2022.186.

ESDN. 2022. European Recovery and Resilience Mechanisms – Challenges in Systemic Approaches in Sustainable Development", ESDN Report, May 2022, ESDN Office, Vienna.

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.

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., 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. June 2020, www.isa.org/ISAGCA.

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 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 9001. 2015. Quality management systems. Requirements. 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 sustain-able 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. 2022. Information Technology – Security Techniques – Information Security Management Systems – Requirements. Geneva.

ISO/IEC 27005. 2022. Information Technology - Security Techniques – Information Security Risk Management. Geneva.

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. 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. In: Handbook of Advanced Performability Engineering (Ed. K.B. Misra), 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.). Safe-ty and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2022. Gdynia Maritime University, Gdynia, 117–132.

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.

Kosmowski, K.T. 2023. Operational resilience regarding safety and security aspects of industrial automation and control systems. In Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar, 99-116.

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.

Noggin. 2023. Operational Resilience Versus Business Continuity: What's the difference? www.noggin.io.

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.

Rieger, C.G. 2013. Resilient Control Systems - Practical Metrics Basis for Defining Mission Impact. DOE Idaho Operations Office Con-tract 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.

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