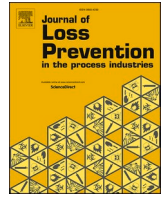



Contents lists available at [ScienceDirect](https://www.sciencedirect.com)

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

Convergence of safety and security within process plants

David Rehak^{a,*} , Alena Splichalova^a, Tomas Lovecek^b, Martin Hromada^c, Simona Jemelkova^a, Alena Oulehlova^d^a VSB – Technical University of Ostrava, Faculty of Safety Engineering, Lumirova 13, 70030, Ostrava, Czech Republic^b University of Zilina, Faculty of Security Engineering, 1. maja 32, 01026, Zilina, Slovakia^c Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stranemi 4511, 76005, Zlín, Czech Republic^d University of Defence, Faculty of Military Leadership, Kounicova 65, 66210, Brno, Czech Republic

ARTICLE INFO

Keywords:

Process plants

Safety

Security

Physical protection system

Organizational resilience

ABSTRACT

Process plants safety is currently an integral part of process industries. This fact is evidenced by a number of important directives, standards, and regulations, such as the Seveso III Directive, Process Safety Management Standard or Occupational Health and Safety Management Systems. By implementing them, personnel safety, process safety, functional safety, etc. are constantly ensured. However, on the other hand, it is necessary to point out that process plants can be a significant source of risk not only from a process point of view, but also as a result of intentional or unintentional external damage. In this context, it is also necessary to pay attention to process plants security. Currently, only a few directives related to the critical infrastructure protection or cyber security pay attention to this area. Based on these facts, the aim of the article is to present possibilities, tools and benefits of the convergence of process plants safety with the physical protection system and organizational resilience. As part of the physical protection system, convergence mechanical barriers, alarm systems, security forces and regime measures can be used for this purpose at the operational level. In contrast, organizational resilience processes can be used to strengthen process plants safety at the management level. In both cases, these security measures can be used in all three-time phases of the accident, i.e. before the accident, during the accident, and after the accident.

1. Introduction

Process plants are an integral part of modern times. Through process plants, basic human needs are provided, i.e. produce a number of important products for everyday use. Process plants include a wide range of processes that transform input raw materials or semi-finished products into a final product or intermediate product (Schlegel, 2023). It is a complex set of process units, modules, supporting infrastructure, operations and processes systematically arranged to provide operational functions related to the creation of the final product (Moran, 2019; Varbanov, 2023). They can also be defined as a complex set of process management, e.g. planning of manufacturing activities, planning assembly, work methods using any process equipments for the transformation of any materials (Gersak, 2022). It is clear that process plants are perceived as one of the key sectors that has a major impact on the global economy, sustainability and technological progress.

Process plants are used for the processing of various materials. Their final products always reflect the industry types in which the process plants are used. Process plants are used in industries such as the food, chemical, metalworking, engineering, metallurgical, textile or other production sectors. These sectors and the way products are processed must adapt to current challenges and rapidly changing technological, economic and environmental conditions, as well as consumer demands. These changes have a significant impact not only on the approach to the choice of technology, the assembly of process equipment (Schindel et al., 2021), implementation of process chains (Qin, 2015) or the introduction of automation systems (Wilson, 2015), but also on process plants safety (Hauptmanns, 2020).

When introducing any change, increased attention must be paid not only to the technical or economic areas, but also to safety (Moran, 2019). This safety must also be ensured during the normal operation of process plants, which is covered by a number of important guidelines,

This article is part of a special issue entitled: Safety Engineering published in Journal of Loss Prevention in the Process Industries.

* Corresponding author.

E-mail address: david.rehak@vsb.cz (D. Rehak).

<https://doi.org/10.1016/j.jlp.2025.105579>

Received 31 October 2024; Received in revised form 31 January 2025; Accepted 4 February 2025

Available online 5 February 2025

0950-4230/© 2025 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC license (<http://creativecommons.org/licenses/by-nc/4.0/>).

standards and regulations. An example is the Seveso III Directive (2012/18/EU), Process safety management standard (OSHA, 2013), or Occupational health and safety management systems (ISO 45001:2018). However, Safety cannot be understood as a separate field. It is a systematically connected, interconnected and comprehensive system of measures (Roland and Moriarty, 1990), which are integrated into process plants. Based on this fact, integral process plants safety is composed of three basic areas, which are personnel safety, process safety, and functional safety (Hauptmanns, 2020; Véchet et al., 2022; Kallambettu and Viswanathan, 2018; Majid et al., 2015; Mannan et al., 2015).

In addition to safety, security is also important for the functioning of process plants. This is mainly applied in the areas of physical security (Williams, 2021), information security (ISO/IEC 27001:2022), and cyber security (Edwards, 2024). Initially, these areas of security were dealt with separately, but since 2007, with the support of the Alliance for Enterprise Security Risk Management (AESRM), their gradual convergence began to occur. Security convergence has been defined in this context as “the integration of the cumulative security resources of an organization in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings” (Tyson, 2007).

Based on the above, the aim of the article is to define the possibilities, tools and benefits of the convergence of safety and security within process plants. This security and safety convergence consist in strengthening process plants safety through the factors of physical protection system (for the operational level) and organizational resilience (for the management level). For this purpose, the article defines both security systems and subsequently defines their factors that are suitable for strengthening process plants safety through this convergence.

The article is logically divided into two main parts, i.e. Background, materials and methods, and Results. The first part is devoted to the importance of safety and security convergence for process plants and at the same time the current shortcomings that can be seen in this system are mentioned. Subsequently, both key security systems, i.e. the physical protection system and organizational resilience, are defined in detail, and their basic factors are described. The second part presents how these factors can be used to strengthen process plants safety, at two key levels, i.e. operational and management.

2. Background, materials and methods

The essence of the article is the presentation of safety and security convergence possibilities as a tool for strengthening process plants safety. For this purpose, attention is first focused on the current development in the field of safety and security convergence. Subsequently, a description of the physical protection system and organizational resilience is presented as approaches suitable for strengthening process plants safety at the operational and management level.

2.1. Safety and security convergence

The beginnings of the application of the converged approach are visible primarily in the field of security. Converged security is a term that refers to the merging of several hitherto separately existing types of security into one unit with a wider scope (Aleem et al., 2013). It is a fusion of the basic types of security, which are close to each other and may have a common partial intersection of controls, hazards and assets. There are several different opinions on the definition of converged security and determining its meaning. However, the most discussed are the mutual relations between physical, information and cyber security, which are based on the need to solve current real situations (Lukas, 2019; McCreight and Leece, 2016; Hromada et al., 2021, 2023).

The security and safety areas convergence may seem quite complex, but in practice it is already partially happening. It is a so-called integrated management system that integrates security management

systems and safety management systems and is framed by international standards of organizations such as the International Organization for Standardization or the International Electrotechnical Commission. From quality improvement to energy efficiency and environmental performance to road safety, management systems are increasingly used as a result of increasingly complex operating conditions. There are a significant number of management systems in the portfolio of ISO standards. Many of these standards are focused on various areas of security and safety, such as quality management systems (ISO 9001:2015), environmental management systems (ISO 14001:2015), occupational health and safety management systems (ISO 45001:2018), information security management systems (ISO/IEC 27001:2022), business continuity management systems (ISO 22301:2019), energy management systems (ISO 50001:2018), asset management systems (ISO 55001:2024), management system for private security operations (ISO 18788:2015), security management systems (ISO 28000:2022), whistleblowing management systems (ISO 37002:2021).

The number of management systems has increased significantly in recent years, reflecting the growing needs and requirements of organizations that want to improve their performance in various areas and sectors. At the same time, many companies implement several of these systems. For this reason, the ISO Handbook: The Integrated Use of Management System Standards was published in 2018 (ISO, 2018), which provides guidance to organizations on how to integrate individual management systems. The common features of individual management systems is that they are built on risk management in addition to process management (ISO 31000:2018; IEC 31010:2019; ISO/TS 31050:2023).

The above-mentioned standards issued by international organizations are non-binding for individual member state organizations. For this reason, generally binding legal regulations are also issued at the level of the EU and member states, which in some cases regulate safety requirements in areas that have a significant impact on the functioning of states, the environment and, last but not least, on the life, health and property of citizens (2012/18/EU; 2022/2555; 2022/2557; 2016/679).

The security and safety areas convergence at the level of EU regulations and directives is similar to the case of managerial ISO systems. In many cases, the issue of physical security is absent. For example in Seveso III Directive (2012/18/EU) and its implementation methodologies (e.g. ARAMIS: Accident Risk Assessment Methodology for Industry) exclusively take into account safety hazard, such as technological accidents or unintentional human factor failure. However, procedures regarding physical security hazard are completely absent here.

2.2. Physical protection system

A security management system is a system of coordinated policies, processes and procedures through which an organization manages its security objectives (ISO 28000:2022). One of the key tools of this system is the physical protection system. According to Lovecek et al. (2018) physical protection system, as a purposeful method of organizing protective measures, makes it possible to prevent a purposefully acting unauthorized person from achieving his goal, which may be the theft, damage or destruction of a protected interest. According to (Garcia, 2008) the physical protection system is perceived as a system realized by mechanical barriers, alarm systems, security forces and regime measures (see Fig. 1).

Mechanical barriers are used to deter, slow down or stop an intruder, while alarm systems are used to subsequently detect an intruder/attacker and trigger an alarm. Alarm systems include electronic security systems and emergency alarm systems (EN 50131-1:2006), video surveillance systems (EN 62676-1-1:2014), electronic access control systems (EN 60839-11-1:2013), social alarm systems (EN 50134-1:2002), or alarm transmission systems and equipment (EN 50136-1:2012). An integral part of the protection system are the security forces, which ensure timely intervention and detention of the intruder. Mode protection ensures the correct functioning of the mentioned protective

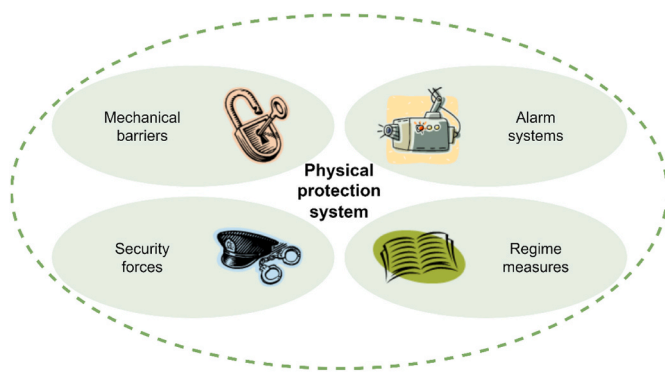


Fig. 1. Physical protection system elements.

measures (Lovecek and Reitspis, 2011). These protective measures must be arranged in such a way as to meet the basic requirement for system functionality.

In the phase of planning, designing and implementing these measures, from the point of view of their assessed, we can talk about the functionality, effectiveness and reliability (i.e. overall quality) of the protection system (Lovecek et al., 2015). From an economic point of view, the effectiveness of the system can be defined as the return of funds invested in the system and assessed in terms of its results. The economic effectiveness of the physical protection system can be defined as a relationship that, using economic indicators, expresses the dependence between the economic benefits of the system's effect on reducing economic losses due to criminal activity and the economic costs of its creation.

System reliability is characterized by its complex property, expressing the general ability to maintain functional properties at a given time and under specified conditions (Lovecek et al., 2015). Reliability is usually expressed as the probability that the system (e.g. electrical security system, camera surveillance system) or its element (e.g. detector, control panel, communicator) will perform the required function for a specified time and under predetermined conditions. In practice, reliability is stated as the number of failures per unit of time during the monitored period (Wilde et al., 2008). In many cases, the reliability of a physical protection system also depends on the reliability of a human agent, e.g. a guard service worker, a surveillance centre operator.

The quality of physical protection system can be in the context of quality management system (ISO 9001:2015) perceived as the sum of the factors of the entire system, which make it capable of satisfying the legitimate and anticipated needs of a specific entity (e.g. owner, operator, administrator) and thus ensure security the given environment, time and for the specified purpose.

The search for optimal protection means the search for a solution that would be reliable, economically efficient and at the same time meet the requirements of a functional physical protection system. A functional physical protection system is considered to be such a system that meets the basic condition that, from the moment of detection, the attack time is greater (including the total time to break through the passive protection elements and the intruder's movement time) than the reaction time of the intervention unit. This means that the system is efficient if the ratio of times is greater than one (Garcia, 2008).

Credible proof of fulfilment of this basic and seemingly elementary condition for system functionality is often difficult to achieve in practice. Existing practices (e.g. standards, norms, methodologies, guidelines, etc.) aimed at protecting objects use one of two basic approaches, namely a qualitative approach or a quantitative approach.

Procedures using a qualitative approach are based on expert estimates of assessors, where it is not possible to exactly verify the sufficiency of the proposed level of protection, and one must rely on the professional competence of the creators of these procedures. In this case, it is not possible to verify whether the protection system from the point

of view of the proposed protective measures is not under-dimensioned or, on the contrary, over-dimensioned (CEN/TS 14383-3:2005; CEN/TS 14383-4:2006; CEN/TS 14383-6:2022; CEN/TS 16850:2015).

Procedures based on a quantitative approach make it possible to accurately prove the validity of the proposed protective measures using measurable input and output quantities. In this case, it is already possible to verify whether the protection system, from the point of view of the proposed protective measures, is not undersized or oversized (Bennett, 1977; Matter, 1988; Garcia, 2008; Phillips et al., 2005; Jang et al., 2009; Lovecek et al., 2010).

The quantitative approach is the least subjective, but at the same time the least used in practice. The main reason is the fact that the existing software tools (e.g. SAVI, SAVI/ASSESS from Sandia National Laboratories, USA) were created to assess the protection of specific non-commercial devices (e.g. nuclear facilities and military facilities) and are not available for civil or unclassified sectors. However, another important reason is also the fact that in practice there is a lack of real values of input quantities, such as (Garcia, 2005; Vintr et al., 2012):

- breakthrough resistance of passive protection elements changing depending on the used type of tool expected to overcome them;
- the probability of detection of active elements of protection changing depending on the intruder's knowledge of the technologies used, e.g. the method of evaluating a change in a physical quantity as a result of a violation of the protected space;
- reliability of active protection elements;
- the reliability of the human factor.

For these reasons, the mentioned tools are used in practice only for a specific area, e.g. the protection of nuclear facilities. In practice, procedures based on a qualitative approach are used much more often, which can be further classified into (Lovecek and Reitspis, 2011):

- a directive approach, where protective measures are precisely defined, regardless of the specifics of operation and the environment in which the object is located;
- a variant approach, where it is possible to choose from a finite number of proposed solutions, combining various protective measures, which will make it possible to consider to a certain extent not only the specifics of operation and the environment, but also the financial, technical or personnel possibilities and capacities of the owner or manager of the object.

The first and most important step in the process of planning and designing an object's protection system is the determination of the minimum level of protection, from which the choice of technologies of active and passive protection elements, dislocation, parameters and functionalities is subsequently derived (EN 16763:2017). The minimum protection level determines which protective measures are to be implemented, in what proportion and with what characteristics, e.g. security level/class, purpose of use, key parameters of system elements, dislocations.

The minimum protection level results from security requirements, which can be defined either by the basic condition for the protection system functionality or by third parties, e.g. the state, standardization authority, insurance company, customer, parent company. In the case of determining the minimum protection level based on the fulfilment of the basic condition for the functionality of the protection system, a quantitative approach is used, which uses the time and probability bases of the values of input and output quantities, e.g. breakthrough resistance times, transfer times and reaction times, detection probabilities (Garcia, 2005, 2008; Godovykh et al., 2016; Wely and Chetaine, 2021). In the case of determining the minimum protection level based on the fulfilment of the security requirements of third parties, a qualitative approach is used in most cases, either a directive or a variant approach.

Physical protection system can be used not only as a measure to

reduce the risk level arising from intentional anthropogenic hazard, but also risks arising from hazard that have a technological, environmental or unintentional anthropogenic origin. For this reason, it is advisable to investigate the possibilities of using a physical protection system in the area of process plants safety. Such an approach can have an impact on more effective investment in increasing the protection of not only the life and health of employees, but also the assets of the organization.

2.3. Organizational resilience

The second important area that can contribute to the safety and security convergence within process plants is organizational resilience. It is evident from the first definitions that organizational resilience was first perceived only as “*the adaptive capacity of an organization in a complex and changing environment*” (ASIS, 2009). In the following years, it was already expanded with the capacity of absorption: “*Organizational resilience is the ability of an organization to absorb and adapt in a changing environment*” (ISO 22316, 2017). Currently, organizational resilience is perceived in a significantly broader context, as “*the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper*” (BS 65000, 2022).

The current perception of organizational resilience reflects its development. The standard known as ASIS SPC.1 became the default publication (2009), which provides a comprehensive approach to strengthening resilience in the areas of security, preparedness, and continuity management systems. In accordance with the requirements of the management system, organizational resilience is strengthened in four phases, i.e. planning, implementation, operation, and checking (evaluation). Another important document is the technical standard ISO 22316 (2017), which focuses not only on the area of strengthening resilience, but also on the adaptation phase, i.e. the ability to adapt to changes, challenges and crises. Based on this fact, the main attributes of organizational resilience are considered adaptability and flexibility, speed of recovery, use of information, availability of resources, identification and risks management, ability to anticipate and managing change, planning and implementation, improvement of processes or skills diversity, leadership, knowledge and experience. The last major standard closely linked to the concept of organizational resilience is BS 65000 (2022) providing more detailed information on strategic resilience management. This standard emphasizes long-term preparedness and adaptability to changes, through aspects such as leadership and management, protection and continuity, preparedness for hazards and adaptation, a comprehensive approach to risks or a safety culture.

Over the past twenty years, a large number of professional publications have also been devoted to the issue of organizational resilience. Here, too, the concept of organizational resilience has undergone significant development and various approaches and strategies have been identified. This statement is substantiated by, for example, Denyer (2017), who, in his book, identified specific requirements that are key to properly setting up organizational resilience. These requirements are foresight (anticipate, predict and prepare for your future), insight (to interpret and respond to your present conditions), oversight (monitor and review what has happened and assess changes), hindsight (learn the right lessons from your experience).

In recent years, research on organizational resilience, i.e. determination of factors and their assessment, has become an increasingly frequent subject of interest in professional literature. This statement is also evidenced by the existence of many methods that are focused precisely on the identification of factors and the subsequent assessment of their level. An example is the ASOR method (Rehak, 2020), in which the factors of risk management, education and development processes, and organizational innovation processes are used to strengthen organizational resilience. It is also possible to increase organizational resilience through managerial disciplines, such as business continuity/continuity of operations management, crisis and risk management, human resource management, or incident response (ICOR, 2024). Each of these

disciplines is designed as a system that must be integrated into the overall framework for the organization to effectively respond to hazards and adapt to change.

Based on the approaches presented above, it is possible to define factors determining organizational resilience. It is appropriate to classify these factors according to their purpose into three basic groups, which are designated as components of organizational resilience. These components are resistance, robustness and adaptability. The essence of resistance is the anticipation and preparation of the organization for gradual changes and sudden disruptions (i.e. the prevention phase). The essence of robustness is the organization's response to gradual changes and sudden disruptions (i.e. the response phase). The essence of adaptability is the adaptation of the organization to gradual changes and sudden disturbances (i.e. the adaptation phase). The classification of factors into individual components is presented in Fig. 2.

The first factor determining organizational resilience in the prevention phase is risk management. It is an internal process of the organization consisting in the coordination of activities with the aim of minimizing risks (ISO 31000, 2018). The level of this factor is shaped by the level of risk management, the risk assessment methodology used, the scope of implementation of safety standards and the level of risk scenarios specification (Rehak, 2020; Bernatik et al., 2013).

Another preventive factor is anticipation. These are procedures and measures related to predicting the occurrence of incidents (ISO 22316, 2017; BS 65000, 2022). This factor includes preventive control activities and the process of indicating disruptions to organizational resilience.

The third factor determining resistance is security measures. These are regime and organizational measures for monitoring, physical and cyber protection of the organization. This factor primarily includes physical protection and regime measures (Kampova et al., 2020).

The last preventive factor is crisis preparedness. These are analytical and planning documents that serve to increase the organization's preparedness for incidents (Carmeli and Schaubroeck, 2008). This factor consists in defining responsibilities, duties and authorities, training staff, preparing planning documentation and continuity planning.

The first factor determining organizational resilience in the response phase is the organization's responsiveness to an incident. These are organizational procedures and measures, the essence of which is the reporting and management of incidents. For this purpose, a short time interval for the protective measures activation and an adequate state of forces and means to manage incidents are important (Rehak et al., 2024a).

The second factor is incident management. Its essence is managing incidents that have already occurred and minimizing their impact on the organization (ASIS, 2009). Incident management is based primarily on the capabilities and skills of crisis management and a set system of communication and information sharing.

Another factor determining the robustness of the organization is business continuity management. The essence of this factor is the creation of an environment and procedures that will allow to ensure the continuity and recovery of key processes and activities of the organization, at a predetermined minimum level, in the event of their disruption or loss (ISO 22301:2019; ICOR, 2024).

The final factor of the response phase is recovery processes. This factor lies in the disaster preparedness of processes that control or deal with material resources, financial resources/reserves and human resources. This is an process assessment of securing these resources for the restoration of the organization's function from the point of view of crisis preparedness and preparation for repeated incidents (Mohan, 2023).

The final component of organizational resilience is adaptability. The first factor of this component is the educational and development processes that shape the knowledge, skills and attitudes of the organization's employees (Armstrong and Taylor, 2014). These processes are determined by the scope and quality of professional training, the training level to deal with incidents and the assessment of the effectiveness of these training and development processes.

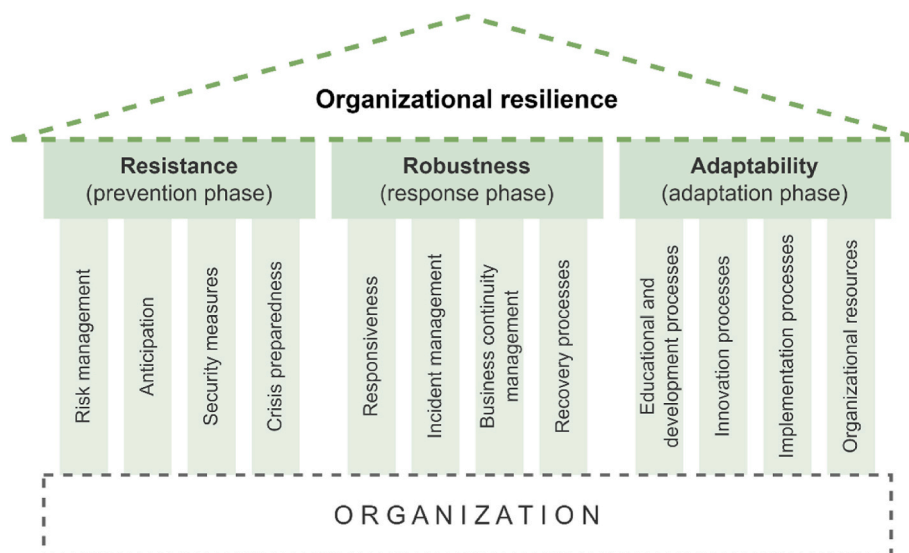


Fig. 2. Classification of components and factors of organizational resilience.

The second factor of the adaptation phase is innovation processes, which significantly contribute to strengthening organizational resilience. The essence of these processes is the support of inventions, science and research and the implementation of safety measures. This support should be directed primarily to the area of facilities, processes, products, marketing and organizational activities (OECD/Eurostat, 2005).

Another important factor is the implementation processes that enable the implementation of tools to strengthen organizational resilience (ASIS, 2009). This is mainly the implementation of new processes, the implementation of management systems, the implementation of software tools and the implementation of security measures.

The last factor determining the adaptability of an organization is its resources. These resources can be classified as financial, human and material and their availability has a significant impact on the effectiveness of the organization (Mwai et al., 2018). In the case of financial resources, their allocation and timeliness are important. In the case of human resources, their capacity, expertise and time availability are particularly important. In the case of material resources, the availability of components needed to carry out repairs or replacement of damaged or destroyed parts of the infrastructure is important.

In conclusion, it can be stated that both organizational resilience and physical protection system are important tools contributing to the safety

and security convergence. In this context, it is appropriate to focus attention on the possibilities of their use to strengthen process plants safety, both at the operational and management level. International standards play a significant role in this convergence, contributing to varying degrees to strengthening safety and security in different areas (see Fig. 3).

In the context of process plants, the area of safety management systems can be considered primarily occupational health and safety management systems (ISO 45001:2018), environmental management systems (ISO 14001:2015), energy management systems (ISO 50001:2018), or social alarm systems (EN 50134-1:2002).

In contrast, the area of security management systems is represented by organizational resilience (BS 65000:2022; ISO 22316:2017), security management systems (ISO 28000:2022), management system for private security operations (ISO 18788:2015); information security management systems (ISO/IEC 27001:2022), crime prevention standards (CEN/TS 14383-6:2022; CEN/TS 14383-4:2006; CEN/TS 14383-3:2005), or other standards dealing with alarm systems, such as electronic security systems and emergency alarm systems (EN 50131-1:2006), video surveillance systems (EN 62676-1-1:2014), electronic access control systems (EN 60839-11-1:2013).

Converged management systems can be considered business

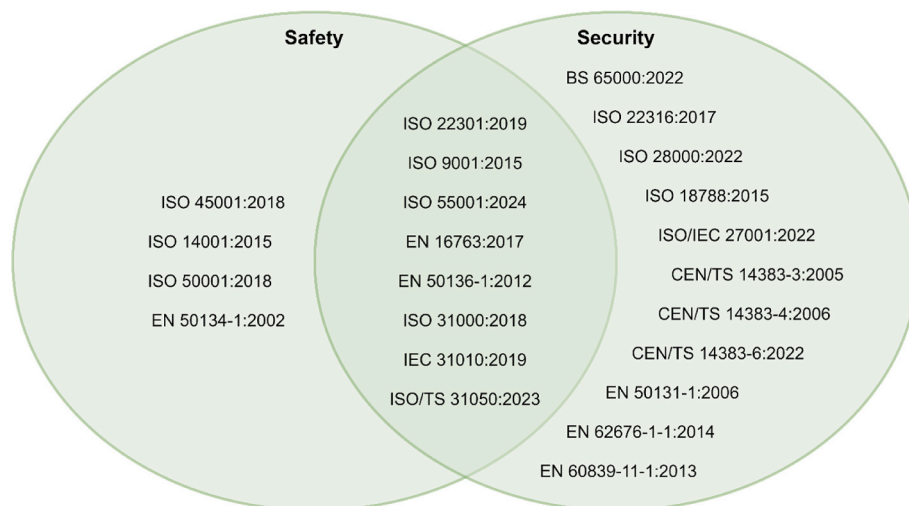


Fig. 3. Management system standards suitable for convergence of safety and security within process plants.

continuity management systems (ISO 22301:2019), quality management systems (ISO 9001:2015), asset management systems (ISO 55001:2024), services for fire safety systems and security systems (EN 16763:2017), alarm transmission systems and equipment (EN 50136-1:2012), or some standards dealing with risk management (ISO 31000:2018; IEC 31010:2019; ISO/TS 31050:2023).

3. Results

From the text so far, it is clear that the main attention in protecting the life and health of process plants employees is primarily devoted to the area of safety. This fact is evidenced by a number of important directives, standards, and regulations, such as the Seveso III Directive (2012/18/EU), Process safety management standard (OSHA, 2013), or Occupational health and safety management systems (ISO 45001:2018). However, the authors present a solution within which some process plant safety measures (primarily personnel safety, process safety, functional safety) could be strengthened through convergence with specific security measures (see Fig. 4).

These security measures are physical protection system and organizational resilience. Physical protection system and its factors are suitable for strengthening process plants safety at the operational level. In contrast, organizational resilience and its factors are suitable for strengthening process plants safety at the management level. The factors of both security measures can be used to strengthen process plants safety in all three phases of an accident, i.e. before an accident (i.e. minimizing risks and increasing preparedness), during an accident (i.e. managing the consequences of an accident and monitoring the development of the situation) and after an accident (i.e. monitoring changes in process plants and strengthening safety).

3.1. Convergence of the physical protection system to strengthen the process plant safety at the operational level

In the past, security and safety were considered separate areas that solved local security problems in organizations. From the point of view of security, physical security is the oldest and most widespread area, which was expanded over time by other specific areas, such as personal security or administrative security. Later, with the development of information systems, information security began to be promoted end masse (ISO/IEC 27001:2022). With the development of computer networks and the increasing occurrence of various types of cyber-attacks, the importance of cyber security has begun to be emphasized (ISO/IEC 27032:2023), which is a specific area of information security. For a long time, cyber security was the domain of information technologies based on TCP/IP protocols. However, cyber security is now extending into operational technologies such as industrial control

systems and manufacturing technologies (ISO/IEC 27019:2017; IEC 62443-3-2:2020).

In recent years, there has already been a trend to solve the physical and information security of organizations as a set of optimized solutions suitable for a given object, which consists in merging them into a single resulting security convergence (Lukas, 2017). Security convergence refers to the convergence of two historically different security functions, physical security and information security, which are an integral part of a coherent risk management program. Security convergence is motivated by the knowledge that corporate assets are increasingly information-based. Although security convergence is generally used in connection with cyber and physical convergence, in its essence it can also refer to the convergence of security and specific safety areas.

3.1.1. Strengthening personal safety

Convergence of the physical protection system to strengthen process plants safety can be implemented at the operational level in three basic safety areas, i.e. personnel, process, and functional. In the field of personal safety, mechanical barriers, alarm systems, security forces and regime measures can be used for this purpose. Mechanical barriers are considered standard protective measures that clearly contribute to increasing occupational health and safety. These are, for example, permanent or mobile barriers, back pressure barriers, hole fillings with increased back pressure and chemical resistance (EN 356:1999; EN 13124-2:2004). From the point of view of the individual phases of the accident, mechanical barriers serve to minimize risks, primarily from the point of view of reducing the probability of an incident occurring. In the event of an accident, they make it possible to protect a person from the consequences of the event from the point of view of protecting his life and health.

In operation, it is often not possible due to layout reasons to install mechanical barriers to prevent access of people to individual process plants. For this reason, alarm systems are key elements for strengthening process plants safety (EN 50398-1:2017). These systems include electronic security systems and emergency alarm systems, video surveillance systems, electronic access control systems or emergency call systems. The effectiveness of individual alarm systems depends on the type of operation and mode of movement of people and property in operation. The primary function of alarm systems is the detection of unauthorized access to a protected area. Security systems and emergency alarm systems can be effectively used here, the task of which is to detect and indicate the presence of an intruder (EN 50131-1:2006).

Depending on the type of process plants, spatial, directional, point or line motion detectors can be used (Lovecek et al., 2015). Motion detectors usually have a detection characteristic determined by the manufacturer depending on the technology used. Space detectors are used to cover a certain space, e.g. a zone in a given space. Directional

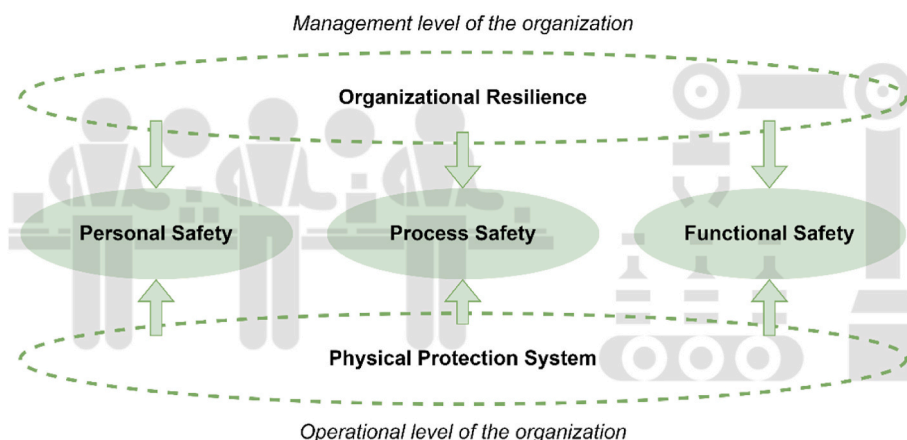


Fig. 4. Convergence of process plants safety with physical protection system and organizational resilience.

detectors sense a change of state only in a certain direction, e.g. in a part of a room, in a corridor, in front of a door. Point detectors sense a change of state at just one point, e.g. a microswitch. Line detectors sense the change of state between two points, i.e. receiver and transmitter. The very operation of process plants creating various disturbing influences (e.g. temperature, sound, magnetic fields, etc.) can influence the choice of technology. Passive detectors sense physical changes in their surroundings (e.g. temperature) and based on them evaluate the disturbance. Active detectors create their own working environment by actively acting on their surroundings and detect changes in the physical environment created in this way, e.g. microwave, ultrasonic, or dual detectors.

Surveillance video systems can also provide detection and indication of the presence, entry or attempt to intentionally or unintentionally enter a protected area (EN 62676-4:2015). Currently, the standard functions of security cameras include video detection of the entry of an unauthorized person into the protected area, or monitored space. The detection in this case is not caused by a change in any of the physical quantities, but is caused by a change in the bitmap raster of the recorded image of the scanned scene. Regardless of which alarm system is used to detect unauthorized movement of people in a protected area, in addition to detection, a certain form of response to an alarm condition must also be ensured. In the case of a security application, it is about notifying the person that he is unintentionally moving in a space in which he should not be. Here, several technical solutions can be used to notify her, ranging from local acoustic-optical signalling, through notification of personal mobile devices she carries, to voice notification from the surveillance and alarm reception centre operated by the guard service.

From the point of view of personal safety, alarm systems can also be used to detect changes in the environment, and not only the already mentioned changes in temperature, but it is also possible to monitor, detect and understand other changes in the properties of the environment, such as changes in the chemical composition of the air. The use of alarm systems can therefore be included from the point of view of the individual phases of the accident, as well as mechanical barriers, among measures to minimize risks.

3.1.2. Strengthening process safety

To strengthen process plants safety at the operational level in the area of process safety, the physical protection system can again be used in several applications. For this purpose, it is possible to use any of the alarm systems, especially video surveillance systems and electronic access control systems. In this case, however, it is not about their use to detect the unauthorized movement of persons in a protected area, but about monitoring and tracing of persons in the given area.

The purpose of such monitoring and tracing is whether the person is following the established work procedure. In the case of the use of surveillance video systems, it must be considered that standard video detection is no longer sufficient, but security cameras using intelligent video analytics functions must be used. These functions, based on machine learning, make it possible to evaluate not only the presence of a person in the monitored space, but also their behaviour. The disadvantage of the implementation of surveillance video systems for monitoring and tracking people is the need to ensure sufficient coverage of the space with the detection characteristics of the cameras at the reconnaissance level (EN 62676-4:2015) and also the fact that the purpose of use may be in conflict with personal data protection regulations (Regulation, 2016).

In the case of electronic access control systems, multiple technologies can be used depending on the application. Current location or monitoring systems represent a combination of several technologies that allow monitoring the movement of various people or objects in the internal and external spaces of the organization (Lovecek et al., 2023). This is, for example, Global Position System (GPS), Radio-frequency identification (RFID), Near-Field Communication (NFC), Bluetooth Low Energy (BLE), or QR codes. All these technologies have certain operating limits. At the same time, however, most of these technologies

are suitable for localization in external and internal environments.

GPS technology can be used in an environment that is covered by a signal. However, indoor use is often limited due to the impermeability of signals through building structures or natural terrain. BLE, RFID and NFC technologies can be implemented especially in the interior of buildings. Some of the technologies have a limited range within which the transmitting and receiving devices are able to communicate with each other. Technologies such as NFC or QR codes can be characterized as short-range technologies. While RFID technology allows devices to receive transmitted signals up to a distance of 50 m. In terms of localization, RFID, NFC, and QR codes only provide information about the presence or absence of an entity (person or object) in a given space. Monitoring is possible based on information about the time and place of presence of the entity in the given premises. This requirement can be implemented using BLE technology, but it is not possible to determine the movement of the entity in space. Even NFC and QR codes do not allow locating more people and entities.

From the point of view of the individual phases of an accident, alarm systems serve not only to minimize risks (primarily to reduce the probability of an accident), but also to monitor changes in process plants and strengthen safety after an accident (retrospective analysis of events in order to optimize processes during the restoration of operations).

3.1.3. Strengthening functional safety

Last but not least, the physical protection system can be used to strengthen process plants safety at the operational level in the field of functional safety. As in the area of process safety, it is possible to use surveillance video systems and electronic access control systems again, but it will no longer be a matter of monitoring and tracing non-standard behaviour of people, but of non-standard behaviour of technological devices. In this case, in addition to the above-mentioned technical solutions, thermal imaging cameras can also be used as part of video surveillance systems, which will allow to evaluate whether process plant components are overheating.

In the context of individual phases of an accident, alarm systems can be used both to minimize risks in the pre-accident phase (e.g. to monitor the escalation of a problem by monitoring the deviation of a physical quantity from a set value level) and during an accident, specifically to monitor the development of the situation.

3.2. Convergence of organizational resilience to strengthen the process plant safety at the management level

Similar to the case of the physical protection system, the convergence of organizational resilience can also be used to strengthen process plants safety. In this case, however, it is about strengthening safety at the management level, where individual areas (i.e. personnel, process, and functional) are strengthened preferentially in the context of emergency phases, i.e. before an accident, during an accident and after an accident.

3.2.1. Strengthening process plants safety before the accident

Strengthening process plants safety before an accident can be implemented primarily through preventive measures used to minimize risks and increase preparedness. In the context of organizational resilience, these are factors determining the organization's resistance. These factors are risk management, anticipation, security measures and crisis preparedness.

As part of risk management, process plants safety can be strengthened through processes aimed at early risk assessment and management, including detailed specification of scenarios. Specifically, it is about setting the appropriate level of risk management (ISO/TS 31050:2023), choosing an appropriate risk assessment methodology (IEC 31010:2019), implementation of related technical standards (e.g. ISO/IEC 27001:2022; ISO 45001:2018; ISO 12100:2010) or accident modelling using modern technologies, e.g. digital twins (ISO/IEC 30173:2023; ISO 23247:2021; Brucherseifer et al., 2021).

Process plants safety can be further strengthened through anticipation, the essence of which is the prediction of the occurrence of an accident due to the action of a hazard. For this purpose, it is advisable to carry out regular preventive checks in order to obtain feedback on employee awareness and the current state of production facilities and processes (Denyer, 2017). The information resulting from the process of indicating the disruption of the organization's resilience can also be used to predict the occurrence of an accident (Rehak et al., 2024b).

Another important factor in strengthening process plants safety are security measures. These measures can be used in two areas, namely for physical and cyber protection. In the area of physical protection, these are primarily regulatory measures to control the entry and entry of people and vehicles into the area of process plants (Lovecek and Reitspis, 2011). In the field of cyber protection, these are regime measures for the systematic protection of electronic or printed data (ISO/IEC 27001, 2022).

The last factor suitable for strengthening process plants safety in the prevention phase is crisis preparedness, the essence of which is the preparation of workers and management of the organization for crisis situations. To increase the crisis preparedness of process plants, it is advisable to clearly define responsibilities, obligations and powers (ISO 9001, 2015), regularly implement training and staff training (ISO 9001, 2015) and assess the level of processing of safety documentation, especially the emergency plan (Philpott, 2016).

Every process plant is a potential source of risk, therefore it is necessary to reduce the probability of an accident to a minimum. For this purpose, it is possible to use, among other things, the preventive factors of organizational resilience. Risk management plays a fundamental role in hazard identification, safety assessment, safety analysis or estimation of process safety hazards. Risk management can also be used within the Safety Integrity Level (SIL) analysis (IEC 61508:2010). Anticipation and crisis preparedness, as proactive approaches to identifying weak points, can be used, for example, in process safety or process engineering. These factors can influence the development of processes, their effective design or optimization. On the other hand, security measures contribute to increasing personal safety by minimizing the risk of disrupting the operation of process plants as a result of hacker or terrorist attacks.

3.2.2. Strengthening process plants safety during the accident

Strengthening process plants safety during an accident can be implemented primarily through reaction measures used to manage the consequences of the accident and monitoring the development of the situation. In the context of organizational resilience, these are factors determining the robustness of the organization. These factors are responsiveness, incident management, business continuity management and recovery processes.

The responsiveness is determined by measures and procedures for detecting and handling incidents (Rehak et al., 2019). In this context, an adequate state of internal forces and resources, which are necessary to interrupt the causes and solve the effects of accidents in the production process, can contribute to the strengthening of process plants safety. A significant factor is also the short reaction time of these forces and means, which will ensure the timely activation of key protective measures leading to the minimization of losses.

Another important factor in strengthening process plants safety is incident management, the essence of which is the preparedness of crisis management and the system of communication and information sharing. Crisis management preparedness lies in the capabilities and skills of the organization's management in handling incidents (Carneli and Schaubroeck, 2008). An integral part of crisis management is a properly configured system of communication and information sharing, which serves to effectively resolve incidents (Savolainen, 2017).

Process plants safety can be further strengthened through business continuity management. It is the strategic and tactical capability of an organization consisting of the readiness and ability to respond to incidents and disruptions of the organization's activities in order to

continue at a predetermined acceptable level. Significant activities in this area are the development of business continuity management strategy, development and implementation of business continuity plans, and testing, maintenance and review of the entire process (ISO 22301:2019).

The last factor suitable for strengthening process plants safety in the final phase of an accident is recovery processes supporting the rapid restoration of the required performance of the process plant. These processes are the preparation of a disaster recovery plan and the time point of recovery of the process plant function. A disaster recovery plan includes an assessment of the level of processes that control or use material, financial and human resources in order to increase the technical efficiency of a given facility (Mohan, 2023). The key factor in restoring the function of the process plant is the time course of restoring performance after the incident has ended (Zorn and Shamseldin, 2015).

From the point of view of individual types of safety, the above-mentioned factors primarily contribute to the strengthening of personal and functional safety. In this context, it is possible to identify the organization's responsiveness and incident management as key factors. These factors ensuring immediate response and handling of accidents can be used, for example, to reduce the number of accidents or machinery, plant, and equipment safety. In contrast, business continuity management is directly intended to ensure the continuous operation of process plants and thus significantly influences the use of safety management tools for plant operations. Recovery processes subsequently ensure post-incident adaptation for future mitigation.

3.2.3. Strengthening process plants safety after the accident

Strengthening process plants safety after an accident can be seen as a phase of the organization's adaptation to past incidents. The essence of this phase is primarily the monitoring of changes in process plants and the implementation of measures to strengthen safety. In the context of organizational resilience, this phase is determined by adaptability factors, i.e. educational and development processes, innovation processes, implementation processes and organizational resources.

Education and development processes are the primary factor strengthening process plants safety in the area of adaptability. The essence of these processes is the development of knowledge, skills and attitudes of the organization's employees in the area of safety. Key activities are the scope and quality of professional education (Yamoah, 2014) and incident response training, including evaluation of its effectiveness (Rodriguez and Walters, 2017).

Another important factor in strengthening process plants safety are innovation processes. The essence of these processes is the support of invention, science and research for the implementation of security measures. This support can be realized through innovations in management processes, innovations in measures and technologies, and investments in these innovations. Management process innovations can be implemented either once, i.e. Business Process Reengineering (Fetais et al., 2022), or long-term, i.e. Business Process Improvement (Syed Ibrahim et al., 2019). Innovations of measures and technologies consist in assessing the extent of implementation of measures and technological innovations (Fayomi et al., 2019). The imaginary roof of innovation processes are investments in innovations, in which not only the amount of funds spent, but also their adequacy, expediency and timeliness of expenditure should be assessed (Lazonick, 2023).

Process plants safety can be further strengthened through implementation processes (Duchek, 2020), which include the implementation of management systems and new processes, software solutions and security measures. The essence of the implementation of management systems and new processes is a comprehensive assessment of the organization's readiness, i.e. implementation procedures and tools. The implementation of software solutions consists in the implementation of actions whose goal is to ensure security in cyber space based on information resulting from the analysis of incidents, needs and requirements of the organization. The implementation of safety measures consists in

the preparation and implementation of processes and technical means to increase the level of safety.

The last and absolutely necessary factor in strengthening process plants safety after an accident is the organization’s resources. These resources are generally classified as financial, human and material. Key indicators of the availability of financial resources are their optimal allocation and timeliness (Zhang et al., 2018). In the case of human resources, the key indicators are their capacity, expertise and time availability (Proag, 2021). The essence of material resources is the availability of components for repair, replacement or upgrade of security measures.

After the end of the accident in the process plants, it is necessary to focus attention on the adaptation of the organization’s processes and resources in connection with the implementation of measures to strengthen safety. In the context of the above, it is possible to state that educational and development processes can contribute to the adjustment of behavioural controls that ensure personal safety, e.g. use personal protective equipment (PPE), use the right tools, follow procedures, etc. By combining innovation and implementation processes, e.g. safe process structure, plant design, or process plants design can be significantly influenced. Organizational resources are essential for management of change, safer design (e.g. implementation of safety instrumented system) or instrumentation in protective systems.

3.3. Benefits of convergence of safety and security within process plants

The convergence of safety and security in process plants brings a comprehensive approach to protecting not only technologies and processes, but also human lives and the environment. The combination of these two areas allows the identification and elimination of a wide portfolio of unintentional or intentional incidents, such as technical accidents, operational errors, sabotage or cyber-attacks. This approach increases the resilience of the equipment, improves the effectiveness of preventive measures, and contributes to the continuity and long-term sustainability of process plants. In the current increasingly complex and dynamic environment of industrial processes, this convergence is becoming a necessity. Based on these facts, a simple diagram was compiled, illustrating the possible division of methods and tools that can be used to strengthen process plants safety (see Fig. 5).

Physical Protection System (PPS) can be effectively used to strengthen process plants safety in three areas, namely personal, process, and functional. In the area of personal safety, mechanical barriers and alarm systems contribute to the protection of the health and lives of personnel by minimizing the risk of accidents and reducing the probability of accidents. Suitable mechanical barriers are, for example, pressure barriers, opening fillings with increased pressure and chemical resistance. In addition, suitable alarm systems are, for example, motion

detectors, electronic security systems and emergency alarm systems, video surveillance systems, electronic access control systems or emergency call systems. The effectiveness of these tools can also be supported by regime measures aimed at controlling the entry and movement of unwanted persons.

Process safety can also be supported by alarm systems, such as video surveillance systems and electronic access control systems, which monitor and track the movement of people, ensure compliance with work procedures and identify risky situations. Modern technologies, such as GPS or RFID, enable localization and analysis of movement, thereby contributing to minimizing risks and restoring operations after an accident.

In the area of functional safety, PPS help to monitor technological equipment, detect deviations (e.g. overheating) and respond to them. Surveillance systems including thermal imaging cameras contribute to the prevention of accidents and the management of technical failures. Risk assessment techniques can also be used in the process and functional area, through which potential risks can be treated and thus significantly minimized.

Organizational resilience can also be used to strengthen the areas of personnel, process, and functional safety in process plants. In the area of personnel, educational and development processes are key, where personal safety is increased through incident management training, development of knowledge, skills, and attitudes of personnel. Security measures, which include protective equipment, regular training, and clearly defined procedures in the event of incidents, also contribute to minimizing the likelihood of occupational accidents and errors caused by personnel.

However, potential incidents are mainly resolved through incident management (the ability and skill of crisis management to handle incidents) or crisis preparedness (a proactive approach to identifying weaknesses). These tools are mainly used for rapid response and effective resolution of incidents, thereby contributing to the protection of processes and accelerating the return to safe operation. On the other hand, risk management focuses on the identification or assessment of risks, which allows for the prevention of failures, reducing the likelihood of accidents and thus increasing the safety of the processes themselves. In contrast, Business Process Reengineering or Business Process Improvement focus on the radical redesign of key processes in the organization with the aim of achieving significant improvements in safety, efficiency, productivity and quality of processes.

Various plans are also used in the area of functional safety, such as the Disaster Recovery Plan, which serves to quickly restore key systems and technologies after an incident, thereby ensuring the continuity of security functions and minimizing the risk of secondary failures that could endanger processes, employees or the surrounding environment. Business Continuity Management also ensures, among other things, the

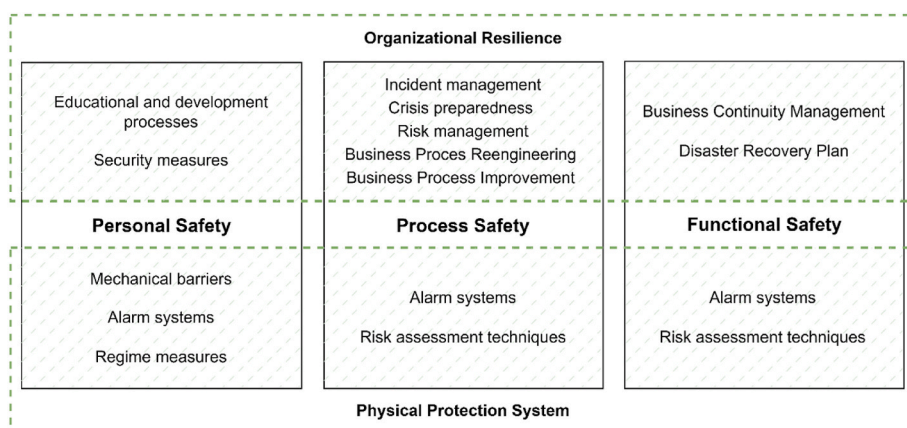


Fig. 5. Categorisation of methods and tools suitable for strengthening process plant safety.

functionality of the security system during incidents, which contributes to reducing the likelihood of interruption of operations and protecting processes and personnel.

As already mentioned, the presented framework of safety and security convergence within process plants is composed of two key areas, i.e. physical protection system and organizational resilience, which strengthen personal, process, and functional safety within process plants. This framework is applicable at two levels, i.e. operational and management. Both these levels are interconnected. Information and stimuli from the operational level serve as a basis for decision-making at the management level, and this decision-making influences the way of working at the operational level. However, contradictions can arise between these levels, such as a different approach to risk management. These misunderstandings or conflicts can be caused by different understandings of priorities, approaches to risk assessment, investments in safety or changes in the safety culture.

In some cases, some requirements from the area of physical protection system and organizational resilience may contradict each other. A possible contradiction may arise, for example, when increasing quality control, which involves increasing the frequency of process/product measurements by an employee. More frequent checks can be considered a preventive measure to minimize risks (management level) and at the same time these more frequent checks are likely to reveal a defect in the process/product more quickly (operational level). However, frequent checks can fatigue employees, which leads to frequent measurement errors and at the same time may reduce the personal safety of employees. Another example may be the introduction of new sensors, which may result in longer downtimes in production or changes in the structure of the process flow, which may reduce the efficiency of process plants.

These discrepancies, shortcomings or potential problems may arise when implementing any new system, requirement or measure. However, by using convergence, these potential discrepancies can be minimized and prevented. It is for this reason that the authors presented the framework of safety and security convergence within process plants, which represents a possible approach to preventing discrepancies between the operational and management levels. It can be assumed that by using this convergence, any discrepancies will be reduced to a minimum.

4. Conclusion

Convergence of individual separately existing types of security is currently increasingly used in practice. It is most often a convergence of physical security, information security, and cyber security. By converging these areas, the organization's cumulative security resources are integrated to optimize complex security solutions. This effective way of managing security was a source of inspiration for the authors of the article for the transposition of converged security into the area of process plants safety. The result of this transposition is the creation a framework for a possible approach and the possibility of using safety and security convergence within process plants.

The essence of this safety and security convergence is the strengthening of process plants safety through security measures. Specifically, it is the convergence of process plants safety with factors of physical protection system and organizational resilience. Security factors of the physical protection system can be used to strengthen safety on the operational level, while security factors of the organizational resilience can be used to strengthen safety on the management level.

The benefit of the safety and security convergence within process plants is the strengthening of core safety areas, i.e. personnel, process, and functional. Strengthening process plants safety can be implemented in three-time phases of the accident, i.e. before the accident (i.e. minimizing risks and increasing preparedness), during the accident (i.e. managing the consequences of the accident and monitoring the development of the situation) and after the accident (i.e. monitoring changes

in process plants and strengthening safety). Based on the conclusions presented above, it is appropriate to state that follow-up research should focus especially on the possibilities of convergence of individual types of safety in the context of efficiency, effectiveness, and economy.

CRediT authorship contribution statement

David Rehak: Writing – review & editing, Writing – original draft, Visualization, Supervision, Resources, Project administration, Methodology, Conceptualization. **Alena Spichalova:** Writing – review & editing, Writing – original draft, Visualization, Resources, Investigation, Formal analysis, Data curation. **Tomas Lovecek:** Writing – review & editing, Writing – original draft, Supervision, Resources, Project administration, Methodology, Conceptualization. **Martin Hromada:** Writing – review & editing, Writing – original draft, Validation, Methodology, Conceptualization. **Simona Jemelkova:** Writing – review & editing, Writing – original draft, Resources, Formal analysis, Data curation. **Alena Oulehlova:** Writing – review & editing, Writing – original draft, Resources, Formal analysis, Data curation.

Funding

This work was supported by the Ministry of the Interior of the Czech Republic [grant number VK01030014], by the Ministry of Education, Science, Research and Sport of the Slovak Republic [grant number VEGA1/0257/23] and by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia [grant number 17R05-04-V01-00005].

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: David Rehak reports financial support was provided by Ministry of the Interior of the Czech Republic. Tomas Lovecek reports financial support was provided by Ministry of Education Science Research and Sport of the Slovak Republic and by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

- Aleem, A., Wakefield, A., Button, M., 2013. Addressing the weakest link: implementing converged security. *Secur. J.* 26, 236–248. <https://doi.org/10.1057/sj.2013.14>.
- Armstrong, M., Taylor, S., 2014. *Armstrong's Handbook of Human Resource Management Practice*, thirteenth ed. Kogan Page, London.
- ASIS, 2009. *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*. American National Standards Institute, Washington, DC.
- Bennett, H.A., 1977. *EASI Approach to Physical Security Evaluation* (Tech. Rep., SAND-76-0500). Sandia National Laboratories, Albuquerque, NM.
- Bernatik, A., Senovsky, P., Senovsky, M., Rehak, D., 2013. Territorial risk analysis and mapping. *Chem. Eng. Trans.* 31, 79–84. <https://doi.org/10.3303/CET1331014>.
- Brucherseifer, E., Winter, H., Mentges, A., Mühlhäuser, M., Hellmann, M., 2021. Digital twin conceptual framework for improving critical infrastructure resilience. *Automatisierungstechnik* 69 (12), 1062–1080. <https://doi.org/10.1515/auto-2021-0104>.
- BS 65000, 2022. *Organizational Resilience. Code of Practice*. British Standards Institution, London.
- Carmeli, A., Schaubroeck, J., 2008. Organisational crisis-preparedness: the importance of learning from failures. *Long. Range Plan.* 41 (2), 177–196. <https://doi.org/10.1016/j.lrp.2008.01.001>.
- CEN/TS 14383-3, 2005. *Prevention of Crime – Urban Planning and Building Design – Part 3: Dwellings*. European Committee for Standardization, Brussels.

- CEN/TS 14383-4, 2006. Prevention of Crime – Urban Planning and Design – Part 4: Shops and Offices. European Committee for Standardization, Brussels.
- CEN/TS 14383-6, 2022. Prevention of Crime – Urban Planning and Building Design – Part 6: Schools and Educational Institutions. European Committee for Standardization, Brussels.
- CEN/TS 16850, 2015. Societal and Citizen Security – Guidance for Managing Security in Healthcare Facilities. European Committee for Standardization, Brussels.
- Denyer, D., 2017. Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking. BSI and Cranfield University, Cranfield.
- Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the Control of Major-Accident Hazards Involving Dangerous Substances, Amending and Subsequently Repealing Council Directive 96/82/EC.
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive).
- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC.
- Duchek, S., 2020. Organizational resilience: a capability-based conceptualization. *Bus. Res.* 13, 215–246. <https://doi.org/10.1007/s40685-019-0085-7>.
- Edwards, J., 2024. Mastering Cybersecurity: Strategies, Technologies, and Best Practices. Apress, Berkeley, CA. <https://doi.org/10.1007/979-8-8688-0297-3>.
- EN 356, 1999. Glass in Building – Security Glazing – Testing and Classification of Resistance against Manual Attack. European Committee for Standardization, Brussels.
- EN 13124-2, 2004. Windows, Doors and Shutters – Explosion Resistance – Test Method – Part 2: Range Test. European Committee for Standardization, Brussels.
- EN 16763, 2017. Services for Fire Safety Systems and Security Systems. European Committee for Standardization, Brussels.
- EN 50131-1, 2006. Alarm systems – intrusion and hold-up systems – Part 1: system requirements. European Committee for Electrotechnical Standardization, Brussels.
- EN 50134-1, 2002. Alarm Systems – Social Alarm Systems – Part 1: System Requirements. European Committee for Electrotechnical Standardization, Brussels.
- EN 50136-1, 2012. Alarm Systems – Alarm Transmission Systems and Equipment – Part 1: General Requirements for Alarm Transmission Systems. European Committee for Electrotechnical Standardization, Brussels.
- EN 50398-1, 2017. Alarm Systems - Combined and Integrated Alarm Systems – Part 1: General Requirements. European Committee for Electrotechnical Standardization, Brussels.
- EN 62676-1-1, 2014. Video Surveillance Systems for Use in Security Applications – Part 1-1: System Requirements – General. European Committee for Electrotechnical Standardization, Brussels.
- EN 62676-4, 2015. Video Surveillance Systems for Use in Security Applications – Part 4: Application Guidelines. European Committee for Electrotechnical Standardization, Brussels.
- EN 60839-11-1, 2013. Alarm and electronic security systems – Part 11-1: electronic access control systems – system and components requirements. European Committee for Electrotechnical Standardization, Brussels.
- Fayomi, O.S.I., Adelakun, J.O., Babaremu, K.O., 2019. The impact of technological innovation on production. *J. Phys. Conf.* 1378, 022014. <https://doi.org/10.1088/1742-6596/1378/2/022014>.
- Fetais, A., Abdella, G.M., Al-Khalifa, K.N., Hamouda, A.M., 2022. Business process Re-engineering: a literature review-based analysis of implementation measures. *Information* 13, 185. <https://doi.org/10.3390/info13040185>.
- García, M.L., 2005. Vulnerability Assessment of Physical Protection Systems. Butterworth-Heinemann, Oxford.
- García, M.L., 2008. Design and Evaluation of Physical Protection Systems, second ed. Butterworth-Heinemann, Oxford. <https://doi.org/10.1016/C2009-0-25612-1>.
- Gersak, J., 2022. Planning clothing manufacturing. In: Design of Clothing Manufacturing Processes, second ed. Woodhead Publishing, Sawston, pp. 219–282. <https://doi.org/10.1016/B978-0-08-102648-9.00005-0>.
- Godovykh, A.V., Stepanov, B.P., Sheveleva, A.A., Sharafieva, K.R., 2016. Simulation of the effectiveness evaluation process of security systems. In: 8th International Scientific Conference "Issues of Physics and Technology in Science, Industry and Medicine, vol. 135, 012014. <https://doi.org/10.1088/1757-899X/135/1/012014>, 1-3 June 2016, Tomsk, Russia.
- Hauptmanns, U., 2020. Process and Plant Safety. Springer Vieweg, Berlin, Heidelberg. <https://doi.org/10.1007/978-3-662-61484-6>.
- Hromada, M., Rehak, D., Lukas, L., 2021. Resilience assessment in electricity critical infrastructure from the point of view of converged security. *Energies* 14 (6), 1624. <https://doi.org/10.3390/en14061624>.
- Hromada, M., Rehak, D., Skobiej, B., Bajer, M., 2023. Converged security and information management system as a tool for smart city infrastructure resilience assessment. *Smart Cities* 6 (5), 2221–2244. <https://doi.org/10.3390/smartcities6050102>.
- ICOR, 2024. Organizational resilience framework. The International Consortium for Organizational Resilience. Lombard, IL.
- IEC 31010, 2019. Risk Management – Risk Assessment Techniques. International Electrotechnical Commission, Geneva.
- IEC 61508, 2010. Functional Safety of Electrical/electronic/programmable Electronic Safety-Related Systems. International Organization for Standardization, Geneva.
- IEC 62443-3-2, 2020. Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment for System Design. International Electrotechnical Commission, Geneva.
- ISO 9001, 2015. Quality Management Systems – Requirements. International Organization for Standardization, Geneva.
- ISO 12100, 2010. Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction. International Organization for Standardization, Geneva.
- ISO 14001, 2015. Environmental Management Systems – Requirements with Guidance for Use. International Organization for Standardization, Geneva.
- ISO 18788, 2015. Management System for Private Security Operations – Requirements with Guidance for Use. International Organization for Standardization, Geneva.
- ISO 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 23247, 2021. Automation Systems and Integration – Digital Twin Framework for Manufacturing. International Organization for Standardization, Geneva.
- ISO/IEC 27001, 2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. International Organization for Standardization, Geneva.
- ISO/IEC 27019, 2024. Information Security, Cybersecurity and Privacy Protection – Information Security Controls for the Energy Utility Industry. International Organization for Standardization, Geneva.
- ISO/IEC 27032, 2023. Cybersecurity – Guidelines for Internet Security. International Organization for Standardization, Geneva.
- ISO/IEC 30173, 2023. Digital Twin – Concepts and Terminology. International Organization for Standardization, Geneva.
- ISO 28000, 2022. Security and Resilience – Security Management Systems – Requirements. International Organization for Standardization, Geneva.
- ISO 31000, 2018. Risk Management – Guidelines. International Organization for Standardization, Geneva.
- ISO/TS 31050, 2023. Risk Management – Guidelines for Managing an Emerging Risk to Enhance Resilience. International Organization for Standardization, Geneva.
- ISO 37002, 2021. Whistleblowing Management Systems – Guidelines. International Organization for Standardization, Geneva.
- ISO 45001, 2018. Occupational Health and Safety Management Systems – Requirements with Guidance for Use. International Organization for Standardization, Geneva.
- ISO 50001, 2018. Energy Management Systems – Requirements with Guidance for Use. International Organization for Standardization, Geneva.
- ISO 55001, 2024. Asset Management – Asset Management System – Requirements. International Organization for Standardization, Geneva.
- ISO, 2018. The Integrated Use of Management System Standards (IUMSS). International Organization for Standardization, Geneva.
- Jang, S.S., Kwan, S.W., Yoo, H.S., Kim, J.S., Yoon, W.K., 2009. Development of a vulnerability assessment code for a physical protection system: systematic analysis of physical protection effectiveness (SAPE). *Nucl. Eng. Technol.* 41 (5), 747–752. <https://doi.org/10.5516/NET.2009.41.5.747>.
- Kallambettu, J., Viswanathan, V., 2018. Application of functional safety to electrical power equipment and systems in process industries. *J. Loss Prev. Process. Ind.* 56, 155–161. <https://doi.org/10.1016/j.jlp.2018.07.009>.
- Kampova, K., Lovecek, T., Rehak, D., 2020. Quantitative approach to physical protection systems assessment of critical infrastructure elements: use case in the Slovak Republic. *Int. J. Crit. Infrastruct. Protect.* 30, 100376. <https://doi.org/10.1016/j.ijcip.2020.100376>.
- Lazonick, W., 2023. Investing in Innovation: Confronting Predatory Value Extraction in the U.S. Corporation. Cambridge University Press, Cambridge. <https://doi.org/10.1017/9781009410700>.
- Lovecek, T., Maris, L., Siser, A., 2018. Planning and Designing Object Protection Systems. University of Zilina, Zilina (in Slovak).
- Lovecek, T., Reitspis, J., 2011. Designing and Evaluation of Object Protection Systems. University of Zilina, Zilina (in Slovak).
- Lovecek, T., Ristvej, J., Simak, L., 2010. Critical infrastructure protection systems effectiveness evaluation. *J. Homel. Secur. Emerg. Manag.* 7 (1), 34. <https://doi.org/10.2202/1547-7355.1613>.
- Lovecek, T., Skypalova, E., Boros, M., Kuffa, R., 2023. Locating people in a confined space using iBeacon technology. In: IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1–9. <https://doi.org/10.1109/ICCST59048.2023.10474277>.
- Lovecek, T., Velas, A., Durovec, M., 2015. Security Systems: Alarm Systems. University of Zilina, Zilina (in Slovak).
- Lukas, L., 2017. Security theory I. Zlin: Radim Bacuvcik - VeRBuM (in Czech).
- Lukas, L., 2019. Converged Security. Zlin: Radim Bacuvcik - VeRBuM (in Czech).
- Majid, N.D.A., Shariff, A.M., Rusli, R., 2015. Process Safety Management (PSM) for managing contractors in process plant. *J. Loss Prev. Process. Ind.* 37, 82–90. <https://doi.org/10.1016/j.jlp.2015.06.014>.
- Mannan, M.S., Sachdeva, S., Chen, H., Reyes-Valdes, O., Liu, Y., Laboureur, D.M., 2015. Trends and challenges in process safety. *AIChE J.* 61, 3558–3569. <https://doi.org/10.1002/aic.15019>.
- Matter, C., 1988. SAVI: A PC-Based Vulnerability Assessment Program (Tech. Rep., SAND-88-1279). Sandia National Laboratories, Albuquerque, NM.
- Mccreight, T., Leece, D., 2016. Physical security and IT convergence: managing the cyber-related risks. *J. Bus. Continuity Emerg. Plan.* 10 (1), 18–30.
- Mohan, P.S., 2023. Disasters, disaster preparedness and post disaster recovery: evidence from Caribbean firms. *Int. J. Disaster Risk Reduc.* 92, 103731. <https://doi.org/10.1016/j.ijdrr.2023.103731>.
- Moran, S., 2019. How to lay out a process plant. In: An Applied Guide to Process and Plant Design, second ed. Elsevier, Amsterdam, pp. 237–255. <https://doi.org/10.1016/B978-0-12-814860-0.00016-1>.

- Mwai, G.M., Namada, J.M., Katuse, P., 2018. Influence of organizational resources on organizational effectiveness. *Am. J. Ind. Bus. Manag.* 8 (6), 1634–1656. <https://doi.org/10.4236/ajibm.2018.86109>.
- OECD/Eurostat (Organisation for Economic Co-operation and Development), 2005. *Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data*. OECD Publishing, Paris. <https://doi.org/10.1787/9789264013100-en>.
- OSHA, 2013. *Process Safety Management of Highly Hazardous Chemicals*. Occupational Safety and Health Administration, Washington, D.C. Standard Number 29 CFR 1910.119.
- Phillips, G., et al., 2005. *New vulnerability assessment technologies vs the old VA tools*. National Security Program Office Y-12. Oak Ridge, TN.
- Philpott, D., 2016. *Emergency preparedness: a safety planning guide for people*. Property and Business Continuity, second ed. Bernan Press, Lanham, MD.
- Proag, V., 2021. *Human resources management for infrastructure*. In: *Infrastructure Planning and Management: an Integrated Approach*. Springer, Cham, pp. 563–593. https://doi.org/10.1007/978-3-030-48559-7_20.
- Qin, Y., 2015. Overview of micro-manufacturing. In: *Micromanufacturing Engineering and Technology*, second ed. William Andrew, Norwich, NY, pp. 1–33. <https://doi.org/10.1016/B978-0-323-31149-6.00001-3>.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).
- Rehak, D., 2020. Assessing and strengthening organisational resilience in a critical infrastructure system: case study of the Slovak Republic. *Saf. Sci.* 123, 104573. <https://doi.org/10.1016/j.ssci.2019.104573>.
- Rehak, D., Senovsky, P., Hromada, M., Lovecek, T., 2019. Complex approach to assessing resilience of critical infrastructure elements. *Int. J. Crit. Infrastruct. Protect.* 25, 125–138. <https://doi.org/10.1016/j.ijcip.2019.03.003>.
- Rehak, D., Splichalova, A., Janeckova, H., Oulehlova, A., Hromada, M., Kontogeorgos, M., Ristvej, J., 2024a. Critical entities resilience assessment (CERA) to small-scale disasters. *Int. J. Disaster Risk Reduc.* 111, 104748. <https://doi.org/10.1016/j.ijdrr.2024.104748>.
- Rehak, D., Splichalova, A., Hromada, M., Walker, N., Janeckova, H., Ristvej, J., 2024b. Critical entities resilience failure indication. *Saf. Sci.* 170, 106371. <https://doi.org/10.1016/j.ssci.2023.106371>.
- Rodriguez, J., Walters, K., 2017. The importance of training and development in employee performance and evaluation. *World Wide J. Multidiscip. Res. Dev.* 3 (10), 206–212.
- Roland, H.E., Moriarty, B., 1990. *System Safety Engineering and Management*, second ed. John Wiley & Sons, New York, NY.
- Savolainen, R., 2017. Information sharing and knowledge sharing as communicative activities. *Inf. Res.* 22 (3), 9.
- Schindel, Polyakova, Harding, Weinhold, Stenger, Grünwald, Bramsiepe, 2021. General approach for technology and Process Equipment Assembly (PEA) selection in process design. *Chem. Eng. Process. - Process Intensif.* 159, 108223. <https://doi.org/10.1016/j.cep.2020.108223>.
- Schlegel, J., 2023. *Manufacturing processes*. In: *The World of Steel*. Springer, Wiesbaden. https://doi.org/10.1007/978-3-658-39733-3_8.
- Syed Ibrahim, M., Hanif, A., Jamal, F.Q., Ahsan, A., 2019. Towards successful business process improvement – an extension of change acceleration process model. *PLoS One* 14 (11), e0225669. <https://doi.org/10.1371/journal.pone.0225669>.
- Tyson, D., 2007. *Security Convergence: Managing Enterprise Security Risk*. Butterworth-Heinemann, Oxford. <https://doi.org/10.1016/B978-0-7506-8425-5.X5000-9>.
- Varbanov, P.S., 2023. Basic process integration terminology. In: *Handbook of Process Integration (PI)*, second ed. Woodhead Publishing, Sawston, pp. 25–72. <https://doi.org/10.1016/B978-0-12-823850-9.00007-4>.
- Véchet, L.N., Olewski, T., Al-Qahtani, A.H., 2022. Development and implementation of a process safety competency development program (PSCDP) for process safety engineers: a unique collaboration between industry (SABIC) and academia (MKOPSC). *J. Loss Prev. Process. Ind.* 80, 104917. <https://doi.org/10.1016/j.jlp.2022.104917>.
- Vintr, Z., Vintr, M., Malach, J., 2012. Evaluation of physical protection system effectiveness. In: *IEEE International Carnahan Conference on Security Technology (ICCST)*, pp. 15–21. <https://doi.org/10.1109/CCST.2012.6393532>. Newton, MA.
- Wely, I.C.E., Chetaine, A., 2021. Analysis of physical protection system effectiveness of nuclear power plants based on performance approach. *Ann. Nucl. Energy* 152, 107980. <https://doi.org/10.1016/j.anucene.2020.107980>.
- Wilde, J., Reindl, L., Stewart, C., 2008. Testing, calibration and compensation. In: *Microsystems, Comprehensive*, Gianchandani, Y.B., Tabata, O., Zappe, H. (Eds.), *Comprehensive Microsystems*, vol. 1. Elsevier, Amsterdam, pp. 495–538. <https://doi.org/10.1016/B978-0-44452190-3.00026-4>.
- Williams, A.D., 2021. Physical security: methods and practices. In: Shapiro, L.R., Maras, M.H. (Eds.), *Encyclopedia of Security and Emergency Management*. Springer, Cham, pp. 759–766. https://doi.org/10.1007/978-3-319-70488-3_93.
- Wilson, M., 2015. Automation system components. In: *Implementation of Robot Systems: an Introduction to Robotics, Automation, and Successful Systems Integration in Manufacturing*. Butterworth-Heinemann, Oxford, pp. 39–73. <https://doi.org/10.1016/B978-0-12-404733-4.00003-5>.
- Yamoah, E.E., 2014. The link between human resource capacity building and job performance. *Int. J. Hum. Resour. Stud.* 4 (3), 139–146. <https://doi.org/10.5296/ijhrs.v4i3.5938>.
- Zhang, Ch, Kong, J.J., Simonovic, S.P., 2018. Restoration resource allocation model for enhancing resilience of interdependent infrastructure systems. *Saf. Sci.* 102, 169–177. <https://doi.org/10.1016/j.ssci.2017.10.014>.
- Zorn, C.R., Shamseldin, A.Y., 2015. Post-disaster infrastructure restoration: a comparison of events for future planning. *Int. J. Disaster Risk Reduc.* 13, 158–166. <https://doi.org/10.1016/j.ijdrr.2015.04.004>.