European Research Studies Journal
Volume XXIV, Issue 3, 2021

pp. 1153-1188

The Role of Integral Model of Critical Infrastructure Safety in Industry 4.0

Submitted 19/06/21, 1st revision 12/07/21, 2nd revision 23/07/21, accepted 28/08/21

Michał Wiśniewski[1]

Abstract:

Purpose: *This paper aims to create a dedicated tool for managing the level of availability of services delivered by critical infrastructure (CI) facilities, which will affect the Sustainable Development Goals. The paper established a link between sustainability, Industry 4.0, and critical infrastructure. The literature analysis has indicated that the security of Industry 4.0 is discussed almost exclusively in the perspective of cyber security.*
Design/Methodology/Approach: *Verification of the tool was carried out based on simulations and computational experience using data PKN ORLEN Refinery Inc.*
Findings: *As a result of the work carried out, an Integral Model of Critical Infrastructure Safety (IMCIS) was obtained, which allows us to present CI's current characteristics. It was established that the canon of characterization of CI objects consists of a set of resources, a set of functionalities, a set of threats, a set of safeguards, a set of threat dependencies, and a set of dependencies of objects recognized as CI.*
Practical Implications: *A universal application of the IMCIS is to estimate the level of risk before and after implementing safeguards and generating adverse event scenarios. The identified threats are the decision-making areas of the decision problem, whose solution is indicated by a set of safeguards reducing the risk level to an acceptable level.*
Originality/Value: *The solution can be used to identify a set of safeguards that, on the one hand, will reduce the cost of the business operator to a minimum and, on the other hand, achieve the required level of availability of CI functionality. In addition, IMCIS allows analyzing all threats that may affect the infrastructure of Industry 4.0, taking into account many independent decision-making centers.*

Keywords: *Critical infrastructure, industry 4.0, sustainability, management of safety, adverse events scenarios.*

JEL codes: *C10, H12.*

Paper type: *Research article.*

Acknowledgment: *The article results from a project funded by the National Centre for Research and Development of Poland entitled "Methodology of risk assessment for the purposes of crisis management system in Poland" contract number DORB/0077/R/ID3/2013/03 and the author's cooperation with the Government Centre for Security of Poland.*

[1] *Ph.D. Eng., Faculty of Management, Warsaw University of Technology, ORCID: 0000-0003-3435-3114, e-mail: Michal.Wisniewski@pw.edu.pl;*

1. Introduction

The main ideas of Industry 4.0 were published in 2011 (Kagermann *et al.,* 2011), and also became a strategic initiative of the German government and was included in the High-Tech Strategy 2020 Action Plan (Kagermann *et al.*, 2013). Similar strategies have also been implemented in other countries, e.g., the USA (Advanced Manufacturing Partnership), United Kingdom (Smart Factory), or China (Made in China 2025) (Kumar *et al.,* 2020). Despite the fact that Industry 4.0 is one of the most discussed topics among practitioners and scientists in the past years, no single, commonly accepted definition of this concept has been developed (Buer *et al.,* 2018; Mrugalska and Wyrwicka, 2017). Researchers and practitioners have divided opinions on which elements create Industry 4.0, how these elements are interrelated and where Industry 4.0 applies. Regardless of the definition, the idea of industry 4.0 indicates from centralized production towards production that is very flexible and self-controlled.

Over time, the concept of Industry 4.0 has become synonymous with the fourth industrial revolution (Buer *et al.,* 2018; Gierszewska *et al.*, 2020). Kolberg and Zuehlke (2015) present Industry 4.0 as a further development of Computer Integrated Manufacturing (CIM) and thus a network approach that complements CIM through ICT. The integration of automation technologies supports this approach, e.g., cyber-physical systems (CPS), collaborative robots, cloud computing, and big data sets, with the production environment via the Internet of Things (IoT) (Xu *et al.,* 2018). Embedded systems, semantic machine-machine communication, CPS, and IoT enable connection of the physical and virtual world which is the main goal of Industry 4.0 (Xu *et al.,* 2018). This allows connecting the entire factory into a network, creating an intelligent environment. Therefore, Industry 4.0 is dependent on infrastructure efficiency, which provides access to energy, water, communications, transport, ICT networks. Part of this infrastructure is called Critical Infrastructure (CI). The definition of CI is contingent on the legal system of states.

Regardless of the definition, CI components are exposed to different types of threats due to human activities, natural disasters, military operations, terrorism, or cybercrime. The efficiency of CI, measured by the availability of these facilities' functionality, determines the sense of citizens' safety, rate of economic growth, social satisfaction, the sovereignty of the state, and effectiveness of public administration entities. On the other hand, the limited functionality of CI results in economic losses, environmental pollution, and a real threat to the population's health and life (FEMA, 2017).

The combination of AI, robotics, and other advanced technologies applied across many sectors of the economy, e.g., the supply chain, distribution channels, manufacturing, provides a significant impact on the natural environment leading to reduction of pollution, decrease in greenhouse gases emission, decrease in energy consumption and increase in profits, simultaneously. The emergence of Industry 4.0

opens the opportunity of connectivity of technology with resources and skills in terms of sustainability benefits (zero impact-lower cost-social equity). Industry 4.0 can reduce the environmental impact of a product, a process, or a service based on footprint data availability and traceable analysis (Peukert *et al.,* 2015, p. 29). Additionally, it helps to leverage a greater efficiency of functions, e.g., reduction of resource consumption.

Industry 4.0 as a contributor to the Sustainable Development Goals (SDGs) (Ejsmont *et al.*, 2020) builds connectivity between the industry and sustainability by finding a significant relation between their components. In contrast, CI systems are the basis for Industry 4.0. In this regard, CI does essential to economic, environmental, and social sustainability.

CI protection procedures worldwide are a part of the crisis management process, which definition can be found in national methodologies of crisis management. The methods and techniques which can be found in national methodologies are appropriate for public administrations. However, such actions will be inadequate and cannot be applied to the operation of economic entities that possess CI items. The application of methods and techniques related to operational risk management used in business organizations is also inefficient for the challenges of the CI operators. CI operators are obligated to maintain the profitability of the activities undertaken and to generate profits.

Moreover, they must ensure the proper level of CI functionality required by society. This situation indicates a new type of complication in management science, where the effectiveness of action has a higher priority than their efficiency. This problem fits into the issue of social logistics (Szołtysek, 2014). The solution requires the adaptation of methods and techniques used in business organizations. They allow for a formal definition of the decision-making problem, whose objective function has two dimensions. The selection of safeguards protects against excessive loss of CI availability of functionality and minimizing the cost of additional risk reduction activities.

The author's main objectives were to develop an integrated model of critical infrastructure safety (IMCIS). In this case, it is understood as a set of issues enabling model mapping of situation of CI[2], recognition of adverse events scenarios, estimation of risk resulting from the threats to which CI is vulnerable, and subsequently, identification of the decision problem of CI safeguards that potentially could be applied in response to the recognized threats. IMCIS will impact the reliability of the infrastructure for Industry 4.0, which will contribute to the achievement of the SDGs.

[2] *Situation of CI - current characteristics of CI determined in the domain of resources, functionality, threats and safeguards, including the relationship between the CI and related facilities.*

The set goal indicates two research questions:

- What issues must IMCIS integrate?
- What components have to be included in CI's characteristics to ensure the usability of IMCIS regardless of the CI type and the entity responsible for CI protection?

2. Background

An analysis of the available literature was conducted to confirm the research gap. The analysis included a search for available knowledge in four areas:

- the link between industry 4.0 and sustainability,
- the link between industry 4.0 and critical infrastructure,
- protection of industry 4.0,
- protection of critical infrastructure.

The literature review was done in two ways: using available review studies or using a knowledge base review using filters composed of keywords.

Two databases were used for literature analysis: Web of Science Core Collection (WoSCC) and Scopus, because those are the most common databases for conducting literature searches (Joshi, 2016). These databases are also considered the two most important multidisciplinary bibliometric databases (Van Eck and Waltman, 2017) used for field delineation (Strozzi *et al.,* 2017). WoSCC and Scopus are also leading databases with significant scientific impacts characterized by a high quality of reported documents (Powell and Peterson, 2017).

The search was limited to scientific research works published after 2011 because, in this year, the term "Industry 4.0" was used for the first time, and the basic assumptions of the Fourth Industrial Revolution were defined (Kagermann *et al.*, 2013). Only articles in English from reviewed journals were considered for further analysis. The Scopus database contained the majority of compact studies in WoSCC (about 70%). Therefore, the search results from the Scopus database were chosen for further analysis. The objective was to select studies that concerned the relationship in the indicated areas.

2.1 The Relationship between Industry 4.0 and Sustainability

The relationship between Industry 4.0 and Sustainability was established using a review study (Ejsmont *et al.,* 2020). The authors used Systematic Literature Network Analysis (SLNA) (Strozzi *et al.,* 2017; Colicchia and Strozzi, 2012) to analyze the paper after 2011 indexed in Scopus and WoSCC databases.

The conducted literature review indicates that the selected papers are dominated by one subject area, engineering (80 papers). It proves that in most articles, the authors focused on aspects related to manufacturing in which the integration of Industry 4.0 and sustainability concepts enables the creation of new engineering solutions to achieve more sustainable and green production. The next most numerous subject areas regarding the analyzed topic are environmental science (59 papers) and energy (53 paperes). It may indicate that these papers concentrated on using Industry 4.0 technologies and tools to protect the natural environment, increase energy efficiency and achieve sustainable development goals.

Next up are articles related to business, management, and accounting (46 papers), social sciences (46 papers), and computer science (37 papers). These articles examine the impact of Industry 4.0 on business management issues based on the triple bottom line (TBL) framework. The impact can be measured using IT tools/algorithms based on Industry 4.0 technologies. Other subject matters are less numerous in terms of articles and cover many different fields (although all of them are related to engineering and management), indicating the interdisciplinary nature of sustainability and Industry 4.0 (Ejsmont *et al.*, 2020).

Synergy exists between Industry 4.0 and sustainability due to digital technology. Using Industry 4.0-technology affecting sustainability through the responsible, effective use of resources, circular economy (CE) can be reached. The concept lying on decentralization of manufacturing embodied in an IT technology framework was the response to the pressure on changing conventional business models to develop new sustainable business models (circular business model). An indispensable way to achieve CE is based on technologies that are often successful when combined with IoT. Industry 4.0 can act as a driver of a redesign of traditional supply chains aiming at resource efficiency and circularity. The Industry 4.0 technologies, e.g., sensors deployed in many machines, enable tracking production performance and product data over the full product life cycle. Consequently, an analysis of collected data results in productivity improvements (Ejsmont *et al.*, 2020).

Technologies and tools can be integrated into sustainability practices on a theoretical and practical basis. Mainly IoT, digitization, sensors, and big data could be employed to monitor sustainability. The study confirms that IIoT is an important element of Industry 4.0 and has an impact on sustainability. Smart technologies of Big Data Analytics, sensors, etc., displaced conventional computer-aided manufacturing industry to deliver tremendous business values or outcomes. On the one hand, it provides socio-economic values; on the other hand, it creates challenges for scientific research on the real-time speed of manufacturing data and data storage.

The application of Industry 4.0 technologies and tools efficiently should give opportunities to manage big data (acquisition, extraction, transmission, storage). The Industry 4.0 technologies can help to reduce both machine operational time and waste thanks to more effective machine and resources utilization, consequently ensuring a cost-effective operation. Sensors used in production allow gathering a machine's status data to analyze a load of machines, reduce downtime, and protect products against unexpected failures that greatly impact product quality (Ejsmont *et al.*, 2020).

Results of the research indicate that Industry 4.0 supports the implementation of sustainability concepts. There are no papers reporting research on reverse relations, i.e., how selected sustainability concepts could support the implementation of selected Industry 4.0 technologies. There is a lack of research approaching issues of sustainability and Industry 4.0 in a comprehensive way. Frameworks exist, findings on barriers, success factors, the state of the art of Industry 4.0 implementation in selected economies, industries, research directions presented by researchers (Adamiak and Nowacki, 2020; Młody and Weinert, 2020).

2.2 The Relationship between Industry 4.0 and Critical Infrastructure

A review of available studies on CI and Industry 4.0 was performed using a query of (1). The query returned 519 papers. The areas of Engineering (232 papers) and Computer Science (293 papers) dominated the results.

KEY (industry 4 OR i4 OR i4.0 OR industry 4.0) & (ci OR critical AND infrastructure) (1)

A further reduction of the results obtained was made by excluding subject areas: Mathematics, Materials Science, Physics and Astronomy, Biochemistry, Genetics, and Molecular Biology, Chemistry, Psychology, Medicine, Arts and Humanities, Agricultural and Biological Sciences, Earth and Planetary Sciences, Health Professions, Immunology and Microbiology, Pharmacology, Toxicology, and Pharmaceutics. As a result of this activity, 315 papers were selected. Articles were included through the following process: firstly, by reading the title (all), secondly by reading the abstract (90 articles), and thirdly by reading the full paper (21 articles).

It has been observed that works combining CI and Industry 4.0 issues appear from 2013 to 2021. It is a natural consequence of the young age of these concepts. The analyzed research indicates that the issue of CI appears in the context of technologies enabling the realization of the Industry 4.0 idea. However, the available studies indicate differences between the needs of developing and developed countries. The lack of a digital strategy alongside resource scarcity emerges as the most prominent barrier in developed and developing economies. The influencing barriers identified suggest that improvements in standards and government regulation could facilitate the adoption of Industry 4.0 technologies in developing country cases. In contrast, technological infrastructure is needed to promote the adoption of these technologies in developed country cases (Raj *et al.*, 2020).

Particularly many works in the area of using network technologies cyber-physical Systems, IoT, cloud computing, Industrial Integration, Enterprise Architecture, SOA, Industrial Information Integration, and others (Jasperneite, 2012; Kagermann *et al.,* 2013; Lasi *et al.,* 2014; Hermann *et al.,* 2016; Moeuf *et al.,* 2017; Xu *et al.,* 2018; Ivanov *et al.,* 2020).

The studies reviewed do not consider Industry 4.0 a critical infrastructure sector from a state or societal perspective. However, the Industry 4.0 phenomenon offers opportunities and challenges to all business models (Asif, 2020; Ghadge *et al.*, 2020). The available study identified 26 drivers associated with Industry 4.0 that impact improved business process management (BPM). These drivers are presented in an integrative framework considering BDA, CPS, and the IoT (Figure 1).

Furthermore, Industry 4.0 proposes the adoption of advanced ICT in manufacturing to enhance manufacturing efficiency and competency. The emergence of interest in Industry 4.0 has increased in recent years due to the belief that the current Industry 4.0 movement is marking a major turning point in history (Colombo *et al.,* 2015). Industry 4.0 is no longer a future trend. For many enterprises, it is now at the heart of their strategic and research agenda (PWC, 2016). Successful Industry 4.0 relies upon more sophisticated technologies than those that are available now. Technologies will act as an enabler in Industry 4.0 for tomorrow's more effective and competitive industrial ecosystems. Currently, efforts focusing on blending the proposed capabilities of Industry 4.0 and emerging technologies are needed. With this blending, Industry 4.0 will be able to harness the power of current and emerging technologies to dramatically improve the complex industrial ecosystems (Xu *et al.*, 2018).

Figure 1. *Main elements of Industry 4.0*

CPS – cyber-physical systems	provides ICT integration with physical components and computational	Industry 4.0
IoT – internet of things	is a network of objects that can communicate with each other by ICT	
BDA – big data analytics	refers to new techniques to storage, processing, and analyze large amounts of data	
CC – cloud computing	is an ICT that provides a set of web services with resources optimization	
SPS – smart production	provides optimization and flexibility in the production process, supported mainly by IoT and CPS	
CM – cloud manufacturing	uses intense ICT, providing resources circularity and on-demand in the lifecycle of a product	
3DP/AM – 3D printing /additive manufacturing	provides rapid prototyping in the production process, generating decentralized manufacturing	
M2M – maschine to maschine	machines can communicate with each other and take self-decisions according to demand patterns	
BC – blockchain	distributed database that permits peer-to-peer transactions with high-level of cryptography	
AGV – autonomous guided vehicles	driverless transport used in production systems to transfer materials according to demand	
AI – artificial intelligence	machines and devices with intelligence to perform tasks without or with human-interaction	

SC – smart cities	ICT that integrate human, equipment and city, intelligently, providing sustainability	

Source: *Queiroz et. al., 2020, p. 1076.*

In this context, Industry 4.0 and the technologies enabling its implementation may in the future be included in the CI category, on which the proper functioning of the economy, society, and public administration will depend (Hossain and Thakur, 2020). It is indicated by the actions of, among others, the governments of Germany and China. In 2013, amongst one of 10 Future Projects identified by the German government as part of its High-Tech Strategy 2020 Action Plan, the Industry 4.0 project was considered a major endeavor for Germany to establish itself as an integrated industry leader. In 2014, China's State Council unveiled their ten-year national plan, Made-in-China 2025, designed to transform China from the world's workshop into a world manufacturing power (Xu *et al.,* 2018).

Although the Third Industrial Revolution also focused on the automation of machines and processes (Tan *et al*., 2010), Industry 4.0 focuses more on the end-to-end digitization and the integration of digital industrial ecosystems by seeking completely integrated solutions. Industry 4.0 comprises many complex components and has broad applications in numerous industrial sectors. At present, one of the challenges is making use of cutting-edge ICT and engineering technology to make Industry 4.0 successful (Mousterman and Zander, 2016; Xu *et al.,* 2018).

This success depends on the undisturbed functioning of dispersed Industry 4.0 components. It indicates the need for risk analysis of many dependent resources not necessarily managed by the same operator. Identified risks require responses that must reduce the level of risk to the overall system and take into account multiple decision-making centers. This perspective prompts attention to the issue of Industry 4.0 safety.

2.3 The Protection of Industry 4.0

A review of available studies on models of safety Industry 4.0 was performed using a query of (2). The query returned 2454 papers. The areas of Engineering (1430 papers) and Computer Science (1318 papers) dominated the results.

KEY (industry 4 OR i4 OR i4.0 OR industry 4.0) AND (protection OR safety OR security OR resilience OR vulnerability) (2)

A further reduction of the results obtained was made by excluding subject areas: Mathematics, Materials Science, Physics and Astronomy, Biochemistry, Genetics, and Molecular Biology, Chemistry, Psychology, Medicine, Arts and Humanities, Agricultural and Biological Sciences, Earth and Planetary Sciences, Health Professions, Immunology and Microbiology, Pharmacology, Toxicology, and Pharmaceutics. As a result of this activity, 1660 papers were selected. Articles were included through the following process: firstly, by reading the title (all), secondly by reading the abstract (202 articles), and thirdly by reading the full paper (37 articles).

A literature review indicates that the main topic of current scientific discussion in the protection area of Industry 4.0 is the issue of cyber security. It is a natural consequence of the numerous works on network technologies enabling Industry 4.0. An analysis of keywords showed that IoT is mentioned in 286 papers, machine learning in 83, virtual reality in 24, cloud computing in 48, blockchain in 35, and big data in 56. The prevalence of these issues has also been confirmed in review papers on trends in developing technologies supporting Industry 4.0 (Wang and Hsu, 2021; Chae and Olson, 2021; Ghobakhloo and Iranmanesh, 2021).

The work analyzed focuses on identifying the threats caused by network technologies. The results revealed a field of study in a fledgling stage, with a limited number of experts operating somewhat in isolation and offering single-point solutions instead of taking an integrated, holistic approach. Key publication outlets were identified, and the main focus of research undertaken to be in the technical areas of smart buildings, smart industry, and environmental sustainability (Xu *et al.*, 2020; Furstenau *et al.*, 2020; Kerin and Pham, 2019). For example, research findings indicate a roadmap for designing an IoT-based smart warehouse infrastructure. The findings of the study indicate the first critical components to design an IoT-based smart warehouse infrastructure. Second, essential factors contribute to the successful implementation of IoT-based smart warehouse infrastructure (Affia and Aamer, 2021).

Research conducted on Blockchain technology indicates it can contribute to the circular economy by helping to reduce transaction costs, enhance performance and communication along the supply chain, ensuring human rights protection, enhancing healthcare patient confidentiality and welfare, and reducing carbon footprint. Also in the study evaluated the challenges to blockchain implementation for the circular economy in terms of trust, illegal activities, the potential for hacking, and the need to address these through suitable legislation and policy development (Upadhyay *et al.*, 2021). Research on the Industrial Internet of Things (IIoT) shows that the IIoT enablers (digital technologies, connectivity, data, capabilities, and management) are highly related to the manufacturing network coordination mechanism. The results indicate that IIoT initiatives and manufacturing network coordination should be designed to support each other (Deflorin *et al.*, 2021).

A few works present solutions as holistic cybersecurity management where the decision-making model can select an optimal portfolio of security safeguards. All for minimize cybersecurity investment and expected cost of losses from security breaches in a supply chain (Stawik, 2020).

The topic of cyber security is complemented by analyses of the importance of other technologies for Industry 4.0. For example, the importance of radio frequency identification (RFID) is discussed, demonstrating its growing role in the coming years, and some specific challenges were observed and discussed (Gładysz *et al.*, 2021).

In addition to the challenges arising from the use of modern technologies supporting Industry 4.0, the literature also recognizes the risks arising from the changing role of humans in the production process. Research indicates that although automation and assistance technologies are becoming more prevalent in production and logistics, there is consensus that humans will remain an essential part of operations systems. It then develops a conceptual framework that integrates several key concepts from the human factors engineering discipline that are important in the context of Industry 4.0, and that should thus be considered in future research in this area.

The framework can be used in research and development to consider human factors in Industry 4.0 designs and implementations systematically. It enables the analysis of changing demands for humans in Industry 4.0 environments and contributes towards a successful digital transformation that avoids innovation's pitfalls without attention to human factors (Neumann *et al.*, 2021). As a result of the research, and organization-level maturity model was developed to optimize overall sociotechnical work system performance in the context of rapid technological development in manufacturing industries (Reiman *et al.*, 2021). Study results showed that lack of IT/digital skills has a critical role in workforce development for Industry 4.0 (Ozen and Kazancoglu, 2021).

Consideration of the security of elements identified as essential to Industry 4.0 does not consider all the threats to which the element of Industry 4.0 is susceptible. Available works focus on the impact of single technologies supporting Industry 4.0 or the role of humans in the new industrial reality. There is also no consideration and methods to consider different types of threats in the decision-making process to reduce the risk to an acceptable level. The available work is in the form of theoretical considerations identifying success factors or barriers to applying technologies supporting Industry 4.0.

This observation is also confirmed in studies on cybersecurity itself. Industry 4.0 implies that cyber risks of supply chain nodes can no longer be managed in isolation; rather, the cybersecurity investment should be addressed for the entire supply chain (Stawik, 2020). It confirms the research gap identified in the introduction to the paper.

2.4 The Protection of Critical Infrastructure

A review of available studies on CI was performed using a query of (3). The query returned 2209 papers. The areas of Engineering (1281 papers) and Computer Science (1056 papers) dominated the results.

KEY ((critical AND infrastructure OR ci) AND protection OR safety OR security OR resilience OR vulnerability) AND (EXCLUDE (PUBYEAR, 2000) OR EXCLUDE (PUBYEAR, 1998) OR EXCLUDE (PUBYEAR, 1995)) (3)

Due to the intent to identify methods for CI protection, a further reduction of the results obtained was made by excluding subject areas: Mathematics, Materials Science, Earth, and Planetary Sciences, Physics and Astronomy, Medicine, Arts and Humanities, Agricultural and Biological Sciences, Biochemistry, Genetics, and Molecular Biology, Psychology, Health Professions, Immunology and Microbiology, Nursing, Pharmacology, Toxicology, and Pharmaceutics. As a result of this activity, 1611 papers were selected. Articles were included through the following process: firstly, by reading the title (all), secondly by reading the abstract (214 articles), and thirdly by reading the full paper (42 articles).

The first use of critical infrastructure was attributed to president Bill Clinton's Commission on Critical Infrastructure Protection in 1996, and the concept received additional attention after the 9/11 attacks in 2001 (Moteff and Parfomak, 2004). The concept is centered on the notion that CI is of essential importance for economic security, defense of the state, and the functioning of the public. Many states have initiated activities targeted towards CI issues, e.g., establishing the European Program for Critical Infrastructure Protection (EPCIP) in 2006 (European Union, 2006). There is no consensus on which systems should be considered as CI. However, systems such as electrical power, transportation, health care, gas and oil, telecommunication, transportation, banking and finance, emergency services, continuity of government, and water supply are regularly considered as CI (Moteff, and Parfomak, 2004; European Union, 2006; Gellerbring *et al.*, 2014).

CI studies can be divided into two categories. The first part of the research study critical infrastructures and their respective issues, one by one. The other part of the research focuses on analyzing and governing critical infrastructures from a cross-sector perspective. However, the focal point of this paper is the second part. Despite their distinctive characteristics, CI cannot be managed as separate entities since they are dependent on each other (Rinaldi *et al.*, 2001; Johansson *et al.*, 2015; Luiijf *et al.*, 2010). These dependencies are crucial to consider when performing risk assessments (Setola nd Theocharidou, 2016; Johansson and Hassel, 2010; Haraguchi and Kim, 2016). If an adverse event is threatening to cause cascading disruptions to several dependent CI, it can be challenging to determine who is responsible for implementing risk-reducing measures (Utne *et al.*, 2011). These challenges require CI operators to cooperate and exchange information that should be processed and analyzed comprehensively.

However, cooperation poses a challenging task as managerial responsibilities tend to be fragmented among many actors (OECD, 2011). Such a context necessitates the development of approaches and frameworks that will allow mapping of CI characteristics, risk analysis, predicting adverse event scenarios, and proposing actions to reduce the level of risk in a multi-actor context.

Complicating factor is the issue of confidentiality, either for national security or for competitive reasons. Confidentiality prohibits sharing vital risk and vulnerability information between CI operators, which hinders a comprehensive approach to managing the security of dependent CI. This setting makes it difficult to understand and analyze the dependent behavior of CI and how to share, communicate and coordinate risk-related activities between key actors, which all are essential for effective cross-sector governance and decision-making (Arvidsson *et al.*, 2021).

In the reviewed literature, there is an evident limitation concerning the type of infrastructure sectors being studied. CI sectors such as finance, healthcare, food supply, public administration, safety and security, social insurance, and trade and industry are not present or, to a small extent, only included in combination with other sectors (3 papers). Instead, there is a clear dominance of sectors such as transportation (19 papers), energy (23 papers), water and sanitation (15 papers), and information and communication (7 papers). Consequently, there is a limited amount of CI papers that focus on more than one CI sector.

The lack of fewer technological sectors in the reviewed literature poses a challenge for attaining a more comprehensive picture of CI management and governance of cross-sector risks. For example, excluding the healthcare, finance, or public administration sectors is likely to overlook crosssector risks associated with these sectors. It can, for example, lead to an underestimation of the consequences that arise on a societal level, given CI adverse events in this sector. It is critical for CI research to also relate to these types of sectors and their dependencies, as is highlighted in OECDs report on governance for CI resilience (OECD, 2019).

Several articles focus on general CI topics, such as the overall strategies for management or protecting CI (Sajeva and Masera, 2006; Brem, 2015; Brassett and Vaughan-Williams, 2015), issues relating to the identification of CIs (Riegel, 2015; Fekete *et al.* 2012) and using CI as variables for estimating the vulnerability to flooding of various areas (Armenakis *et al.*, 2015; Johnston *et al.*, 2014). One way for researchers to analyze the behavior of interdependent CIs is to use models and simulation approaches for CI systems (Ouyang, 2014). However, these models, simulations, and validation require data collected under a single framework.

The ability to recognize and anticipate threats towards CI entities and indicate how to act when a threat occurs is of great practical importance. Many research initiatives have been recently carried on:

- the impact of CI on national security in the domains of economic development, state sovereignty, and the increase in the population's standard of living (Rehak, Markuci, and Hormada, 2016; Pursiainen, 2018),

- the mutual influence of systems of CI (Alcaraz and Zeadally, 2015; Macaulty, 2016; Chen and Milanovic, 2017; Bloomfield *et al.,* 2017),
- dependent risk (Edi and Rosato, 2016; Pescaroli and Kelman, 2017),
- methods from the domain of management science which can be adapted to issues management of CI safety (Ouyang, 2014; Hurley, 2017; Cai *et al.,* 2017; Tien and Kiureghain, 2017; Johansen and Tien, 2018),
- methods for exchange of information on the threats to which CI facilities are vulnerable (Caldwell, 2015; Häyhtiö and Zaerens, 2017),
- establishing a safety threshold[3] for the functionality of CI facilities (Manas, 2017; Hatton *et al.,* 2018).

However, the progress of research work in these areas is differential. Each study covers only one or two areas related to the CI safety management process. There is a lack of a proposal for a holistic solution that would create a set of safeguards based on the threats to which CI is vulnerable. The majority of research only indicates the need to develop dedicated methods and define the framework model for CI safety management (Hofreiter and Zvakova, 2016; Häyhtiö and Zaerens, 2017).

To address the above, one necessary component is the ability to compile and analyze a variety of data from several sectors. From a practical perspective, there is a need for more developed standards on managing and facilitating the sharing of CI data (Arvidsson *et al.,* 2021).

The analyzed articles indicate that there is no universal method for analyzing or managing CI-related risks. Instead, it is common to use a combination of methods to address the multitude of challenges. The reason may be the lack of a model mapping the characteristics of CI that is applicable in any sector of CI.

Another commonly available source of information on risk analysis methods and CI protection are crisis management methodologies. The strategies undertaken to maintain the safety of CI in many countries are defined in methodologies of risk assessment of crisis management. Those methodologies provide knowledge about the stages of the process of risk assessment and are a source of practical working methods for stakeholders responsible for CI safety. According to this criterion, the methodologies used in Poland (Kosieradzka and Zawiła-Niedźwiecki, 2017) and those of the countries that are considered leading in this domain, i.e., Germany (Bbk.bund.de, 2011), Sweden (Msb.se, 2012), Canada (Publicsafety.gc.ca, 2013), USA (FEMA, 1997), Ireland (Memie, 2010), Netherlands (Preventionweb.net, 2009) were analyzed. The criterion for selecting methodologies was built on the number of crisis events. The countries mentioned above have dealt with and the expert evaluation of the maturity of methodological solutions. Expert opinion was obtained through interviews with three employees of the Government Security Center.

[3] *Safety threshold - a level of functionality considered by the CI operator to be enough to fulfil the CI's duties under its commitment to society.*

The model for the methodologies mentioned above is PN-EN ISO 31000:2018 risk management - principles and guidelines, which assumes the implementation of the risk assessment process in three stages: setting the context, risk estimation (identification, analysis, and evaluation), and decision on dealing with the risk.

The analysis shows that almost all methodologies start from the stage of context setting. At this stage, the resources and threats to which they are vulnerable are identified. An exception to this rule is the Methodology of the Netherlands and the Methodology of Sweden. The methodology of the Netherlands' first stages is the development of an emergency scenario. The Methodology of Sweden starts with defining areas of responsibility and adopting the risk analysis method.

All methodologies assume implementing components of the risk assessment process recommended by PN-EN ISO 31000:2018, i.e., risk analysis and risk estimation. The final stage of risk assessment methodologies for the crisis management process, which was analyzed, was to decide how to deal with the risk. This decision was made based on results for the risk assessment stage containing the selection of adequate safeguards to eliminate or mitigate the risk.

An analysis of seven states' risk assessment methodologies for crisis management allowed for identifying the base stages and good practices related to CI safety management. The analysis also indicates the lack of a single standard of conduct in the domain of CI safety management, even though all methodologies refer to elements of PN-EN ISO 31000:2018. The lack of a single standard may result from the fact that the considered methodologies refer to the process of crisis management and not directly to the process of management of CI safety. Treating the process of management of CI safety as a part of the process of crisis management is a global tendency, as a result of which the attention is not paid to the development of the model of CI characteristics.

3. Research Methodology

The realization of the research goal was split into five stages, presented in detail in Table 1.

Table 1. *Stages of a research plan*

Stage of research	Research methods	Result of the stage
Analysis of issues of CI safety management	Literature research Analysis of original sources	Determination of stages in the methodology of CI safety management. Identification of good practices in the domain of management of CI safety.
Determination of the IMCIS concept	Literature research Analysis of original sources Research actions	Indication of methods and techniques in the domain of management sciences that could be applied in the framework of CI safety management. Identification of the set of tools used in the CI safety management. Development of the IMCIS concept.

Analytical and experimental validation of IMCIS components	Research actions Modelling Computational experiments	Development of IMCIS components.
Integration of IMCIS components	Research actions Computational experiments	Integration of IMCIS elements.
Verification of IMCIS using approximate real-world data	Research actions Computational experiments	Acknowledgment of the usability of IMCIS for entities responsible for the safety of CI.

Source: *Own elaboration.*

The literature review was done in two ways: using available review studies or using a knowledge base review using filters composed of keywords. Two databases were used for literature analysis: WoS, CC and Scopus. The search was limited to scientific research works published after 2001 because, in this year, the term "Critical Infrastructure" the concept received additional attention. Literature research in the domain of CI safety management allowed for the identification of factors negatively affecting the liaison of CI protection entities, determining differences in the definitions of critical infrastructure and CI protection, and the lack of a standard of characteristics of CI.

The comparative analysis of primary sources, regulatory acts, strategies, programs, standards, and risk assessment methodologies for crisis management allowed to establish the fundamental stages for the process of CI safety management. The conducted analysis of legal acts in crisis management and civil planning regulations, considering regulations of the EU Civil Protection Mechanism, allowed to create of the basic set of data the model of CI characteristics.

The relation between elements of IMCIS was designed using the modeling method and computation experiments (simulations) so that the results of one stage of the IMCIS were subsequently input data for another stage. The simulation method made it possible to approximate the reproduction of a phenomenon or behavior of an object by means of its model. It is a procedure in which random numbers are generated by probability. They are assumed to be associated with a source of uncertainty such as, for example, capital expenditures, sales revenues, operating costs, or risks to which companies are vulnerable. The data associated with the input variables are analyzed to determine the likely outcomes of the output variable and the risk assigned to it (Pawlak, 2012). Simulation methods are divided into two classes:

- deterministic simulation - the random components of the model are omitted, what in linear models- means operating on the expected values of individual variables,
- stochastic simulation - a random component and properties of its distribution are taken into account (then an appropriate subroutine generating realization

of a random component and taking into account real properties of its distribution must be embedded in the computational program).

The stochastic simulation was used in the study. The use of simulations allowed the reproduction of the CI structure. It means the developed model of CI characteristics. It makes it possible to analyze the impact of threat materialization on the studied objects in terms of effects and domino effect. Moreover, it is possible to check the effect of implementing additional safeguards.

The verification of IMCIS functionality was based on the computational experiments utilizing data characterizing PKN ORLEN Inc. refinery obtained from the Crisis Management Plan of Płock District (Powiat-plock.pl, 2015). Information on the structure of the investigated CI, the threats to which the considered objects are susceptible, and the applied safeguards were obtained from the Crisis Management Plan of Płock District. Specifically, data were extracted on the probability of threat occurrence. Data on CI functionality performance were obtained from reports published by ORLEN Inc (Orlen, 2016). On the other hand, the impact of threats on the functionality of CI and the impact of additional safeguards features were randomly generated.

The research process was complemented at various stages by the action research method consisting of presenting the results in expert panels organized for the research project Methodology of risk assessment for crisis management system in Poland. The so-called experts were employees of the Government Centre for Security. Action research is a philosophy and methodology of research generally applied in the social sciences. It seeks transformative change through the simultaneous process of taking action and doing research linked together by critical reflection. Kurt Lewin described action research as comparative research on the conditions and effects of various forms of social action and research leading to social action that uses a spiral of steps, each of which is composed of a circle of planning, action, and fact-finding about the result of the action (Zuber-Skerritt, Wood, 2019).

The presented case study of the IMCIS application uses the data to characterize a Rafinery PKN ORLEN Inc. (Powiat-plock.pl, 2015). The IBM Web Sphere Business Modeler 7.0 environment was used to execute the method of generating Adverse Event Scenarios (AES).

4. Integral Model of Critical Infrastructure Safety

As a result of the analysis of legal conditions governing the protection of CI, it has been established that each facility of this type constitutes a set of resources (V) allowing for the execution of obligations of the operator of CI, the so-called functionalities (Φ). The characteristics of CI also include the set of threats (Z) to which CI is vulnerable and the set of applied safeguards (M). Threats that materialize may be an excitation of other threats[4], e.g., a technical failure may reduce the functionality of the CI and, at the same time, cause a fire contributing to further damages. Therefore, the characteristics of CI have to be complemented by a set of relationships between threats (H).

There is also a dependency between the CI objects - set (G). The availability of the functionality of CI is a requirement for the functionality of another CI[5]. The loss or reduction of functionality creates conditions conducive to the threats to which other CIs are vulnerable.

Hence, CI's situation is defined as the state of CI at a considered point of time (determined in the domain of resources), functionality, threats, and safeguards, taking into account the dependence on the CI under consideration CI. Based on the above reasoning, a model of the situation of CI was created (equation 4).

$$\langle V, \Phi, Z, H, M, G, T \rangle \tag{4}$$

where:
V – considered CI,
Φ – set of CI functionalities,
Z – set of threats,
H – set of excitations of threats,
M – set of safeguards,
G – set of CI dependencies between CI entities,
T – a point of time of determining CI characterizes.

The definition of the CI situation model allows us to define the situation management of critical infrastructure safety as a set of activities in the area of management functions, depending on the CI situation, maintaining the aim to achieve the required safety threshold. IMCIS methods are used to establish a set of actions to improve the safety level:

- method of risk assessment,
- method of generating adverse event scenarios,
- method of formulation of the decision-making problem.

The indicator for IMCIS is the risk of loss of functionality expressed by equation (5).

$$R_{\alpha,\beta} = P_{\alpha,\beta} * |\Delta\Phi_{\alpha,\gamma}| * (U_{\alpha,\beta} - M_{\alpha,\beta}) \tag{5}$$

$U_{\alpha,\beta} - M_{\alpha,\beta} = 0$ for $M_{\alpha,\beta} \geq U_{\alpha,\beta}$

[4] *Excitation of threat - occurrence of favourable conditions for the materialisation of the threat*

[5] *Example: The sewage pumping station needs electricity to supply the pumps to collect waste. Breaking the catenary line causes lack of power supply to the pumps and loss of functionality of the sewage pumping station.*

where:
α - the CI index,
β - the index of threat,
γ - the index of the functionality of the considered CI,
Rα,β - the level of risk [0..100]%,
Pα,β - the probability of β threat on the scale [0..1],
Uα,β - the CI vulnerability to β threat on the scale [0..1],
ΔΦα,γ - the effect of β threat occurrence [0..100]%,
Mα,β - the impact of security on CI's vulnerability to β threat on a scale [0..1].

The loss of CI's considered functionality is a discrete random variable with a specific scale for each threat to which CI is vulnerable. These scales are equal to the probability of threat which may materialize $P_{\alpha,\beta}$ divided by the sum of the probabilities of the threats which affect CI (equation 6):

$$R_{\Phi_{\alpha,\gamma}} = \sum_{\alpha=1}^{n} \sum_{\beta=1}^{j} \frac{P_{\alpha,\beta}}{\sum_{\alpha=1}^{n} \sum_{\beta=1}^{j} P_{\alpha,\beta}} * |\Delta\Phi_{\alpha,\gamma}| * (U_{\alpha,\beta} - M_{\alpha,\beta}) \qquad (6)$$

where:
$R_{\Phi_{\alpha,\gamma}}$ – the level of risk of losing functionality at the considered CI,
j – number of threats to which a CI with an index α is vulnerable,
n – number of considered CI.
The knowledge of the value of the risk of loss of functionality in combination with data coming from the model of the situation of the CI makes it possible to determine what will be the availability of functionality when the threat occurs (equation 7):

$$\Phi_{\alpha,\gamma}(t_{n+1}) = \Phi_{\alpha,\gamma}(t_n) - R_{\Phi_{\alpha,\gamma}}(t_n) \qquad (7)$$

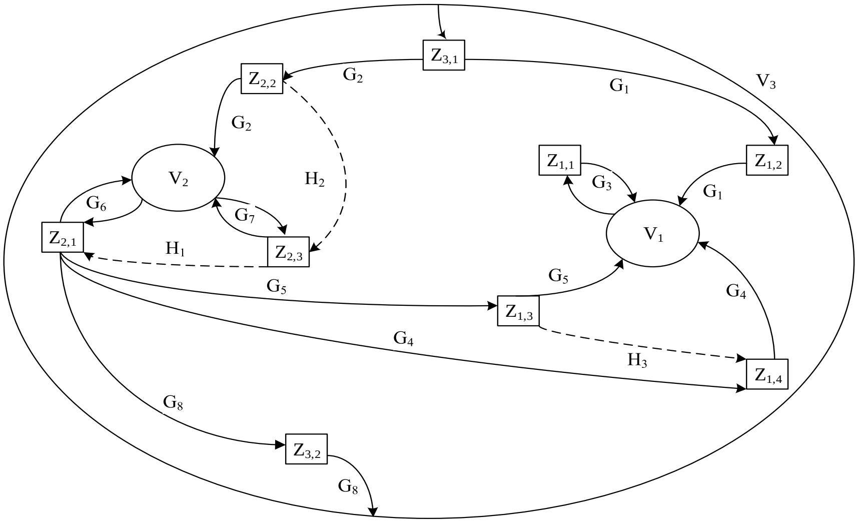
where:
$\Phi_{(\alpha,\gamma)}$ (t_{n+1}) - the expected level of functionality at the moment t_{n+1},
$\Phi_{(\alpha,\gamma)}$ (t_n) - the measured/estimated functional level at the moment t_n resulting from the Model of CI Situation,
$R_{\Phi_{\alpha,\gamma}}(t_n)$ - the level of risk of losing functionality at the considered moment t_n.

The ability to estimate the availability of functionality due to the occurrence of a threat allows us to define a strategy for dealing with the risk. The inclusion of adverse event scenarios (AES) in the risk analysis process responds to the need of the entities responsible for CI's safety, which have to prepare plans for responding to threats and use the resources at the right time and place. The adverse event spreading is due to the relationships that occur between CI or threats. Dependencies may be determined based on expert knowledge, statistical data, process analysis, or analysis of the models of CI situations.

The method of generating adverse event scenarios assumes two stages: developing a system of associated critical infrastructures (SACI) and establishing a SAC inventory. The creation of SACI includes the development of a graphical model (Figure 2), which consist of:

- nodes that represent random variables:
  - probability of the threat (symbols of rectangles),
  - the vulnerability of CI to threats (ellipse symbols),
- arrows connecting nodes understood as mapping the dependencies of threats (dotted arrows) and CI's dependencies (straight arrows).

***Figure 2.** Example of identification of CI dependencies in the considered model*



***Source:** Own elaboration.*

The development of the SACI and the use of Bayes's theory allow us to determine the probability of a sequence of events caused by the threat's occurrence. Establishing the level of risk resulting from the analysis of individual threats or the AES indicates the decision-making problems of the entities responsible for the safety of CI. The method for the decision problem developed for IMCIS is modifying the method for analysis of interconnected decision areas (AIDA). In IMCIS, the decision problem is understood as a set of decision areas ($Z_{\alpha,\beta}$) resulting from threats to which CI is vulnerable. The decision problem's solution is to create a combination of safeguards ($M_{\alpha,\beta,\lambda}$ elementary decisions), one for each decision area.

The relative importance of the decision-making area ($D_{\alpha,\beta}$) depends on the share of the risk associated with the considered threat in the total value of risks included in the model of CI or AES situation (equation 8):

$$D_{\alpha,\beta} = \frac{R_{\alpha,\beta}}{\sum_{\beta=1}^{j} R_{\alpha,\beta}} * 100 \tag{8}$$

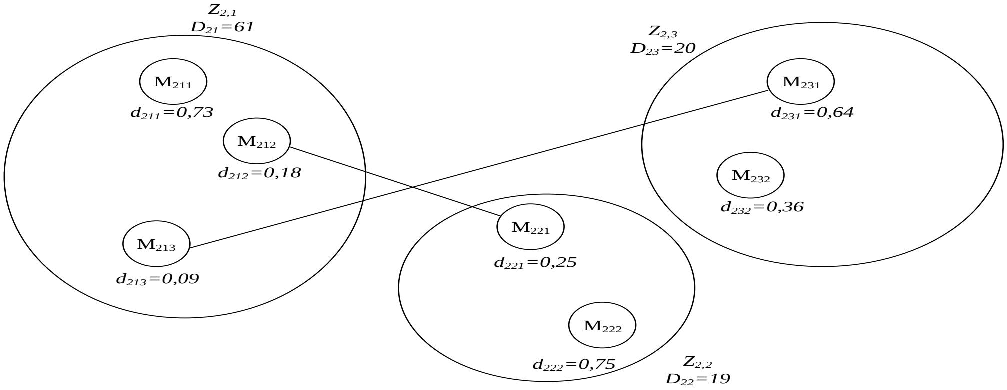
where:
$D_{\alpha,\beta}$ – the relative significance of the decision area related to the β-index threat,
j – a number of threats to which a CI is vulnerable.
The relative importance of an elementary decision is defined as the share of the impact of the considered safeguard in the total impact of the safeguards indicated for the decision area $Z_{\alpha,\beta}$ (equation 9):

$$d_{\alpha,\beta,\lambda} = \frac{m_{\alpha,\beta,\lambda}}{\sum_{\lambda=1}^{i} m_{\alpha,\beta,\lambda}} \qquad (9)$$

where:
$d_{\alpha,\beta,\lambda}$ – the relative importance of the λ elementary decision related to the threat with an index β, to which CI with an index α is vulnerable,
$m_{\alpha,\beta,\lambda}$ – the value of the increase in the resistance of the considered CI with an index α to a threat with index β as a result of using a safeguard with index λ,
i – number of all available safeguards to the entity responsible for the safety of CI, which can be used in reaction to a threat with an index β.

The contradiction of elementary decisions (conflict of safeguards) may result, among others, from technical, legal, organizational, or financial obstacles. The contradiction of elementary decisions can be used to implement the achievement of the SDGs. By mechanism the contradiction of elementary decisions solutions with negative environmental, economic or social impacts can be excluded. Using the AIDA method's principles, the contradiction of elementary decisions is marked with a continuous line connecting two elementary decisions of the decision problem (Figure 3).

Figure 3. *An example of a decision problem*



Source: *Own elaboration.*

The solution to the decision problem requires a cost assessment of all acceptable solutions for the decision problem (without safeguards conflicts). The decision problem can be presented in the form of a matrix equation (Table 2). The establishment of a cost assessment of the solutions to a decision problem can directly identify the best answer to maximize or minimize the impact of safeguards. The resolution is to decide on the highest or lowest cost rating. The cost assessment of solutions to a decision problem does not allow for a direct indication of decisions that fulfill the goal of maintaining functionality within the assumed range. In this case, the obtained solutions should be substituted for the risk equation (5). Its value calculated, and subsequently, the availability of functionality after the occurrence of the considered threats should be estimated using equation (7).

Table 2. *An example of cost estimation of solutions to a decision problem*

	$\mathbf{d_{2,1,\lambda}}$	$\mathbf{d_{2,2,\lambda}}$	$\mathbf{d_{2,3,\lambda}}$		$\mathbf{D_{2,\beta}}$		**Cost assessment**
Decision 1	$M_{2,1,1}$	$M_{2,2,1}$	$M_{2,3,1}$		$D_{2,1}$		$(M_{2,1,1*}\ D_{2,1})+(M_{2,2,1*}\ D_{2,2})+(M_{2,3,1*}\ D_{2,3})$
Decision 2	$M_{2,1,1}$	$M_{2,2,1}$	$M_{2,3,2}$		$D_{2,2}$		$(M_{2,1,1*}\ D_{2,1})+(M_{2,2,1*}\ D_{2,2})+(M_{2,3,2*}\ D_{2,3})$
Decision 3	$M_{2,1,1}$	$M_{2,2,2}$	$M_{2,3,1}$		$D_{2,3}$		$(M_{2,1,1*}\ D_{2,1})+(M_{2,2,2*}\ D_{2,2})+(M_{2,3,1*}\ D_{2,3})$
Decision 4	$M_{2,1,1}$	$M_{2,2,2}$	$M_{2,3,2}$	*		=	$(M_{2,1,1*}\ D_{2,1})+(M_{2,2,2*}\ D_{2,2})+(M_{2,3,2*}\ D_{2,3})$
Decision 5	$M_{2,1,2}$	$M_{2,2,2}$	$M_{2,3,1}$				$(M_{2,1,2*}\ D_{2,1})+(M_{2,2,2*}\ D_{2,2})+(M_{2,3,1*}\ D_{2,3})$
Decision 6	$M_{2,1,2}$	$M_{2,2,2}$	$M_{2,3,2}$				$(M_{2,1,2*}\ D_{2,1})+(M_{2,2,2*}\ D_{2,2})+(M_{2,3,2*}\ D_{2,3})$
Decision 7	$M_{2,1,3}$	$M_{2,2,1}$	$M_{2,3,2}$				$(M_{2,1,3*}\ D_{2,1})+(M_{2,2,1*}\ D_{2,2})+(M_{2,3,2*}\ D_{2,3})$
Decision 8	$M_{2,1,3}$	$M_{2,2,2}$	$M_{2,3,2}$				$(M_{2,1,3*}\ D_{2,1})+(M_{2,2,2*}\ D_{2,2})+(M_{2,3,2*}\ D_{2,3})$

Source: *Own elaboration.*

5. Case study

Rafinery PKN ORLEN Inc. area (V_1) includes Basell Orlen Polyolefins Ltd. (V_2) and ORLEN OIL Ltd. (V_3). These facilities belong to the group of companies whose mutual location is conducive to deepening the effects of adverse events. Due to their mutual location, it should be assumed that the CI under consideration is composed of these three facilities. Due to their technological processes, all three facilities are vulnerable to three threats: fire, explosion, and environmental contamination. In response to the threats, the operators of CI may apply similar safeguards: the facility fire brigade, the facility security service, the facility medical service, and environmental monitoring. The main activities of Rafinery PKN ORLEN Inc. are:

- $\Phi_{1,1}$ - the processing of crude oil and production of petroleum products and semi-finished products (refinery and petrochemicals),
- $\Phi_{1,2}$ - storage and warehousing of crude oil and liquid fuels as well as creation and maintenance of fuel stocks,
- $\Phi_{1,3}$ - generation, transmission, and trade in heat and electricity.

The main activity of Basell Orlen Polyolefins Ltd. is:

- $\Phi_{2,1}$ - production of polyethylene and polypropylene type artificial plastics.

The main activities of ORLEN OIL Ltd. Are:

- $\Phi_{3.1}$ - production of base oils,

- $\Phi_{3.2}$ - production of paraffin gauze,
- $\Phi_{3.3}$ - production of furfurol extract.

The situation of the CI under consideration is described in Table 3.

Table 3. *Synthetic record of the situation of the Refinery ORLEN Inc., the Basell Orlen Polyolefins Ltd., and the Orlen Oil Ltd.*

CI	Functionalities		Threats							Vulnerability
								Safeguards		
	Mark	Value of functionality	Mark	Type	Excited threat	Probability	Effect	Mark	Degree of reduction of vulnerability	
V_1	$\Phi_{1,1}$	93%	$Z_{1,1}$	IN	explosion, environmental contamination	0,7	-47% ($\Phi_{1,1}$)	$M_{1,1,1}$	0,46	0,88
							-37% ($\Phi_{1,2}$)			
							-13% ($\Phi_{1,3}$)	$M_{1,1,2}$	0,31	
	$\Phi_{1,2}$	93%	$Z_{1,2}$	IN	fire	0,56	-42% ($\Phi_{1,1}$)	$M_{1,2,1}$	0,16	0,81
							-39% ($\Phi_{1,2}$)			
							-46% ($\Phi_{1,3}$)			
	$\Phi_{1,3}$	93%	$Z_{1,3}$	IN	-	0,81	-9% ($\Phi_{1,1}$)	$M_{1,3,1}$	0,16	0,31
							-9% ($\Phi_{1,3}$)			
V_2	$\Phi_{2,1}$	93%	$Z_{2,1}$	IN	explosion, environmental contamination	0,42	-94% ($\Phi_{2,1}$)	$M_{2,1,1}$	0,27	0,56
								$M_{2,1,2}$	0,18	
			$Z_{2,2}$	IN	fire	0,35	-48% ($\Phi_{2,1}$)	$M_{2,2,1}$	0,17	0,91
			$Z_{2,3}$	IN	-	0,61	-5% ($\Phi_{2,1}$)	$M_{2,3,1}$	0,52	0,82
V_3	$\Phi_{3,1}$	93%	$Z_{3,1}$	IN	explosion, environmental contamination	0,58	-55% ($\Phi_{3,1}$)	$M_{3,1,1}$	0,05	0,92
							-34% ($\Phi_{3,2}$)			
							-65% ($\Phi_{3,3}$)	$M_{3,1,2}$	0,75	
	$\Phi_{3,2}$	93%	$Z_{3,2}$	IN	fire	0,52	-41% ($\Phi_{3,1}$)	$M_{3,2,1}$	0,14	0,83
							-27% ($\Phi_{3,2}$)			
							-38% ($\Phi_{3,3}$)			
	$\Phi_{3,3}$	93%	$Z_{3,3}$	IN	-	0,49	-18% ($\Phi_{3,1}$)	$M_{3,3,1}$	0,26	0,36
							-19% ($\Phi_{3,2}$)			
							-15% ($\Phi_{3,3}$)			

Source: *Own elaboration.*

Table 4 summarizes the risk of functionality loss of the CI due to threats occurrence to which they are vulnerable. The inherent and residual risk values have been calculated based on equation (5). The sum of risk for functionalities carried out by the CI has been calculated using the equation (6).

Table 4. *Synthetic record of the risk of functionality loss for considered CI entities*

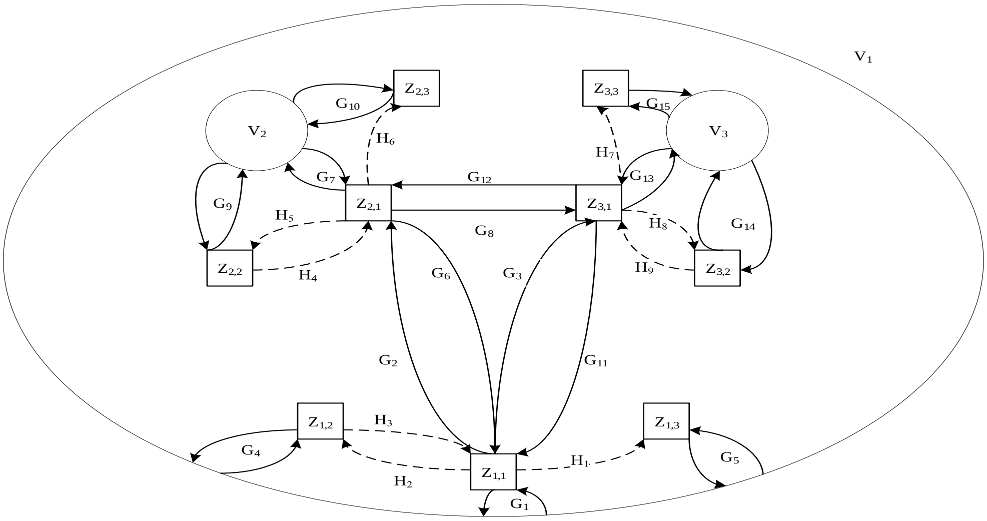
CI	Threat	Probability	Effect		Vulnerability	Safeguard	Inherent risk	Residual risk
V_α	$Z_{\alpha,\beta}$	P	$\Phi_{\alpha,\gamma}$	$\Delta\Phi_{\alpha,\gamma}$	$U_{\alpha,\beta}$	$M_{\alpha,\beta}$	R^i	R^r
V_1	$Z_{1,1}$	0,7	$\Phi_{1,1}$	47%	0,88	0,77	28,95%	3,62%
			$\Phi_{1,2}$	37%			22,79%	2,85%
			$\Phi_{1,3}$	13%			8,01%	1,00%
	$Z_{1,2}$	0,56	$\Phi_{1,1}$	42%	0,81	0,16	19,05%	15,29%
			$\Phi_{1,2}$	39%			17,69%	14,20%
			$\Phi_{1,3}$	46%			20,87%	16,74%
	$Z_{1,3}$	0,81	$\Phi_{1,1}$	9%	0,31	0,16	2,26%	1,09%

CI	Threat	Probability	Effect		Vulnerability	Safeguard	Inherent risk	Residual risk
V_α	$Z_{\alpha,\beta}$	P	$\Phi_{\alpha,\gamma}$	$\Delta\Phi_{\alpha,\gamma}$	$U_{\alpha,\beta}$	$M_{\alpha,\beta}$	R^i	R^r
			$\Phi_{1,3}$	9%			2,26%	1,09%
Sum of risk for						$\Phi_{1,1}$	50,26%	20,00%
						$\Phi_{1,2}$	40,48%	17,05%
						$\Phi_{1,3}$	31,13%	18,84%
V_2	$Z_{2,1}$	0,42	$\Phi_{2,1}$	94%	0,56	0,45	22,11%	4,34%
	$Z_{2,2}$	0,35	$\Phi_{2,1}$	48%	0,91	0,17	15,29%	12,43%
	$Z_{2,3}$	0,61	$\Phi_{2,1}$	5%	0,82	0,52	2,50%	0,92%
Sum of risk for						$\Phi_{2,2}$	39,90%	17,69%
V_3	$Z_{3,1}$	0,58	$\Phi_{3,1}$	55%	0,92	0,8	29,35%	3,83%
			$\Phi_{3,2}$	34%			18,14%	2,37%
			$\Phi_{3,3}$	65%			34,68%	4,52%
	$Z_{3,2}$	0,52	$\Phi_{3,1}$	41%	0,83	0,14	17,70%	14,71%
			$\Phi_{3,2}$	27%			11,65%	9,69%
			$\Phi_{3,3}$	38%			16,40%	13,63%
	$Z_{3,3}$	0,49	$\Phi_{3,1}$	18%	0,36	0,26	3,18%	0,88%
			$\Phi_{3,2}$	19%			3,35%	0,93%
			$\Phi_{3,3}$	15%			2,65%	0,74%
Sum of risk for						$\Phi_{3,1}$	50,22%	19,42%
						$\Phi_{3,2}$	33,15%	12,99%
						$\Phi_{3,3}$	53,73%	18,89%

Source: *Own elaboration.*

The collected data allowed to development of the SACI model (Fig. 4). The simulation of unfavorable events was based on 1000 cases of randomly chosen excitation of threats. As a result of experiment 94, AES was generated.

Figure 4. *Dependencies model of the Refinery ORLEN Inc., the Basell Orlen Polyolefins Ltd, and the Facility Orlen Oil Ltd.*



Source: *Own elaboration.*

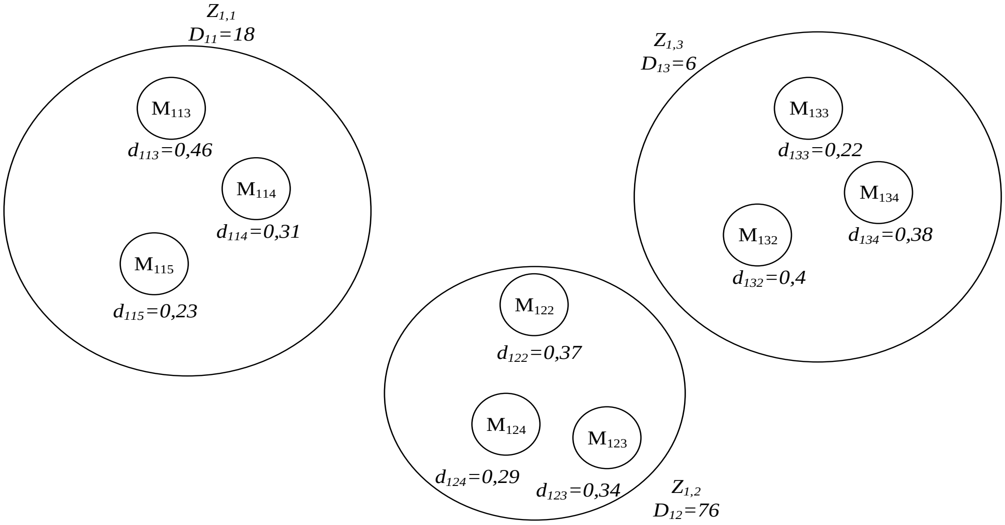
An example of a decision problem resulting from the CI's situation under consideration is the level of almost 20% risk of functionality loss $\Phi_{1,1}$ - the processing of crude oil and manufacturing products (Table 4). The risk of functionality loss $\Phi_{1.1}$ is composed of risks related to threats: $Z_{1.1}$ - fire ($R_{1.1}$ = 1.75%), $Z_{1.2}$ - explosion ($R_{1.2}$ = 7.39%) and $Z_{1.3}$ - environmental contamination ($R_{1.3}$ = 0.53%).

For the example of the calculation, it was assumed that the Rafinery PKN ORLEN Inc. operation is to maintain the functionality of Φ1.1 above the safety threshold established as 90%. Assuming the risk of 9.66% of lost $\Phi_{1.1}$ functionality and availability due to the occurrence of threats, $Z_{1.1}$, $Z_{1.2}$, $Z_{1.3}$ are forecasted at 83.34% (according to 7).

The established safety threshold and the value of the risk associated with the threats to which CI V_1 is vulnerable indicate that the decision problem has three decision areas determined by threats $Z_{1.1}$, $Z_{1.2,}$ and $Z_{1.3}$. Using equation (8), the relative importance of decision areas was calculated (Figure 5). To mitigate the risk of functionality loss, the operator of CI V_1 may apply additional safeguards used in the Rafinery LOTOS Inc. (LOTOS, 2018). Among the additional safeguards available to the operator of CI V_1, no conflicting pairs were indicated (listed safeguards may be used in any configuration).

Due to the lack of data on the effectiveness of the applied protections, their impact on the vulnerability of CI V_1 has been estimated on a scale from 0 to 1. 0 means total lack of effectiveness, and 1 is the total resistance to the threat. Using equation (9), the relative importance of elementary decisions was calculated (Figure 5).

Figure 5. *Illustration of the considered flat decision problem*



Source: *Own elaboration.*

The solution to the decision problem is presented in Table 5. The analysis of the results of the risk of functionality loss $\Phi_{1.1}$ and its forecast value indicates that with the assumed aim of maintaining availability and functionality above 90%, the operator of Rafinery PKN ORLEN Inc. may apply any combination of the considered safeguards. Each of the possible decisions allows us to maintain the availability of $\Phi_{1.1}$ functionality from 90.21% (decisions 8, 17, and 26) to 91.91% (decisions 1, 10, and 19).

Table 5. *List of decisions fulfilling the aim of the operation of the Rafinery PKN ORLEN Inc.*

Decision	Cost assessment	Value of the risk of losing $\Phi_{1,1}$ functionality	Forecasted value of $\Phi_{1,1}$ functionality
Decision 1	38,8	1,09%	91,91%
Decision 2	37,72	1,3%	91,67%
Decision 3	38,68	1,13%	91,87%
Decision 4	36,52	1,66%	91,34%
Decision 5	35,44	1,87%	91,13%
Decision 6	36,4	1,7%	91,3%
Decision 7	32,72	2,57%	90,43%
Decision 8	31,64	2,78%	90,21%
Decision 9	32,6	2,61%	90,39%
Decision 10	36,1	1,09%	91,91%
Decision 11	35,02	1,3%	91,67%
Decision 12	35,98	1,13%	91,87%
Decision 13	33,82	1,66%	91,34%
Decision 14	32,74	1,87%	91,13%
Decision 15	33,7	1,7%	91,3%
Decision 16	30,02	2,57%	90,43%
Decision 17	28,94	2,78%	90,21%
Decision 18	29,9	2,61%	90,39%
Decision 19	34,66	1,09%	91,91%
Decision 20	33,58	1,3%	91,67%
Decision 21	34,54	1,13%	91,87%
Decision 22	32,38	1,66%	91,34%
Decision 23	31,3	1,87%	91,13%
Decision 24	32,26	1,7%	91,3%
Decision 25	28,58	2,57%	90,43%
Decision 26	27,5	2,78%	90,21%
Decision 27	28,46	2,61%	90,39%

Source: *Own elaboration.*

Novel safeguards establish the new situation of the CI (Table 6). For the threat of $Z_{1.1}$ - fire, safeguard $M_{1.1.3}$ - fire-resistant linings have been added, for the threat of $Z_{1.2}$ - explosion, safeguard $M_{1.2.2}$ - a system for evacuation of vapors and gases to a gas torch has been added, for the threat of $Z_{1.3}$ - environmental pollution, safeguard $M_{1.3.2}$ - monitoring of technological parameters has been added.

Table. 6. *The situation of Rafinery PKN ORLEN Inc. after adding new safeguards*

CI	Functionalities	Threats

							Mark	Degree of reduction of vulnerability	
V_1	$Φ_{1,1}$	93%	$Z_{1,1}$	explosion, environmental contamination	0,7	-47% ($Φ_{1,1}$) -37% ($Φ_{1,2}$) -13% ($Φ_{1,3}$)	$M_{1,1,1}$	0,46	0,88
							$M_{1,1,2}$	0,31	
							$M_{1,1,3}$	0,71	
	$Φ_{1,2}$	93%	$Z_{1,2}$	fire	0,56	-42% ($Φ_{1,1}$) -39% ($Φ_{1,2}$) -46% ($Φ_{1,3}$)	$M_{1,2,1}$	0,16	0,81
							$M_{1,2,2}$	0,56	
	$Φ_{1,3}$	93%	$Z_{1,3}$	-	0,81	-9% ($Φ_{1,1}$) -9% ($Φ_{1,3}$)	$M_{1,3,1}$	0,16	0,31
							$M_{1,3,2}$	0,13	

Source: *Own elaboration.*

6. Discussion

The conducted literature research has shown that researchers and practitioners have divided opinions on which elements create Industry 4.0, how these elements are interrelated and where Industry 4.0 applies. Regardless of the definition, the idea of industry 4.0 indicates from centralized production towards production that is very flexible and self-controlled. Kolberg and Zuehlke (2015) present Industry 4.0 as a further development of CIM and thus as a network approach that complements CIM through ICT. The integration of automation technologies supports this approach, e.g., cyber-physical systems (CPS), collaborative robots, cloud computing, and big data sets, with the production environment via IoT (Xu *et al.*, 2018). This provides the opportunity to network the entire factory, creating an intelligent environment.

Industry 4.0 contributes to the SDGs builds connectivity between the industry and sustainability by finding a significant relation between their components. Therefore, Industry 4.0 depends on the efficiency of the infrastructure that provides access to energy, water, communication, transportation, ICT networks. Part of this infrastructure is called critical infrastructure.

The analyzed research indicates that the issue of CI appears in the context of technologies enabling the realization of the Industry 4.0 idea. Particularly many works in the area of using network technologies cyber-physical Systems, IoT, cloud computing, Industrial Integration, Enterprise Architecture, SOA, Industrial Information Integration, and others. The available study identified 26 drivers associated with Industry 4.0 that have an impact on improved BPM. Available studies indicate that Industry 4.0 is no longer a future trend. For many enterprises, it is now at the heart of their strategic and research agenda (PWC, 2016). In this context, Industry 4.0 and the technologies enabling its implementation may in the future be included in the CI category, on which the proper functioning of the economy, society, and public administration will depend.

Industry 4.0 comprises many complex components and has broad applications in numerous industrial sectors. At present, one of the challenges is making use of cutting-edge ICT and engineering technology to make Industry 4.0 successful (Mousterman and Zander, 2016; Xu *et al.*, 2018). This success depends on the undisturbed functioning of dispersed Industry 4.0 components. It indicates the need for risk analysis of many dependent resources not necessarily managed by the same operator. Identified risks require responses that must reduce the level of risk to the overall system and take into account multiple decision-making centers.

A literature review indicates that the main topic of current scientific discussion in the protection area of Industry 4.0 is the issue of cyber security. The work analyzed focuses on identifying the threats caused by network technologies. The results revealed a field of study in a fledgling stage, with a limited number of experts operating somewhat in isolation and offering single-point solutions instead of taking an integrated, holistic approach. In addition, consideration of the security of elements identified as essential to Industry 4.0 does not consider all the threats to which the element of Industry 4.0 is susceptible. Available works focus on the impact of single technologies supporting Industry 4.0 or the role of humans in the new industrial reality. There is also no consideration and methods to consider different types of threats in the decision-making process to reduce the risk to an acceptable level. The available work is in the form of theoretical considerations identifying success factors or barriers to applying technologies supporting Industry 4.0.

A few works present solutions as holistic cybersecurity management where the decision-making model can select an optimal portfolio of security safeguards. All for minimizing cybersecurity investment and the expected cost of losses from security breaches in a supply chain (Stawik, 2020).

Proper implementation of Industry 4.0 enabling sustainable enterprise development requires comprehensive identification of threats affecting a diverse set of resources forming the required infrastructure managed by many independent decision-making centers. Methods and models developed for CI facility management can be a solution to this problem. In particular, solutions developed through research that focuses on issues related to the analysis and management of critical infrastructure from a cross-sectoral perspective are attractive. One way for researchers to analyze the behavior of interdependent CIs is to use models and simulation approaches for CI systems (Ouyang, 2014). However, these models, simulations, and validation require data collected under a single framework.

This problem is solved by the Integral Model of Critical Infrastructure Safety. By using the research results, the model of CI situation (4) was elaborated. The CI situation model integrates data regarding CI characterization and the existing relations between threats and CI facilities. The model of the situation of CI was complemented with methods: risk estimation, generation of AES, and formulation of a decision problem, thus creating IMCIS.

The risk estimation method uses a risk equation that provides the risk value depending on the probability of threat occurrence, CI's vulnerability to the threat, the effects of applied safeguards, and the effects of the threat on the considered functionality of CI.

Utilizing the CI situation model, a method for generating the AES has been developed, which predicts the possible consequences of the occurrence of a threat and verify whether this model of CI situation takes into account all threats affecting CI. The first stage of this process uses data collected in models of CI situations to graphically illustrate random variables (probability of a threat and vulnerability of CI to threats) and relations between CI and relations between threats. In the second stage, SACI is implemented in a simulation tool.

Using the AIDA method and the model of CI situation, a method of formulating decision problems was developed. This approach allows the entities responsible for CI safety to identify the decision areas (threats to which CI is vulnerable), to define elementary decisions for each decision area (to identify available safeguards for responding to a threat), and to determine combinations of safeguards that fulfill the assumed aim (keep the expected availability and functionality levels above the safety threshold).

The presented study shows the usefulness of IMCIS for the entity responsible for CI safety. The scope of IMCIS usage depends on the country's legal conditions that would like to apply it. Table 6 shows a list of stages of analyzed risk assessment methodologies for crisis management, which IMCIS could potentially support.

The use of the CI situation model makes it possible to develop the characteristics of any infrastructure element, allowing for the implementation of Industry 4.0. Thanks to the relations between objects data forming the infrastructure and the data on the relations between threats, it is possible to develop a model of the entire infrastructure of Industry 4.0 in a considered enterprise. This model allows simulations of the domino effect caused by the materialization of a certain threat. These simulations allow us to determine the effects of the threat and determine the risk level linked to it. This risk level indicates the problem of decision-making areas in which it is necessary to identify additional safeguards to reduce the level of risk (ensuring a minimum level of availability of the object's functionality under consideration). Consequently, the reliability of the Industry 4.0 infrastructure in the considered company is increased, which translates into the effectiveness of sustainable development of the enterprise.

The Integral Model of Critical Infrastructure Safety allows for conducting analyses considering many independent decision-making centers, which is important from the point of view of technologies enabling Industry 4.0.

The Integral Model of Critical Infrastructure Safety does not solve the problem of data sharing between decision centers. Whether for national security or competitive reasons, the issue of confidentiality has to be addressed through other methods.

A limitation of the Integral Model of Critical Infrastructure Safety is that it has to be based on quantitative data. Currently, many CI operators do not have appropriate data sets. A similar situation may occur for companies implementing Industry 4.0 ideas.

Further research is needed to adapt the structure of decision-making areas to the requirements of Industry 4.0 and the concept of sustainable development. In particular, the balance between sustainability and Sustainable Development Goals.

7. Conclusions

The presented study shows that IMCIS has to integrate CI site characterization, risk assessment methods, adverse event scenario generation, and decision-making by many independent decision centers.

As a result of conducted analyses, universal elements characterizing CI objects are: set of CI functionalities, set of threats, set of excitations of threats, set of safeguards, set of CI dependencies between CI entities, a point of time of determining CI characterizes. The set of them can be freely extended to conduct detailed analyses characteristic for the considered CI sector.

The presented study shows the usefulness of IMCIS for the entity responsible for CI safety. The scope of IMCIS usage depends on the country's legal conditions that would like to apply it. Table 7 shows a list of stages of analyzed risk assessment methodologies for crisis management, which IMCIS could potentially support.

Table 7. *Stages of methodologies of risk assessment for crisis management supported by IMCIS*

Methodology	Stages of methodology supported by IMCIS
Poland	establishment of context, risk analysis, risk estimation, risk assessment
Australia	establishment of context, risk identification, risk analysis, risk manipulation
Sweden	risk assessment (risk identification, risk analysis), vulnerability assessment (capability assessment, vulnerability analysis), risk manipulation
Germany	description of the area under consideration, selection of threats and description of adverse event scenarios, impact assessment of the threat
Ireland	establishment of context, risk assessment
Canada	establishment of context, risk assessment, risk manipulation
The	development of scenarios, risk assessment, preparation of a summary report and

Netherlands	recommendations
USA	identification of resources, risk estimation (description of threats, classification of threats, an indication of possible actions mitigation of risk), development of risk mitigation plans

Source: *Own elaboration.*

Developed IMCIS is consistent with the conducted research on the CI protection domain. IMCIS is a platform for their integration and a proposal for operationalizing the concepts indicated in the work of Hofreite *et al.* (2016), and Häyhtiö and Zaerens (2017). Additionally, the approach to describing the CI characteristics and generating AES makes it possible to apply IMCIS to the management of essential services safety, which are responsible for public safety indicated in international legal acts (EU Journal of Laws 2016 No 194 item 1).

Developed IMCIS can be used to increase the reliability of the Industry 4.0 infrastructure of the company under consideration. Proper implementation of Industry 4.0 enabling sustainable development of the company requires comprehensive identification of threats affecting a diverse set of resources forming the required infrastructure managed by many independent decision-making centers. This problem is solved by the Integral Model of Critical Infrastructure Safety.

The use of the CI situation model makes it possible to develop the characteristics of any infrastructure element, allowing for the implementation of Industry 4.0. Thanks to the relations between objects data forming the infrastructure and the data on the relations between threats, it is possible to develop a model of the entire infrastructure of Industry 4.0 in a considered enterprise. This model allows simulations of the domino effect caused by the materialization of a certain threat. These simulations allow us to determine the effects of the threat and determine the risk level linked to it. This risk level indicates the problem of decision-making areas in which it is necessary to identify additional safeguards to reduce the level of risk (ensuring a minimum level of availability of the object's functionality under consideration). Consequently, the reliability of the Industry 4.0 infrastructure in the considered company is increased, which translates into the effectiveness of sustainable development of the enterprise.

References:

Adamik, A., Nowicki, M. 2020. Barriers to creating competitive advantage in the age of Industry 4.0-conclusions from international experience. In: Zakrzewska-Bielawska, A., Staniec, I. (Eds.), Contemporary Challenges in Cooperation and Coopetition in the Age of Industry 4.0, 3-43. Cham, Switzerland: Springer Nature Switzerland AG.

Affia, I., Aamer, A. 2021. An internet of things-based smart warehouse infrastructure: design and application. Journal of Science and Technology Policy Management, 2053-4620. doi: 10.1108/JSTPM-08-2020-0117.

Alcaraz, C., Zeadally, S. 2015. Critical Infrastructure Protection: Requirements and

Challenges for the 21st Century. International Journal of Critical Infrastructure Protection, 8, 53-66.

Armenakis, C., Du, E., Natesan, S., Persad, R., Zhang, Y. 2017. Flood risk assessment in urban areas based on spatial analytics and social factors. Geosciences. doi: 10.3390/geosciences7040123.

Arvidsson, B., Johansson, J., Guldaker, N. 2021. Critical Infrastructure, Geographical Information Science and Risk Governance: A systematic cross-field review. Reliability Engineering and System Safety. doi: 10.1016/j.ress.2021.107741.

Asif, M. 2020. Are QM models aligned with Industry 4.0? A perspective on current practices. Journal of Cleaner Production, 258. doi: 10.1016/j.jclepro.2020.120820.

Bbk.bund.de. 2011. Method of Risk Analysis for Civil Protection. Retrieved from: https://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/booklets_leaflets /Method_of_%20Risk_Analysis.pdf?__blob=publicationFile.

Bloomfield, R., Popov, P., Salako, K. 2017. Preliminary Interdependency Analysis: An Approach to Support Critical Infrastructure Risk Assessment. Reliability Engineering & System Safety, vol. 167, 198-217. doi: 10.1016/j.ress.2017.05.030.

Brassett, J., Vaughan-Williams, N. 2015. Security and the performative politics of resilience: Critical Infrastructure protection and humanitarian emergency preparedness. Security Dialogue. doi: 10.1177/0967010614555943.

Brem, S. 2015. Critical infrastructure protection from a national perspective. European 2 Journal of Risk Regulation. doi: 10.1017/S1867299X00004499.

Buer, S., Strandhagen, J., Chan, F. 2018. The link between Industry 4.0 and lean manufacturing: Mapping current research and establishing a research agenda. International Journal of Production Research, 56(8), 2924-2940. doi: 10.1080/00207543.2018.1442945.

Cai, B., Xie, M., Liu, Y. 2017. A Novel Critical Infrastructure Resilience Assessment Approach using Dynamic Bayesian Networks. Book Series: AIP Conference Proceedings, vol. 1890. doi: 10.1063/1.5005245.

Caldwell, B. 2015. Framing, information alignment, and resilience in distributed human coordination of critical infrastructure event response. Procedia Manufacturing, vol. 3, 5095-5101. doi: 10.1016/j.promfg.2015.07.524.

Chae, B., Olson, D. 2021. Technologies and applications of Industry 4.0: insights from network analytics. International Journal of Production Research. doi: 10.1080/00207543.2021.1931524.

Chen, Y., Milanovic, J. 2017. Critical Appraisal of Tools and Methodologies for Studies of Cascading Failures in Coupled Critical Infrastructure Systems. IEEE EUROCON 2017 -17th International Conference on Smart Technologies, 599-604. doi: 10.1109/EUROCON.2017.8011182.

Colicchia, C., Strozzi, F. 2012. Supply chain risk management: A new methodology for a systematic literaturę review. Supply Chain Manag, 17, 403-418.

Colombo, A., Schleuter, D., Kircher., M. 2015. An Approach to Qualify Human Resources Supporting the Migration of SMEs into an Industry 4.0-compliant Company Infrastructure. IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society, 3761-3766. doi: 10.1109/IECON.2015.7392687.

Deflorin, P., Scherrer, M., Schillo, K. 2021. The influence of IIoT on manufacturing network coordination. Journal of Manufacturing Technology Management. doi: 10.1108/JMTM-09-2019-0346.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (EU Journal of Laws 2016 No 194 item 1).

Edi, M., Rosato, V. 2016. Critical Infrastructure Disruption Scenarios Analyses via Simulation. In: Kacprzyk, J. (Eds.), Managing The Complexity of Critical Infrastructures: A Modelling and Simulation Approach, 43-61. Springer Open. doi: 10.1007/978-3-319-51043-9.

Ejsmont, K., Gladysz, B., Kluczek, A. 2020. Impact of Industry 4.0 on Sustainability – Bibliometric Literature Review. Sustainability, 12, 5650. doi: 10.3390/su12145650.

European Union. 2006. European Commission. Communication from the Commission on a European Programme for Critical Infrastructure Protection. Brussels. Retrieved from: https://eur-lex.europa.eu/legal _content/EN/ALL/?uri=celex%3A52006DC0786.

Fekete, A., Lauwe, P., Geier, W. 2012. Risk management goals and identification of critical infrastructures. Int J Crit Infrastruct. doi: 10.1504/IJCIS.2012.050108.

FEMA. 1997. Multi-Hazard Identification and Risk Assessment. Retrieved from: https://www.fema.gov/media-library/assets/documents/7251.

FEMA. 2017. Sandy five years later. Retrieved from: http://fema.gov/sandy-5-year.

Furstenau, L., Sott, M., Homrich, A., Lopez-Robles, J., Cobo, M. 2020. 20 years of scientific evolution of cybersecurity: A science mapping. In: Proceedings of the International Conference on Industrial Engineering and Operations Management, 314-325. Dubai, UAE.

Gellerbring, B., Holmgren, A., Rinne, A., (Eds.). 2014. Vägledning för samhällsviktig verksamhet – Att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid.

Ghadge, A., Weis, M., Caldwell, N., Wilding, R. 2020. Managing Cyber Risk in Supply Chains: A Review and Research Agenda. Supply Chain Management, 25 (2), 223-240. doi: 10.1108/SCM-10-2018-0357.

Ghobakhloo, M., Iranmanesh, M. 2021. Digital transformation success under Industry 4.0: a strategic guideline for manufacturing SMEs. Journal of Manufacturing Technology Management. doi: 10.1108/JMTM-11-2020-0455.

Gierszewska, G. (Eds.). 2020. Zarządzanie w przedsiębiorstwie N.0. Droga do przyszłości (Management in the N.0 enterprise: The way to the future). Warsaw: Oficyna Wydawnicza Politechniki Warszawskiej.

Gladysz, B., Corti, D., Montini, E. 2021. Forecasting the development of RFID technology. Management, and Production Engineering Review, 12(1), 38-47.

Hatton, T., Brown, C., Kipp, R. 2018. Developing a Model and Instrument to Measure the Resilience of Critical Infrastructure Sector Organisations. International Journal of Critical Infrastructures, vol. 14, issue 1, 59-79.

Haraguchi, M., Kim, S. 2016. Critical infrastructure interdependence in New York City during Hurricane Sandy. International Jurnal Disaster Resil Built Environ, 7, 133-143. doi: 10.1108/IJDRBE-03-2015-0015.

Häyhtiö, M., Zaerens, K. 2017. A Comprehensive Assessment Model for Critical Infrastructure Protection. Management and Production Engineering, vol. 8, nr 4, 42-53.

Hermann, M., Pentek, T., Otto, B. 2016. Design Principles for Industrie 4.0 Scenarios. Proceedings of 2016 49th Hawaii International Conference on Systems Science. doi: 10.1109/HICSS.2016.488.

Hofreiter, L., Zvaková, Z. 2016. Theoretical Aspects of Critical Infrastructure Protection. In:

Kravcov, A., Cherepetskaya, E., Pospichal, V. (Eds.) Durability of Critical Infrastructure, Monitoring and Testing. Lecture Notes in Mechanical Engineering. Springer, Singapore. doi: 10.1007/978-981-10-3247-9_16.

Hossain, M., Thakur, V. 2020. Benchmarking healthcare supply chain by implementing Industry 4.0: a fuzzy-AHP-DEMATEL approach, Benchmarking. Journal of Science and Technology Policy Management, 28(2), 556-581. doi: 10.1108/BIJ-05-2020-0268.

Hurley, J. 2017. Quantifying Decision Making in the Critical Infrastructure via the Analytic Hierarchy Process (AHP). International Journal of Cyber Warfare and Terrorism, vol. 7, issue 4, 23-34.

Ivanov, D., Tang, C., Dolgui, A., Battini, D., Das, A. 2020. Researchers' Perspectives on Industry 4.0: Multidisciplinary Analysis and Opportunities for Operations Management. International Journal of Production Research. doi: 10.1080/00207543.2020.1798035.

Jasperneite, J. 2012. Was Hinter Begriffen Wie Industrie 4.0 Steckt. Computer & Automation, 12, 24-28.

Johansson, J., Hassel, H. 2010. An approach for modeling interdependent infrastructures in the context of vulnerability analysis. Reliab Eng Syst Saf. doi: 10.1016/j.ress.2010.06.010.

Johansson, J., Hassel, H., Cedergren, A., Svegrup, L., Arvidsson, B. 2015. Method for describing and analyzing cascading effects in past events: Initial conclusions and findings. ESREL 2015. doi: 10.1201/b19094-581.

Johnston, A., Slovinsky, P., Yates, K. 2014. Assessing the vulnerability of coastal infrastructure to sea-level rise using multi-criteria analysis in Scarborough. Ocean Coast Management. doi: 10.1016/j.ocecoaman.2014.04.016.

Johansen, C., Tien, I. 2018. Probabilistic multi-scale modeling of interdependencies between critical infrastructure systems for resilience. Sustainable and Resilient Infrastructure, vol. 3, issue 1, 1-15.

Joshi, A. 2016. Comparison between Scopus and ISI Web of Science. J. Glob., vol. 7, 1-11.

Kagermann, H., Lukas, W., Wahlster, W. 2011. Industrie 4.0 – Mitdem Internet er Dinge auf dem Wegzur 4. Industriellen Revolution (Industry 4.0: With the Internet of Things towards 4th industrial revolution). VDI nachrichten, nr 13-2011.

Kagermann, H., Wahlster, W., Helbig, J. 2013. Recommendations for Implementing the Strategic Initiative Industrie 4.0: Final Report of the Industrie 4.0 Working Group. Acatech-National Academy of Science and Engineering. Retrieved from: https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf.

Kerin, M., Pham, D. 2019. A review of emerging industry 4.0 technologies in remanufacturing. Journal of Cleaner Production, 237, 117805.

Kolberg, D., Zuehlke, D. 2015. Lean automation enabled by Industry 4.0 technologies. IFACPapersOnLine, 48(3), 1870-1875. doi: 10.1016/j.ifacol.2015.06.359.

Kosieradzka, A. Zawiła-Niedźwiecki, J. (Eds.). 2017. Advanced Risk Assessment Methodology in Public Crisis Management. Warsaw: Warsaw University of Technology Faculty of Management.

Kumar, S., Suhaib, M., Asjad, M. 2020. Industry 4.0: Complex, disruptive, but inevitable. Management and Production Engineering Review, 11(1), 43-51. doi: 10.24425/mper.2020.132942.

Lasi, H., Peter, F., Thomas, F., Hoffmann, M. 2014. Industry 4.0. Business & Information Systems Engineering, 6(4). doi: 239–242.10.1007/s12599-014-0334-4.

LOTOS, 2018. Information about the threats occurring. Retrieved from: http://m.odpowiedzialny.lotos.pl/repository/39634.

Luiijf, H., Nieuwenhuijs, A., Klaver, M., Van Eeten, M., Cruz, E. 2010. Empirical findings on European critical infrastructure dependencies. Int J Syst Eng, 2, 3-18. doi: 10.1504/IJSSE.2010.035378.

Macaulty, T. 2016. Critical Infrastructure – Understanding its Component Parts, Vulnerabilities, Operating Risk, and Interdependencies. London – New York: CRC Press.

Manas, P. 2017. The Protection of Critical Infrastructure Objects - Technical Principles. In: Kravcov, A., Cherepetskaya, E., Pospichal, V. (Eds.) Durability of Critical Infrastructure, Monitoring and Testing. Lecture Notes in Mechanical Engineering. Springer, Singapore. doi: 10.1007/978-981-10-3247-9_27.

Mem. i.e. 2010. A Guide to Risk Assessment In Major Emergency Management. Retrieved from: http://mem.ie/wp-content/uploads/2015/05/A-Guide-to-Risk-Assessment.pdf.

Moeuf, A., Pellerin, R., Lamouri, S., Tamayo-Giraldo, S., Barbaray, R. 2017. The Industrial Management of SMEs in the Era of Industry 4.0. International Journal of Production Research. doi: 10.1080/00207543.2017.1372647.

Młody, M., Weinert, A. 2020. Industry 4.0 in Poland: A Systematic Literature Review and Future Research Directions. In: Zakrzewska-Bielawska, A., Staniec, I. (Eds.) Contemporary Challenges in Cooperation and Coopetition in the Age of Industry 4.0. Springer Proceedings in Business and Economics. Springer, Cham. doi:10.1007/978-3-030-30549-9_2.

Moteff, J, Parfomak, P. 2004. Critical infrastructure and key assets: definition and identification. Retrieved from: https://sgp.fas.org/crs/RL32631.pdf.

Mousterman, P., Zander, J. 2016. Industry 4.0 as a Cyber-Physical System Study. Software and Systems Modeling, 15(1), 17-29. doi: 10.1007/s10270-015-0493-x.

Mrugalska, B., Wyrwicka, M. 2017. Towards lean production in Industry 4.0. Procedia Engineering, 182, 466-473. doi: 10.1016/j.proeng.2017.03.135.

Msb.se. 2012. Swedish National Risk Assessment 2012. Retrieved from: https://www.msb.se/RibData/Filer/pdf/26621.pdf.

Neumann, W., Winkelhaus, S., Grosse, E., Glock, C. 2021. Industry 4.0 and the human factor – A systems framework and analysis methodology for successful development. International Journal of Production Economics, 233, 107992. doi: 10.1016/j.ijpe.2020.107992.

OECD. 2011. Future Global Shocks. Paris: Organisation for Economic Co-operation and Development. Retrieved from: https://www.oecd.org/governance/48329024.pdf.

OECD. 2019. Good Governance for Critical Infrastructure Resilience. Retrieved from: https://www.oecd-ilibrary.org/deliver/02f0e5a0-en.pdf?itemId=/content/publication/02f0e5a0-en&mimeType=pdf.

Orlen. 2016. Orlen Group Integrated Report 2016. Retrieved from: https://raportzintegrowany2016.orlen.pl.

Ouyang, M. 2014. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. Reliability Engineering & System Safety, vol. 121, 43-60.

Ozen, O., Kazancoglu, Y. 2021. Analyzing workforce development challenges in the Industry 4.0. International Journal of Manpower. doi: 10.1108/IJM-03-2021-0167.

Pawlak, M. 2012. Symulacja Monte Carlo w analizie ryzyka projektów inwestycyjnych (Monte Carlo simulation in the risk analysis of investment projects). Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 690.

Pescaroli, G., Kelman, I. 2017. How Critical Infrastructure Orients International Relief in

Cascading Disasters. Journal of Contingencies and Crisis Management, vol. 25, 2, 56-67.

Peukert, B., Benecke, S., Clavell, J., Neugebauer S., Nissen, N., Uhlmann, E., Lang, L., Finkbeiner, M. 2015. Addressing Sustainability and Flexibility in Manufacturing Via Smart Modular Machine Tool Frames to Support Sustainable Value Creation. Procedia CIRP, vol. 29, 514-519. doi: 10.1016/j.procir.2015.02.181.

Powell, K., Peterson, S. 2017. Coverage and Quality: A comparison of Web of Science and Scopus databases for reporting faculty nursing publication metrics. Nurs, 65, 572-578.

Powiat-plock.pl. 2015. Plan of Crisis Management. Retrieved from: http://powiat-plock.pl /attachments/article/44.

Preventionweb.net. 2009. Working with Scenarios, Risk Assessment and Capabilities in the National Safty and Security Strategy of Netherland. Retrieved from: https://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf.

Publicsafety.gc.ca. 2013. All Hazards Risk Assessment Methodology Guidelines. Retrieved from: https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ll-hzrds-rsk-ssssmnt-en.aspx.

Pursiainen, C. 2018. Critical infrastructure resilience: A Nordic model in the making? International Journal of Disaster Risk Reduction, vol. 27, 632-641.

PWC. 2016. Industry 4.0: Building the Digital Enterprise. London: PWC.

Queiroz, M., Fosso Wamba, S., Machado, M., Telles, R. 2020. Smart production systems drivers for business process management improvement: An integrative framework. Business Process Management Journal, 26(5), 1075-1092. doi: 10.1108/BPMJ-03-2019-0134.

Rinaldi, S., Peerenboom, J., Kelly, T. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag, 2, 11-25. doi: 10.1109/37.969131.

Raj, A., Dwivedi, G., Sharma, A., Lopes de Sousa Jabbour, A., Rajak, S. 2020, Barriers to the adoption of industry 4.0 technologies in the manufacturing sector: An inter-country comparative perspective. International Journal of Production Economics, vol. 224. doi: 10.1016/j.ijpe.2019.107546.

Riegel, C. 2015. Spatial criticality - Identifying CIP hot-spots for German regional planning. International Journal of Critical Infrastructure. doi: 10.1504/IJCIS.2015.072157.

Rehak, D., Markuci, J., Hromada, M. 2016. Quantitative Evaluation of the Synergistic Effects of Failures in a Critical Infrastructure System. International Journal of Critical Infrastructure Protection, vol. 14, 3-17.

Reiman, A., Kaivooja, J., Parviainen, E., Pekka-Takala E., Lauraeus, T. 2021. Human factors and ergonomics in manufacturing in the industry 4.0 context – A scoping review. Technology in Society, vol. 65. doi: 10.1016/j.techsoc.2021.101572.

Sajeva, M., Masera, M. 2006. A strategic approach to risk governance of critical infrastructures. Int J Crit Infrastruct, 2, 379-395. doi: 10.1504/IJCIS.2006.011346.

Setola, R., Theocharidou, M. 2016. Modelling Dependencies Between Critical Infrastructures. Management Complex Critical Infrastructure, 19-41. doi: 10.1007/978-3-319-51043-9_2.

Stawik, T. 2020, A linear model for optimal cybersecurity investment in Industry 4.0 supply chains. International Journal of Production Research. doi: 10.1080/00207543.2020.1856442.

Strozzi, F., Colicchia, C., Creazza, A., Noè, C. 2017. Literature review on the Smart Factory concept using bibliometric tools. International Journal of Production Research, 55, 6572-6591. doi: 10.1080/00207543.2017.1326643.

Szołtysek, J. 2014. Przesłanki i założenia koncepcji logistyki społecznej (The Conditions and the Concept of Social Logistics). Gospodarka Materiałowa i Logistyka, vol. 2, 2-7.

Tien, I., Kiureghian, A. 2017. Reliability Assessment of Critical Infrastructure Using Bayesian Networks. Journal of Infrastructure Systems, vol. 23, issue 4.

Xu, L. 2020. The contribution of systems science to Industry 4.0. Systems Research and Behavioral Science, 37(4), 618-631. doi: 10.1002/sres.2705.

Xu, L., Xu, E., Li, L. 2018. Industry 4.0: State of the art and future trends. International Journal of Production Research 56(8), 2941-2962. doi: 10.1080/00207543.2018.1444806.

Upadhyay, A., Mukhuty, S., Kumar, V., Kazancioglu, Y. 2021. Blockchain technology and the circular economy: Implications for sustainability and social responsibility. Journal of Cleaner Production, 293, 0959-6526. doi: 10.1016/j.jclepro.2021.126130.

Utne, I., Hokstad, P., Vatn, J. 2011. A method for risk modeling of interdependencies in critical infrastructures. Reliability Engineering System Safety, 96, 671-678. doi: 10.1016/j.ress.2010.12.006.

Van Eck, N., Waltman, L. 2017. Accuracy of citation data inWeb of Science and Scopus. In: Proceedings of the 16th International Conference of the International Society for Scientometrics and Informetrics, 16-20 October, Wuhan, China, 1087-1092.

Wang J., Hsu, C. 2021. A topic-based patent analytics approach for exploring technological trends in smart manufacturing. Journal of Manufacturing Technology Management, vol. 32, issue 1, 110-135. doi: 10.1108/JMTM-03-2020-0106.

Zuber-Skerritt, O., Wood, L. (Eds.). 2019. Action Learning and Action Research: Genres and Approaches. UK: Emerald Publishing Limited. doi: 10.1108/978-1-78769-537-520191001.