IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 5 July 2022, accepted 26 July 2022, date of publication 1 August 2022, date of current version 10 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3195337

TOPICAL REVIEW

Industry 4.0 Solutions Impacts on Critical Infrastructure Safety and Protection–A Systematic Literature Review

MICHAL WISNIEWSKI[1], BARTLOMIEJ GLADYSZ[2], KRZYSZTOF EJSMONT[2], ANDRZEJ WODECKI[1], AND TIM VAN ERP[3]

[1]Faculty of Management, Warsaw University of Technology, 02-524 Warsaw, Poland
[2]Faculty of Mechanical and Industrial Engineering, Warsaw University of Technology, 02-524 Warsaw, Poland
[3]University of Southern Denmark, 5230 Odense, Denmark

Corresponding author: Michal Wisniewski (michal.wisniewski@pw.edu.pl)

ABSTRACT In today's turbulent and complex times, the importance of the functional security and continuity of critical infrastructure (CI) is of particular importance. The Industry 4.0 (I4.0) toolset contains many technologies that support CI or are an integral part thereof. The purpose of this paper is to examine the relationship between CI and I4.0. The goal will be achieved by (1) conducting a systematic literature review using VOSviewer, (2) identifying leading research topics using Latent Dirichlet Allocation, (3) mapping the results obtained and identifying possibilities for further research. Web of Science, Scopus, and a set of specific keywords were used to select peer-reviewed papers presenting evidence of the considered connections. Selected clusters and topics were used to build a reference framework formed by relations between CI and I4.0. The results revealed that despite the popularity of both issues, studies examining the mutual relations between the same are lacking. The added value of the article is that it organizes the knowledge related to relations between I4.0 and CI, and indicates the research areas that require further scrutiny. It is the first comprehensive literature review focusing specifically on CI & I4.0.

INDEX TERMS Bibliometrics, critical infrastructure, Industry 4.0, literature review, reference framework, smart manufacturing.

I. INTRODUCTION

A. INDUSTRY 4.0 BACKGROUND

Industry 4.0 (I4.0) was first introduced in 2011 as a strategic initiative of the German government [1], [2]. Many modern economies launched similar initiatives, e.g. US' Advanced Manufacturing Partnership', Chinese 'Made in China', British' Smart Factory', Japanese' Super Smart Society', and others [3]. Majstorovic and Mitrovic listed almost 40 national programs under the category of I4.0 [4].

The purpose of the paper is to show the spectrum of I4.0-related topics covered in the in the available literature, especially in the context of links to critical infrastructure. The authors intentionally do not limit themselves to the main currents related to I4.0 by presenting the results of analysis of data available in bibliometric databases.

The idea of I4.0 is to transition from centralized production towards greater flexibility and self-control. This direction naturally follows from the historical developments in computer integrated manufacturing (CIM) and flexible manufacturing systems (FMS) [5] made in past decades, as well as the mass digitization observed in recent years [6]–[8]. I4.0 is a network approach that complements CIM through ICT [9]. It is worth mentioning that the development of the toolset of I4.0 solutions and technologies has benefited not only the

The associate editor coordinating the review of this manuscript and approving it for publication was Francisco Perez-Pinal.

manufacturing sector but also the service sector (e.g. big data solutions in banking or marketing).

With the current advanced technologies, the ideas of CIM and FMS could be implemented at significantly lower (more rational) costs. I4.0 is technology-driven and its toolset covers technologies and solutions such as flexible automation, cyber-physical systems (CPSs), industrial Internet of Things (IIoT), embedded sensors, collaborative and cognitive robotics, cloud and edge computing, big data, computer modeling and simulations, additive manufacturing (3D printing), artificial intelligence, or the industrial Digital Twin [10]–[14].

Substantial benefits are expected from I4.0 technologies and solutions, e.g., more accurate forecasting and planning, shorter lead times, an increase of energy efficiency, decrease of waste, workplace improvements (an increase of ergonomics and occupational health and safety), etc. However, relatively early phases of the I4.0 technologies' lifecycle imply serious questions and concerns regarding, e.g. the related social threats, economic effectiveness, or environmental impact. These can prove cost-intensive and lead to difficulties estimating the actual financial benefits and economic effectiveness, as well as problems related to increased electro-waste, energy consumption, the incidence of human-robot interaction issues, technophobia, unemployment threats, or privacy issues to name just a few [15].

An additional problem is the issue of security, which may be defined differently by each entity. Safety involves a wide range of things, systems, and processes. The security issues could be categorized into three levels, namely, the process level, the data level, and the infrastructure level. Manufacturing companies may define the security of their operations as the continuity of their own processes, for example. Service enterprises operating in cyberspace will define security as: availability, integrity and confidentiality of processed data. CI operators, on the other hand, will focus on the security of managed infrastructure in the context of: cyber security, physical security, technical security, legal security, personal security and business continuity. The accepted understanding of the concept of security determines the set of actions implemented with the intention of protecting the enterprise's operations.

Commonly labelled as the ABCD (i.e., artificial intelligence, blockchain, cloud computing, big data analytics) technologies are essential in enhancing the safety and security of I4.0 systems. However, the digital twin (DT) also plays an important role. DT could be depicted as the successor of the computer simulation approach. It could be used to support the design and flexible reconfiguration of the system. DT enables quick validation and tests to locate the malfunction and inefficiency reasons, rule out the mistakes, and test the practicability and safety/security of physical solutions in a cyber environment [16]–[18].

The Internet of Things (IoT) facilitates the integration of automation technologies under this approach within the production environment [10]. This allows the assets of an entire factory to become interconnected, creating an intelligent network. I4.0 applications also impact systems reliability affecting the same in two distinct ways. On the one hand, they increase reliability by providing new functionalities (like forecasting, planning, real-time data acquisition, etc.). On the other hand, I4.0 technologies facilitate new subsystems and maintenance that need integration with each other and the existing environment [19].

In this paper, the authors focused on safety, which involves many things, systems, and processes. Instead of more narrow and technical security issues, that could be categorized into three levels (process, data, infrastructure). Many studies highlight options to apply different technologies to I4.0 solutions and systems to enhance systems' security, transparency, and traceability.

Special attention is currently put to blockchain solutions and their abilities to obtain:

- sustainable manufacturing and lifecycle [20]–[22],
- secure digital twin technology (off-chain and on-chain merger) [23],
- anti-counterfeiting of things in the industrial internet.

Some current studies focus not only on physical signatures, e.g. optical technologies like QR codes, radio technologies like UHF RFID or NFC, among others, but also on biological features or edible chemical signatures for things counterfeiting in an I4.0 context [24], [25]. Blockchain security is an issue itself as well [26]. The picture shows that some areas like blockchain are discussed in detail on many levels. However, those studies are focused on technical issues. They miss the broader business context of critical infrastructure, where efficacy is over effectiveness. They also ignore the broader context of the holistic environment that is the I4.0 system and focus purely on security aspects, leaving more complex safety issues not covered.

Therefore, I4.0 is dependent on the efficacy of the infrastructure providing access to energy, water, communications, transport, and ICT networks. A part of this infrastructure is referred to as Critical Infrastructure (CI).

B. CRITICAL INFRASTRUCTURE BACKGROUND

The term ''critical infrastructure'' was first coined by president Bill Clinton's 1996 Commission on Critical Infrastructure Protection, and the concept received additional attention after the 9/11 attacks in 2001 [27]. It is centered on the notion that CI is of essential importance for economic security, national defense, and the public. However, there is no global consensus as to which systems should be considered as elements of CI. The specific identification of CI depends on the preference of the state in question. However, systems such as electrical power, transportation, healthcare, gas and oil, telecommunications, transportation, banking and finance, emergency services, continuity of government, and water supply are commonly included [28], [29].

Regardless of the definition, CI components are subjected to different types of threats due to the behavior of individuals, natural disasters, military operations, terrorism, or cybercrime. The efficacy of CI, measured by the availability of

its functionality, determines the citizens' perception of safety, rate of economic growth, social satisfaction, the sovereignty of the state, and effectiveness of public administration entities. Limited functionality of CI results in economic losses, environmental pollution, and a threat to the population's health and life [30].

Research pertaining to CI can be divided into two categories. The first focuses on particular critical infrastructures and their respective issues on a case by case basis, and the second on analyzing and governing critical infrastructures from a cross-sector perspective. The reviewed literature shows an evident limitation concerning the type of the infrastructure sectors analyzed. CI sectors such as finance, healthcare, food supply, public administration, safety and security, social insurance, and trade and industry are not considered or, in several cases, only included in combination with other sectors. Instead, there is a clear focus on sectors such as transportation, energy, water and sanitation, and information and communications. Many research initiatives have recently been carried out in terms of:

- the overall strategies of CI management or protection [31], [32],
- using CI as variables when estimating the vulnerability of various areas to flooding [33], [34],
- the impact of CI on national security in the domains of economic development, state sovereignty, and improvement of the overall standard of living [35], [36],
- the mutual interactions between CI systems [37], [38],
- dependent risk [39], [40],
- methods from the domain of management science which can be adapted to the management of CI safety [41],
- methods of exchanging information on threats to which CI facilities are vulnerable [42], [43],
- establishing a safety threshold for the functionality of CI facilities [44], [45].

C. INDUSTRY 4.0 ROLES IN CRITICAL INFRASTRUCTURE

Some I4.0 technologies will soon become or are already becoming integral parts of CI, e.g.

- Several manufacturing and service sectors widely consider the use of big data, blockchain, and edge computing technologies [46], [47];
- Cybersecurity is rapidly developing and the readiness to fend off large-scale attacks on critical infrastructure has improved dramatically [48], e.g. in the energy sector in the Gulf Cooperation Countries [49], manufacturing sector [50];
- Artificial intelligence supports CI systems [51], [52];
- Industrial automation [53], robotics [54], sensors, CPS [55], [56], IIoT [57], digital twins [58] enrich decision makers with data and enable extensive preventive and resilience capacities in CI;
- Parts manufactured using additive manufacturing can enhance the technical resilience of CI [59], but also create new potential targets for attacks (physical and cybernetic) within safety-critical infrastructure.

Consequently, I4.0 is dependent on CI but at the same time also shapes the same through technological applications [60].

CI systems provide the basis for utilizing I4.0 technologies, and thus impact overall economic, environmental, and social sustainability. The complexity of the relationship between sustainability, I4.0, and CI requires a holistic approach to the management of CI safety, understood as maintaining business continuity. However, the progress of research done in areas relevant to CI varies. Studies cover only excerpts related to the CI safety management process. There is a lack of a proposal for a holistic solution to CI safety management. Therefore, said safety becomes dependent on I4.0 solutions, which means that apart from the efficacy paradigm, it should also be considered from a sustainability perspective.

I4.0 is also discussed in terms of its impact on national security [44]. Some systems and solutions combine recently emerging new technologies, e.g., cyber-physical systems, but no single technology is likely to solve a problem without being integrated with other technologies. Combined, all such technologies might find applications in in CI systems. Therefore, I4.0 could deliver benefits in terms of better CI management, increased CI protection, etc. At the same time, however, when I4.0 solutions become integral parts of CI systems, they become additional sources of potential risk as the respective subsystems must be considered in terms of their safety and security [45] (especially occupational health [46], cybersecurity [47]), and reliability [48], etc.).

Considering the rapidly increasing popularity of I4.0 solutions, their increasingly important role in industrial systems, and the importance of CI security for businesses and economies, the goal of the present study is to deduce their relations and interactions by analyzing the existing body of scientific peer-reviewed literature. In this paper, a literature-based analysis is performed to determine the relationship between I4.0 and CI across different industries. CI and I4.0 relations are still quite fuzzy. The analytical approach proposed below entails a comprehensive qualitative assessment based on a literature review and bibliometrics. Therefore, the paper is focused on a systematic literature network analysis with a view to identifying connections between I4.0 and CI by analyzing the citation network, co-occurrence of keywords network, and Latent Dirichlet Allocation approaches. The review presented below is oriented towards investigating the mutual relationship between CI and I4.0. Therefore, this paper can provide a rationale for understanding the range of interest and implications of I4.0 applications in CI. Furthermore, it contributes to systematizing the existing knowledge about concepts that were traditionally discussed separately (I4.0 and CI). It furthers the trend towards integrating the same, makes a valuable theoretical contribution to the body of scientific literature in the research field, and suggests directions for further study. This will allow scholars and other interested parties to conduct more complex research on the development of quantitative assessment methods combining CI and I4.0, which are still few and far between.

In the context of existing scientific articles, the following paper contributes to the present state of scientific knowledge by providing a comprehensive and systematic review of literature pertaining to CI and I4.0 by:

- Rationalizing and systemizing the state-of-the-art knowledge on the considered topics using the dynamic Systematic Literature Network Analysis;
- Presenting the literature analysis in terms of its three dimensions: (1) systematic review, (2) type and application of reviewed study, and (3) bibliographic networks of the literature review;
- Attempting to provide answers to research questions addressed in current, relevant studies;
- Contributing to the existing body of research literature focused on combining the concepts in question.

The paper is structured as follows. Section 2 presents the research methodology and the bibliometric software used. Then results of the systematic literature network analysis are described in Section 3. Section 4 discusses results derived from the SLNA-based reference framework illustrating the discovered CI and I4.0 relations. Directions for future research are also described in Section 4, while Section 5 outlines the conclusions.

II. MATERIALS AND METHODS

A. SELECTION OF METHODS AND TOOLS

The dynamic development of scientific research in many fields combined with its increasing interdisciplinarity has contributed to the overall body of scientific knowledge, but has also made it difficult for researchers to keep themselves up to date with the current state of research. Limited cognitive resources prevent a complete review of the literature, and the selection of publications based on search engines using specific ranking algorithms runs the risk of omitting interesting papers with a low number of citations, but with high potential impact. As a result, it becomes increasingly difficult to obtain a reasonably comprehensive picture of research in a given field and identify an interesting research gap.

In such situations, data mining and machine learning methods can be employed, especially in terms of natural language processing and analysis, knowledge extraction, and document classification. Clustering and visualization techniques using tools such as VOSviewer [61]–[63], topic modeling analysis methods [64], or trend detection [65] are particularly popular among researchers. The maturity and continuous improvement of these methods encourages researchers to develop methodologies for employing the same in literature review processes as supplementary tools or even, in some cases, in lieu of actually reading scholarly articles. For example, Buchkremer *et al.* [66] proposed the STIRL (Generation and Application of Systemic Taxonomies via Information Retrieval and Semantic Learning) methodology, where they use various data mining and machine learning methods in the stages of information retrieval, taxonomy enhancement, topics mapping, cleaning, corpus creation, evolution, topics and trends identification, predictive analytics and results presentation.

We employed a systematic literature review method, deepened by Global Citation Score (GCS) analysis and network analysis, by using the VOSviewer tool. This was followed by Latent Dirichlet Allocation (LDA) to identify leading topics of research conducted in the I4.0 and CI areas.

The literature search was conducted in two scientific databases: Web of Science Core Collection (WoSCC) and Scopus. The databases were chosen because they are the most-commonly used when conducting literature searches [67] and are also leading databases with significant scientific impact scores. Due to their restrictive indexing procedures, the documents returned from queries processed in the databases tend to be of good quality [68]. The databases are also considered to be the two most important multidisciplinary bibliometric databases [69] used for field delineation [70].

Due to evident similarities between the databases, many authors have commented on their preference for one over the other [71]. For example, Scopus has about 60% more records and includes in-press articles. WoSCC is better when we want to find more accurate citation information [72] and identify 'high-influence' papers [73]. Since both databases have their advantages and disadvantages, it was decided to use both in the present study.

B. SYSTEMATIC LITERATURE REVIEW

A systematic literature review was chosen as a research method to discover relations between I4.0 advancements and issues relevant to critical infrastructure. A systematic review was chosen as it entails strict procedures in searching for and selecting papers to be reviewed, and is therefore ''effective in synthesizing what the collection of studies are showing in a particular question and can provide evidence of the effect that can inform policy and practice'' [74].

The exploration of the existing literature on the relationships (one-way and two-way) between CI and I4.0 was based on the identification of available studies, which in turn was facilitated by a specific set of keywords. The selection of relevant papers for bibliometric research focused on the construction of a search query covering various terms, synonyms, and abbreviations related to the words ''critical infrastructure'' and ''Industry 4.0''. To identify all such relevant terms, synonyms, and abbreviations, the authors analyzed the most cited or recent literature reviews on critical infrastructure [75]–[78] and Industry 4.0 [15], [12], [79], [80] available in the WoSCC and Scopus databases.

The selection of keywords relevant to CI was based on a keyword analysis drawing on 3,290 articles on the topic published since 2018 [75]. The keyword selection was based on the scoping study framework [81]. A scoping study is designed to map the literature relevant to a subject or research area to support the identification of key concepts, research gaps, or evidence to inform practice, policymaking, and research [82]. The discussed scoping study framework [81] is

in line with other systematic review methodologies, e.g. the PRISMA approach [83]. The search strings were iterated to encompass a broad range of articles related to CI. This was achieved by iteratively modifying the search string to either include new keywords or add new restrictions. For example, in some countries, the terms ''lifeline systems'' or ''vital societal function'' are used synonymously to critical infrastructure [36], [84]. There is no real consensus as to exactly which systems or institutions should be considered as critical infrastructures, although different categorizations in national policy frameworks show significant similarities [27], [29]. The eventual selection of keywords for CI was done using the Article Score. The Article Score is developed based on the principle that an article with many high-ranking keywords is more relevant to a given research field than an article with only a few low-ranking keywords. This resulted in a list of CI-related keywords that were used to prepare the queries for this paper. The original set of keywords was modified by excluding the names of critical infrastructure systems, i.e., transportation system, energy system, financial system, etc. This procedure was done to find cross-cutting works on multiple CI systems.

The term ''Industry 4.0'' is mainly used in Europe and is often associated with the Fourth Industrial Revolution. The concept of Industry 4.0 was first presented in 2011, and a full description thereof was first published in 2013 [1]. The core of Industry 4.0 is smart manufacturing, defined by the National Institute of Standards and Technology (NIST) as ''a fully integrated, collaborative manufacturing system that responds in real-time to meet changing requirements and conditions in the factory, in the supply chain, and the needs of customers'' [85]. On other continents, this paradigm is most often referred to as ''smart factory'', ''smart manufacturing'' or ''advanced manufacturing'' [70]. The use of different names results from national strategies that have been developed in response to the need to increase the competitiveness of national economies, especially in the area of manufacturing. A full list of Industry 4.0 equivalent programs is presented in the paper [3]. Literature reviews from various journals were used to include all the common terms, synonyms, and abbreviations applicable to 'Industry 4.0', [3], [15], [79], [80]. There are also other, less popular terms/synonyms related to Industry 4.0, such as industrial Internet or industrial Internet of Things (IIoT), cyber manufacturing, digital transformation, cyber-physical (production) system (CPS), cloud manufacturing, etc. [79]. It should be noted that many terms treated as synonyms of Industry 4.0 are correspond in fact to either its main technologies (IIoT, CPS, big data) or its underlying purpose (digital transformation). For this reason, such terms were not included in the query. It is also worth noting that in the vast majority of papers, apart from the specific terms mentioned above, the term Industry 4.0 itself also appears in the title/abstract/keywords.

In both cases (critical infrastructure and Industry 4.0), abbreviations were omitted to include only papers where the complete term appears in the abstract. In this case, adding abbreviations would only artificially inflate the number of results by including texts where those abbreviations are used in other meanings. Based on the above keyword considerations, the query was formulated for the search within titles, keywords, and abstracts, without a time restriction. The query was entered into the Scopus

$$\begin{aligned} &TITLE-ABS-KEY \\ &((\text{“}critical\ infrastructure\text{”}\ or\ \text{“}criticalbase\text{”} \\ &\quad OR\ \text{critical substructure}\ OR\ \text{critical services} \\ &\quad OR\ \text{key services}\ OR\ \text{key resources} \\ &\quad OR\ \text{“essential services”}\ OR\ \text{“crisis management”}) \\ &\quad AND \\ &\quad (\text{“}Industrie\ 4.0\text{”}\ OR\ \text{“}Industry\ 4.0\text{”} \\ &\quad OR\ \text{4th Industrial Revolution} \\ &\quad OR\ \text{Fourth Industrial Revolution} \\ &\quad OR\ \text{smart manufacturing}\ or\ \text{smart factory} \\ &\quad OR\ \text{smart enterprise}\ or\ \text{enterprise 4.0} \\ &\quad OR\ \text{“}factory\ 4.0\text{”})) \\ &\quad AND \\ &LANGUAGE(english) \end{aligned} \tag{1}$$

and WoSCC databases on November 26, 2021. The dataset obtained from the WoSCC database was fully contained in the dataset obtained from Scopus, hence only the results from the Scopus query are presented hereinbelow.

$$\begin{aligned} &TITLE-ABS-KEY \\ &((\text{“}critical\ in\ frastructure\text{”}\ or\ \text{“}criticalbase\text{”} \\ &\quad OR\ \text{critical substructure}\ or\ \text{critical services} \\ &\quad OR\ \text{key services}\ or\ \text{key resources} \\ &\quad OR\ \text{“}essential\ services\text{”}\ or\ \text{“}crisis\ management\text{”}) \\ &\quad AND \\ &\quad (\text{“}Industrie\ 4.0\text{”}\ or\ \text{“}Industry\ 4.0\text{”} \\ &\quad OR\ \text{4th Industrial Revolution} \\ &\quad OR\ \text{Fourth Industrial Revolution} \\ &\quad OR\ \text{smart manufacturing}\ or\ \text{smart factory} \\ &\quad OR\ \text{smart enterprise}\ or\ \text{enterprise 4.0} \\ &\quad OR\ \text{“}factory\ 4.0\text{”})) \\ &\quad AND \\ &LANGUAGE(english) \end{aligned} \tag{2}$$

This step is very important, because the results may change if another query is used. This choice was made in line with the aim of the paper, i.e., presenting the landscape of scientific literature pertaining to the relationship between critical infrastructure and Industry 4.0. The selected set of keywords allowed the analysis of specific topics and their trends using the adopted methodology.

Only studies in English (including papers in press) with available abstracts and references were considered for further

analysis (inclusion criteria). There were no other exclusion criteria, so documents of all types could be considered and no other restrictions were imposed in terms of the time of publication, affiliations, etc. Altogether, 129 papers from Scopus were considered in further analyses.

C. BIBLIOGRAPHIC NETWORK ANALYSIS USING VOSVIEWER

We calculated the Global Citation Score (GCS) to detect groundbreaking publications. GCS corresponds to the total number of citations in the Scopus database. Studies with high GCS are considered seminal or have a significant impact on the area of knowledge to which they relate [86]. In other words, GCS allows the identification of papers that form the basis of a given field, which are often used by other authors to develop their publications. Citations from the entire Scopus database are counted, even if they are from articles that have not been identified or selected.

To identify recent groundbreaking studies that could have a potentially large impact and promising scientific input on Industry 4.0 & critical infrastructure, papers were ranked according to the number of citations received in the entire Scopus database in 2021, divided by the number of years since the year of publication. This allowed the identification of those studies that have (potentially) low GCS but have recently gained considerable interest from the scientific community. This process 'weighed' citations received in 2021 based relative to the 'lifespan' of papers. The ranking of papers prepared in this way is shown in Table 2.

We also performed a network analysis in terms of the co-occurrence network for authors' keywords and citation network analysis using the VOSviewer approach and tool. Co-occurrence analysis aims to analyze information characteristics. It applies to words, authors, classifications, and other record fields in books, journals, proceedings, and other literature [87]. There are three basic types of co-occurrence analyses [88]: (i) author co-occurrence (co-operation analysis), (ii) author-keywords co-occurrence (coupling analysis), (iii) keywords co-occurrence (co-word analysis). In the paper, it was decided that the author's keywords co-occurrence analysis will be used. This analysis allowed us to obtain the results that are the most important from the point of view of the purpose of the article. It concerns the analysis of keywords indicated by authors in their studies. This method of quantitative analysis allows one to discover the structure of the research area within the considered set of papers and its potential importance for the discipline. Due to the increasingly accurate bibliographic indexing, co-word analysis is widely used nowadays to analyze keywords in books and journals. Author's keywords co-occurrence analysis allows one to obtain information on the number of times that given keywords appeared simultaneously in a published article [89]. Co-occurrence of the author's keywords creates a map in which the size of the nodes corresponds to the frequency of the keyword, while the lines show the relationships between respective keywords [90]. A citation network is a network where the nodes are papers, and the links mean that there are citations between them. Hence, we can observe the flow of knowledge as well as trace the citation connections between papers. This, in turn, makes it possible to isolate clusters (smaller networks), which include papers with least a single connection with another paper within the cluster. Among other reasons, this is done to facilitate easier definition of the thematic scope of the cluster.

D. LATENT DIRICHLET ALLOCATION

This part of our study aimed to identify and analyze the most important topics in the area of I4.0 usage in critical infrastructure, its safety, and management using the Latent Dirichlet Allocation (LDA) method. This provided the basis for generating a fairly comprehensive representation of the current research related to the discussed subject matter. Latent Dirichlet Allocation is one of the most popular topic modeling methods used in scientific research to identify key research topics or research trends in fields such as medical sciences, software engineering, political sciences, geography, or enterprise architecture [91], [92]. First introduced by Blei, Ng, and Jordan [93], it is a generative probabilistic model of a corpus. It represents topics by word probabilities, and the words with the highest probabilities in each topic serve as an idea of the topic characteristics. To make the interpretation easier, Chuan, Manning, and Heer introduced Termite: a method for visualizing and interpreting topics [94], which later inspired Sievert and Shirley to create LDAvis: one of the most popular methods used for LDA results interpretation [95].

The input for the LDA analysis was a clean dataset containing Authors, Titles, and Abstracts from the Scopus database. LDA was used to analyze all the identified papers discussing applications of the I4.0 toolset in Critical Infrastructure management extracted from Scopus using (1).

In our analysis, we used an open-source PyCaret library [96] which utilizes a reliable LDA algorithm implementation supported by the LDAvis visualization technique. In the first step, we initiated the model with the most popular irrelevant words (e.g., use, paper, research, start, etc.) as the so-called stop-words. Next, we performed an intrinsic evaluation and computed a coherence value to identify the optimal number of topics. The highest coherence score ($= 0.35$) we obtained for four topics. The research procedure used in the article is illustrated in Fig. 1.

E. OTHER METHODS

In our analysis, we also applied two other topic modeling and knowledge extraction methods: BERTopic and Knowledge Graphs. BERTopic, a topic modeling technique based on the BERT (Bidirectional Encoder Representations from Transformers) model [97] resulted in an exceptionally high number of outliers (75 out of 129 articles did not fit into any of the topics). On the other hand, knowledge graphs generated with the use of a SpaCy.io library [98] displayed a very high number of relations making it very difficult to infer topic

TABLE 1. The incidence of "critical infrastructure" and "Industry 4.0" topics in scientific databases as at Sep. 1, 2021.

Query	Scopus	WoS CC
"critical infrastructure"	11,574 Query: TITLE-ABS-KEY ("critical infrastructure")	5,200 Query: TS = ("critical infrastructure")
"Industry 4.0"	16,884 Query: TITLE-ABS-KEY ("industry 4.0")	10,307 Query: TS = ("industry 4.0")
"critical infrastructure" AND "Industry 4.0"	64 Query: TITLE-ABS-KEY ("industry 4.0" AND "critical infrastructure")	23 Query: TS = ("industry 4.0" and "critical infrastructure")

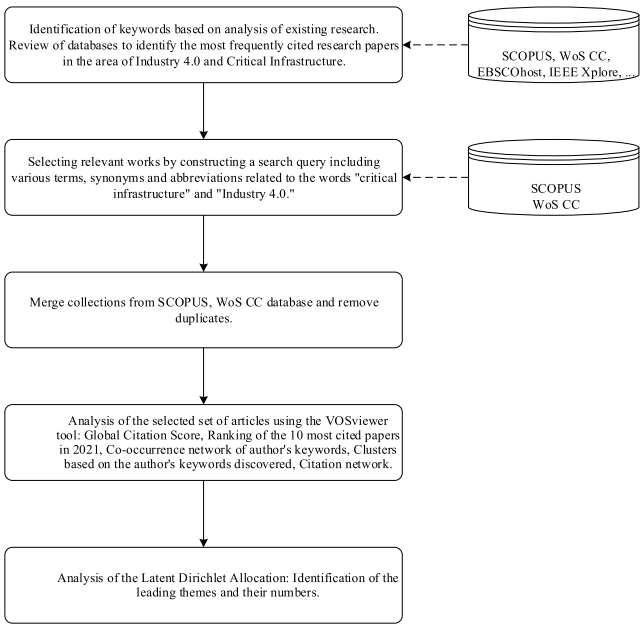

FIGURE 1. The research procedure used in the article.

groups. That is why in this paper, we limited our analysis to LDA and VOSviewer.

The initial results for BERTopic and knowledge graphs justified our decision to focus solely on LDA application to the I4.0 toolset (methods, technologies, tools) in our Critical Infrastructure review: interested readers can find a more in-depth LDA presentation in e.g. [92], [93], [95].

III. RESULTS

A. GENERAL POPULARITY OF TOPICS

Given that the relationship between CI and I4.0 is such a niche topic, it was initially decided to search the Scopus and Web of Science Core Collection databases only for ''critical infrastructure'', for ''Industry 4.0'', and for a conjunction of the same. Under these criteria, the number of papers identified oscillated between 700,000 and 800,000. The results for the full terms ''critical infrastructure'' and ''Industry 4.0'' found in the titles, abstracts, and keywords of papers listed in the Scopus and Web of Science Core Collection databases are presented in Table 1.

Despite the much larger total number of texts on critical infrastructure and Industry 4.0 in the Scopus database (see Table 1), the proportions of texts tackling both issues to the summarized number of all found papers are ca. 2.0‰ (Scopus) and 1.5‰ (WoS CC). That was a good symptom – because it indicated that in both databases the subject of CI & I4.0 taken jointly is rarely discussed. The above considerations proved that critical infrastructure and Industry 4.0 are both separately considered as highly important and interesting. However, cross-thematic research tackling the same jointly seems to be in short supply. There is a gap in the body of knowledge regarding the impact of Industry 4.0 on critical infrastructure, its safety, and management. Meanwhile, both research directions are of crucial interest to modern economies. Therefore, one has to ask if Industry 4.0 technologies can support critical infrastructure, its safety, and management, or not, and whether I4.0 solutions may be considered a part of the critical infrastructure themselves. It is worth discussing the promises and potential of I4.0 as well as the existing threats stemming from its application within critical infrastructure systems.

Other popular databases were also examined for the query (''critical infrastructure'' and ''Industry 4.0''), but results were scarce (EBSCOhost – 3 papers, IEEE Xplore – 11 papers).

B. BIBLIOGRAPHIC NETWORK ANALYSIS USING VOSVIEWER

The Global Citation Score (GCS) is used to determine the group of leading flares in the analyzed study area and to detect groundbreaking publications. Table 2 presents 10 of the most frequently cited papers ranked by their GCS in the Scopus database.

The most seminal works accordingly to GCS are presented in Table 2. A paper Sadeghi *et al.* [99] was by far the highest ranking of the lot. Another ranking of papers was constructed to identify recent groundbreaking studies that could have a potentially significant impact and promising scientific input on Industry 4.0 & critical infrastructure. The ranking based on citations in 2021 divided by years since publication (Table 3) identified four articles [100]–[103] that were not previously included in the GCS ranking (II). It is also important to notice that high GCS values did not always correspond to studies with a large impact and promising scientific input on I4.0 & CI.

TABLE 2. The global citation scores of the 10 most cited papers.

Rank	Paper	GCS	Open Access
1	(Sadeghi et al., 2015) [99]	529	no
2	(Popkova et al., 2019)[104]	81	no
3	(Müller, 2019)[105]	67	no
4	(Serpanos, 2018)[106]	56	no
5	(Kiel et al., 2016)[107]	46	no
6	(Singh et al., 2020)[108]	44	no
7	(Yun et al., 2018)[109]	32	yes
8	(Bag et al., 2021)[110]	29	no
9	(Liu et al., 2019)[111]	28	yes
10	(Kobara, 2016) [112]	27	yes

Based on the GCS, recent groundbreaking publications lean towards topics related to the Internet of Things (IoT) [102], [104], Industrial IoT systems [99], [107], Cyber-Physical Systems (CPSs) as a part of IoT-oriented infrastructure [106], [108], and Industrial Control Systems (ICS) [112]. One paper distinguished by a very high number of citations was also published early [99], i.e. they had initiated a scientific discussion on the security, privacy challenges, and cybersecurity themes. These are undoubtedly the main areas discussed in the most quoted papers. Sub-themes include issues related to the uses of IoT, IIoT, CPSs, and other Industry 4.0 technologies in the management of critical infrastructure, cities (smart cities), or entire economies. There are also studies that only to a very small extent concern critical infrastructure. In the same, the potential of Industry 4.0 is shown in the context of sustainable production and circular economy [110] as well as strategies for providers and users of Industry 4.0 [105].

TABLE 3. Ranking of the 10 most cited papers in 2021.

Rank	Paper	No. of citations in 2021	Citations in 2021 per year since publication	GCS
1	(Bag et al., 2021)[110]	29	29	29
2	(Popkova et al., 2019)[104]	55	18.33	81
3	(Singh et al., 2020)[108]	31	15.5	44
4	(Wu et al., 2021)[101]	15	15	15
5	(Müller, 2019)[105]	38	12.67	67
6	(Sadeghi et al., 2015) [99]	80	11.43	529
7	(Zografopoulos et al., 2021)[102]	10	10	10
8	(Liu et al., 2019)[111]	18	6	28
9	(Klingenberg et al., 2019)[100]	16	5.33	16
10	(Carreras Guzman et al., 2020)[103]	10	5	22

It is worth noting that two papers [101], [102] already have 10 or more citations despite having been published as recently as in 2021.

The reference number of keywords (three) was adopted in accordance with proposals tested in previous studies [113], [114]. Using the VOSviewer program, a network (Fig. 2) consisting of 20 nodes corresponding to 4 clusters was obtained. In Fig. 2, each cluster is highlighted using a different color. Occurrences were used as weights. The size and clarity of a node corresponds to the frequency of its occurrence in the analyzed set. In turn, the proximity of particular elements indicates more frequent co-occurrence in specific sets as compared to the more distant elements.

The minimum number of authors' keywords in the set of selected documents was 3. If a higher value were selected, the number of keywords and clusters identified would decrease, which could lead to the omission of an important issue that has not yet been sufficiently investigated and described or is simply not properly exposed in the paper. For example, if the minimum number of author's keywords in a set of selected documents was set to 4, the query would return 13 keywords and 4 clusters, and for the value of 5, there would only be 8 keywords and 3 clusters. Conversely, setting a value lower than 3 would return too many words as keywords.

To understand the research trajectories, keywords are listed according to their total link strength, i.e. their importance in the cluster [115]. There were 75 links in the developed co-occurrence network and the total link strength was 99. The total link strength attribute indicates the total strength of the co-occurrence of a given keyword with other keywords. The higher the value, the more frequently a given keyword coexists with others and is more relevant to the network. Detailed information on the selected author's keywords is provided in Table 4.

The obtained clusters were described with reference to the papers in which the searched keywords appeared. This allowed us to present the results of research in given areas related to Industry 4.0 and critical infrastructure. The resulting clusters delineated by the authors' keywords are presented in Table 5. The aggregation results are discussed in the discussion section.

Fig. 3 shows a citation network based on the selected papers, using an overlay visualization. As a result, it became possible to identify publications with the largest number of links with others (weights) within the entire network (129 papers). At the same time, the total number of citations in the Scopus database was presented using a color scale (from 0 - blue to 20 citations - yellow).

As we can see in Fig. 3, there was no greater network of citations, and the connected citations formed clusters of only up to 2 papers (5 such mini clusters were identified). Those instances indicate cases where a topic already discussed by one author was elaborated on by another. Klingenberg *et al.* [100] reviewed Industry 4.0 technologies for a data-driven paradigm wherein the analyzed technologies included, inter alia, Industrial Control Systems and IoT [112].

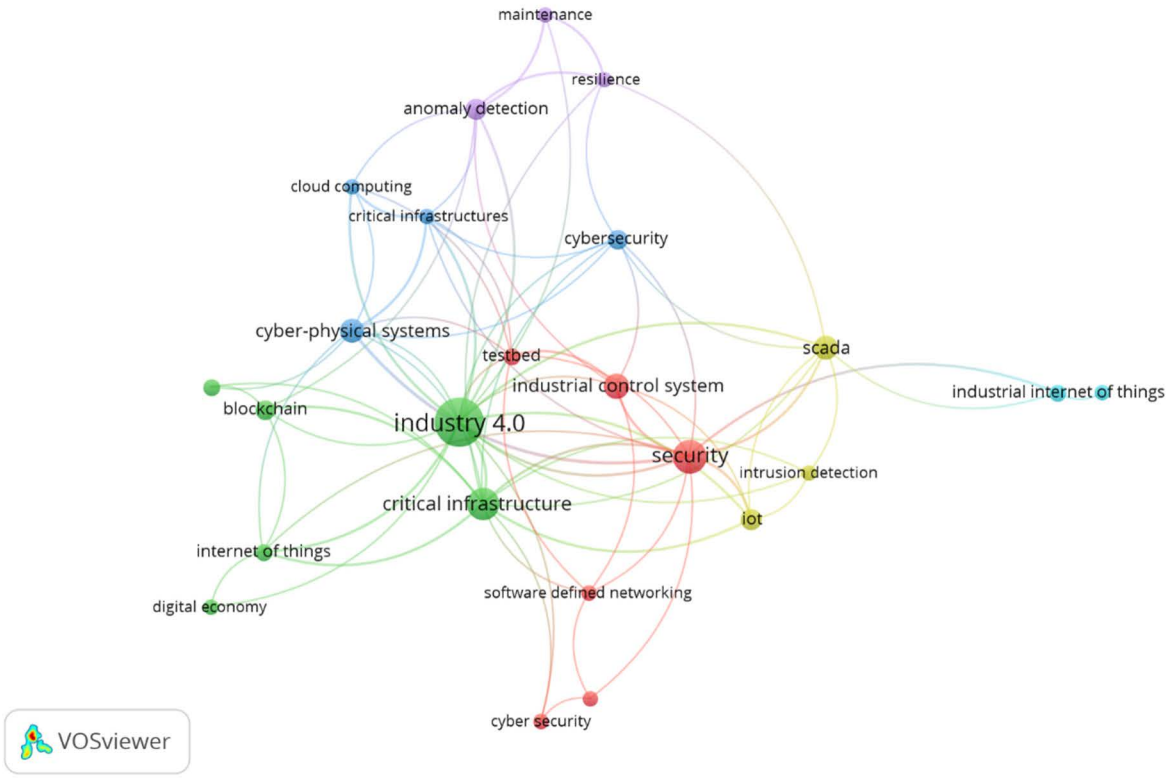

FIGURE 2. Co-occurrence network of author's keywords (minimum number of occurrences of a keyword: 3) created in VOSviewer.

Popkova *et al.* [104] presented a model of state management in an IoT-based economy, and Tagirovet al. [116] proposed development scenarios for regions relying on Digital Economy. One study [117] addressed Industry 4.0 and national security issues, while another paper by the same team [118] presented considerations regarding cryptocurrency and national security. Montalban *et al.* [119] described non-orthogonal multiple access (NOMA) in combination with the 802.11n standard, and Forenbacher et al [120] described the results of a laboratory analysis on the use of an IEEE 802.11 wireless network in the presence of wireless audio transmissions. Another study [99] discussed the issues of security and privacy challenges in IIoT, while [121] discussed the issue of securing emergent IoT applications.

This may be seen as evidence to considerable dispersion of research, as well as disaggregation of the results obtained. Furthermore, no major direction of research could be identified as the respective topics were quite distant from each other. This may have been due to the fact that the authors all focused on rather narrow areas of critical infrastructure.

C. TOPICS IDENTIFIED USING LATENT DIRICHLET ALLOCATION

We employed the LDAvis method to identify and analyze the most important topics in the area of I4.0 usage in critical infrastructure management [76]. Fig. 4, Fig. 5, Fig. 6, and Fig. 7 present characteristics of the corresponding topics.

There were 42 articles under Topic 1, which corresponded to 31.9% of the studies analyzed. The prominent words in terms of frequency of occurrence in Topic 1 were systems, industry, security, technology, infrastructure, attack, critical, and network. The keywords applicable to topic one clearly suggest a focus on network technologies understood as the critical infrastructure of industrial systems. The dominant issues include cyber security and the types of attacks to which the infrastructure that keeps industry running may be susceptible.

There were 38 articles pertaining to Topic 2, which represented 29.9% of the studies analyzed. The prominent words in terms of frequency of occurrence in Topic 2 were systems, security, infrastructure, industry, critical, IoT, smart, cps, challenge, and framework. The thematic scope of the second set of papers can be boiled down to challenges faced by industrial systems security, where the critical infrastructure framework consists specifically of IoT, smart, CPS technologies. The papers in this collection extended the set of network threats to include CPS vulnerabilities. At the same time, the strong connection between IoT, CPS, and human factors required to achieve the benefits of industrial transformation towards I4.0 were emphasized.

There were 32 articles related to Topic 3, which constituted 25.1% of the studies analyzed. The prominent words in terms of frequency of occurrence in Topic 3 were network, systems, service, datum, critical, infrastructure, industry, cloud, and

TABLE 4. Information about the author's keywords analyzed in VOSviewer.

Author's keywords	Total link strength	Links	Occurrences
industry 4.0	25	17	30
security	21	13	14
critical infrastructure	18	13	13
cyber-physical systems	12	9	7
anomaly detection	10	7	6
critical infrastructures	10	7	3
scada	10	8	7
industrial control system	9	7	8
iot	9	6	6
cybersecurity	8	8	5
internet of things	8	6	4
testbed	8	7	4
cloud computing	7	5	3
resilience	7	5	3
blockchain	6	5	5
maintenance	5	3	3
software-defined networking	5	5	3
industrial internet of things	4	3	4
intrusion detection	4	4	3
cyber security	3	3	3
industrial control systems	3	3	3
internet of things (iot)	3	3	4
digital economy	2	2	3
opc ua	1	0	3

smart. The papers classified under this selection pertained to the system of intelligent network services processing data in the computational cloud. The authors identified this system as infrastructure critical to the industry according to the idea of I4.0. However, there was no indication of specific technologies, as was the case for Topic 2. The indication of cloud computing as a platform for the integration of data from various systems was the element that distinguished papers classified under Topic 3 from those related to Topic 1. Moreover, papers under Topic 3 focused more on the network of mutual connections and the model of cooperation of available network services, omitting the aspect of security and vulnerability of such services.

There were 17 articles pertaining to Topic 4, which represented 13.2% of the studies analyzed. The prominent words in terms of frequency of occurrence in Topic 4 were industry, technology, critical, security, infrastructure, model, network, risk, and business. The papers classified under Topic 4 discussed network technologies as elements of infrastructure critical to the industry according to the idea of I4.0 under the modeling approach. Unlike other papers, the works in this group focused on the issues of security management and risks resulting from the utilization of I4.0 tools in the industry. The works were less concerned with technical issues. The discussion was shifted to issues related to the user of such implemented solutions or economic justification for their implementation.

IV. DISCUSSION

A. GENERAL FINDINGS

Our expectation that the scientific discourse does indeed include some deliberations related to the relations between CI and I4.0 were confirmed. However, given the number of works devoted to exclusively I4.0 or CI, the intersection of these two topics proved surprisingly poorly explored and limited to only approx. 100 works (see Table 1).

It is clear that both CI and I4.0, taken separately, are perceived as highly significant by practitioners and researchers alike. This is hardly surprising as both issues constitute building blocks of modern economies. At the same time, the small number of works considering CI and I4.0 jointly demonstrates a shortage of transdisciplinary research oriented towards the impact that I4.0 has on CI, its safety, and management.

As follows from the citation analysis, the most cited work was a publication by Sadeghi *et al.* [99]. It achieved a significantly greater number of citations than any other text in the research area investigated (see Table 2). However, considering additional time factors in the analysis of significance (measured by the number of citations), allowed the identification of additional breakthrough works [100]–[103] that were not evident in the analysis of citation numbers as such. This means that the relatively early work by Sadeghi *et al.* [99] initiated a continued discourse on topics related to the challenges of security, safety, privacy, and cybersecurity. However, the leading topics were those focused on the (industrial) Internet of Things (IoT) and cyber-physical systems (CPSs) as a part of infrastructure dedicated to industrial control systems (ICSs).

Two papers [101], [102] were published fairly recently (2021), but have already gained a relatively high number of citations. Usually, the number of citations increases in the years following the publication, which in this case suggests some potential of the two works to become highly relevant to the discourse on CI and I4.0. Wu *et al.* [101] presented a convergence of blockchain and edge computing for secure and scalable industrial IoT considered as an element of critical infrastructure in I4.0 systems. Due to the digital transformation of I4.0 driven by smart factories, big data, and machine learning, CI is becoming increasing dependent on IoT devices, or IIoT in the context of I4.0, creating the so-called CI with IoT or IoT CI. (The International Data Corporation forecasts that by 2025, there will be approximately 41.6 billion active IoT devices, generating 79.4 zettabytes of data). The authors of the study highlight two major problems. Firstly, industrial control systems (ICS) were originally designed mainly for proprietary and closed infrastructures without paying too much attention to security issues, as traditional CIs are sort of isolated and are not vulnerable to cyberattacks. However, as these infrastructures connected to the internet via IoT, they became vulnerable to a wide range of cyberattacks, including Distributed Denial of Service (DDoS), malware, breach attack, brute force attack, man-in-the-middle attack, SQL injection, and phishing. These

TABLE 5. Clusters based on the author's keywords discovered in VOSviewer.

Cluster	Author's keywords
Cluster 1	cyber security, industrial control system, industrial control systems, security, software-defined networking, testbed
Cluster 2	blockchain, critical infrastructure, digital economy, industry 4.0, internet of things (IoT)
Cluster 3	cloud computing, critical infrastructures, cyber-physical systems, cybersecurity
Cluster 4	intrusion detection, IoT, scada
Cluster 5	anomaly detection, maintenance, resilience
Cluster 6	industrial internet of things, OPC UA

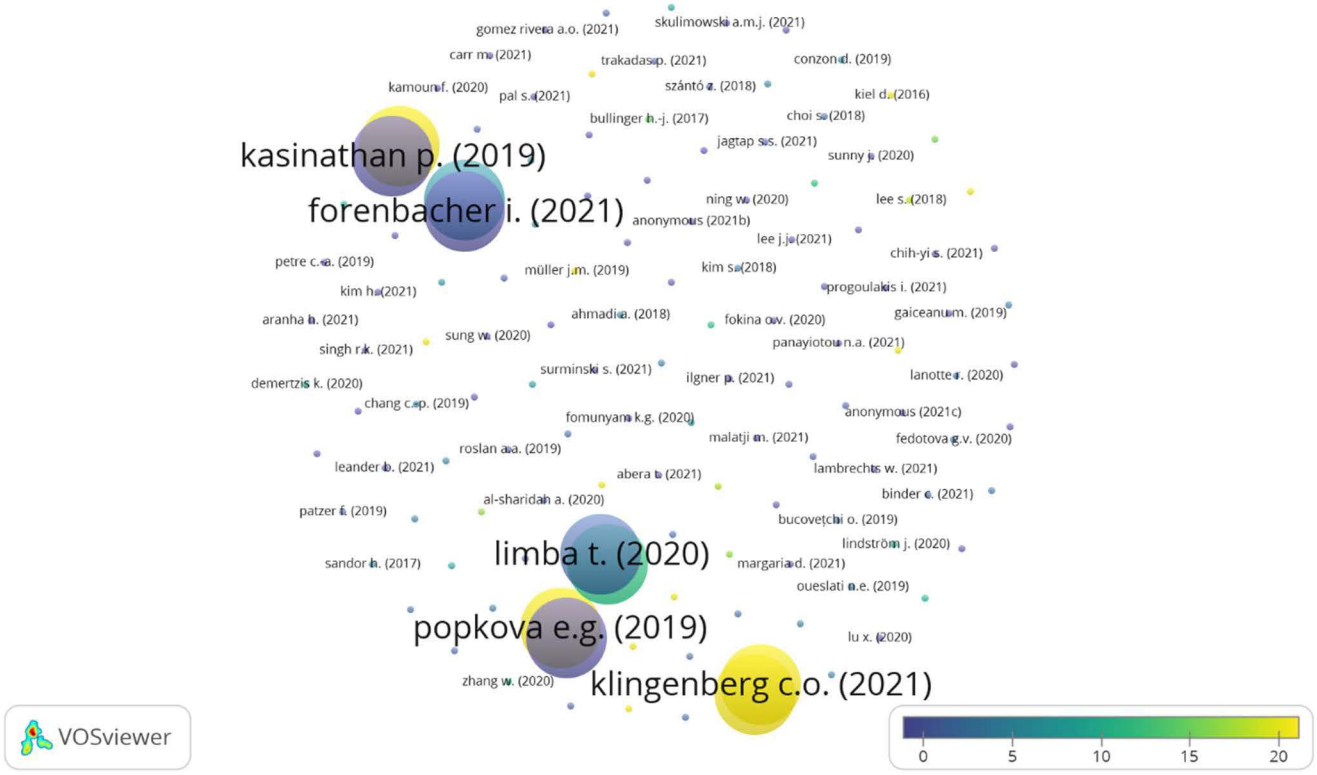

FIGURE 3. Citation network created in VOSviewer.

threaten the ability of ICSs to provide normal support for services. Scalability is another challenge which ICSs were not originally designed to handle. Given the remarkable increase in the number of IoT devices and the volume of data they collect and analyze, the traditional centralized manner of data collection and analysis is becoming the bottleneck of ICSs. The emerging blockchain and edge computing paradigms are promising technologies that can tackle the above challenges in terms of CI security and scalability. The convergence of the two technologies is vital to providing the necessary computation and storage for IoT, while simultaneously guaranteeing the security and scalability CI under I4.0. The authors also identified the following future research directions:

1) The architecture of IIoT CIs:
   a. Standard Application Programming Interface for Application Developers;
   b. Integrated Networking, Computing, Storage, and Power Resource Allocation;
   c. Network Economy (How to design a practical solution for the convergence of edge computing and blockchain, by considering network economy factors, e.g., pricing mechanisms of real-world applications);
2) Secure IIoT CIs:
   a. Security Vulnerabilities of IIoT Devices;
   b. Security Vulnerabilities of Blockchain;
   c. Integration of AI to Secure IIoT CIs;
   d. Data Privacy Preservation;
3) Scalable CIs:
   a. Scalability of IIoT;
   b. Scalability of Blockchain;
   c. Coordination Across Disciplines.

Zografopoulos *et al.* [102] comprehensively analyzed the security and safety of cyber-physical energy systems. Threats were modeled to assess risks. Moreover, the model considered resources and their behavior under adverse scenarios

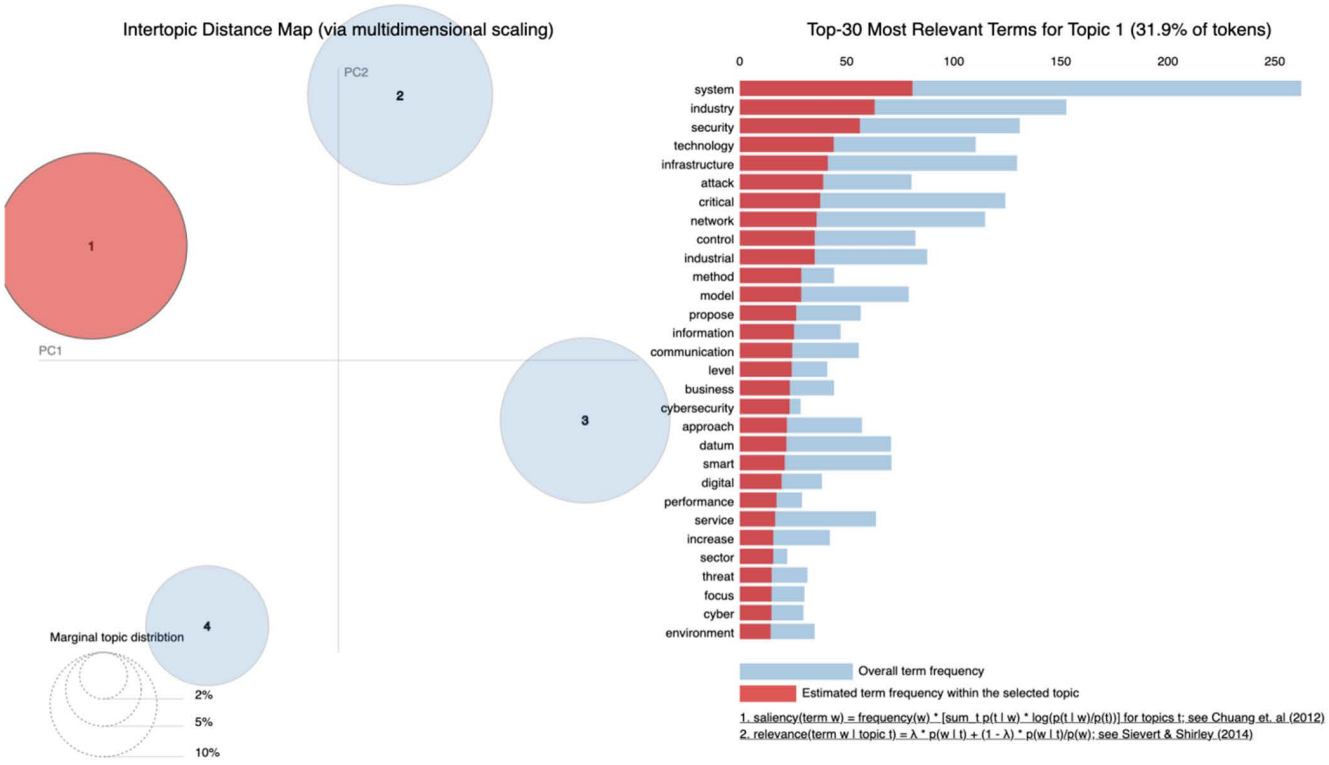

FIGURE 4. **Topic one characteristics visualized with LDAVis.**

using specific metrics to prioritize vulnerabilities. The presented framework for modeling, simulating, assessing, and mitigating attacks in a CPS was examined on the example of four case studies representing possible scenarios of attacks against energy CPS. The reasons behind the attention gained by this paper have been three-fold:

1) APPLICATION DOMAIN

The importance of energy systems as operations domain, their critical nature within the power grid infrastructure where attacks can lead to disastrous consequences;

2) THEMATIC DOMAIN

The increasing importance of cyber-security as such, considering the rapidly growing number of digital solutions in organizations, but also in individuals settings;

3) UTILITARIAN SPECIFIC

The presented computer simulation models allow practitioners to easily modify and adapt the scenarios to specific cases.

The analysis of the two papers corroborated the original assumption that the issue of the safety and security of cyber-physical systems is a highly relevant topic in research pertaining to CI and I4.0.

There is an evident shortage of studies on CI and I4.0 following a more holistic approach, as evidenced by the network analysis performed using VOSviewer software. The whole citation network was composed of 75 links, and their total strength was 99. Given the total number of works (129), this proves the high granularity of isolated studies on separate topics (see Fig. 3). The connected sub-networks of citations consist of a maximum of two papers. Five such mini clusters were identified. This evidences considerable dispersion of research as well as disaggregation of the results obtained. There is also no major direction of research, and topics are quite distant from each other. This was mainly due to the narrowed analyses focusing on specific I4.0 technologies limited to specific CI applications. A holistic overview of different issues pertinent to CI and I4.0 as a total paradigm is lacking. I4.0 technologies (mainly CPS, IoT) are already 'critical', but absent from scientific literature and studies discussing connections between CI and I4.0 issues.

The co-occurrence network consisted of six clusters (C1-C6, see Table 5), but its analysis led to aggregation into three final clusters (FC1-FC3), as described below.

B. TOPICS RESULTING FROM THE VOSVIEWER ANALYSIS

1) FC1 – SECURITY OF INDUSTRIAL CONTROL SYSTEMS

Final cluster 1 (FC1) corresponds to the initially identified cluster C1 (see Table 5) which deals with general issues related to security, with a particular focus on cybersecurity in industrial control systems (ICSs). ICS is considered by many authors to be the heart of critical infrastructure [122], [123] because it is mainly responsible for supervisory control and

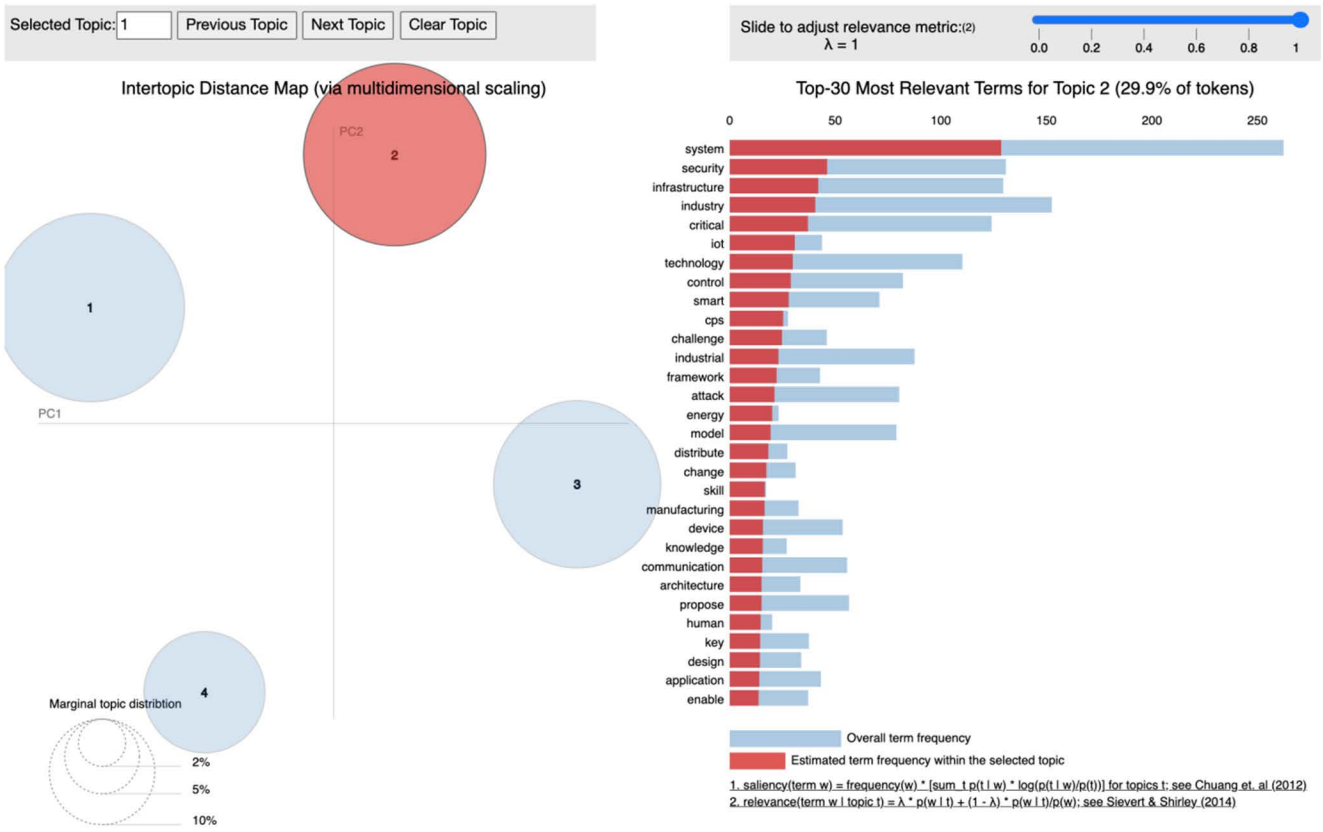

FIGURE 5. Topic two characteristics visualized with LDAVis.

data collection (SCADA), process monitoring, and control of system information flows in the industry. The importance of cybersecurity in this context has been discussed in many papers [99], [101]–[103], [112], [124]. The cluster also includes studies on software-defined networking issues, which is an important element responsible for the security of data transmitted within the network [108] and can be a countermeasure for Address Resolution Protocol (ARP) spoofing in Communication-Based Train Control (CBTC) systems [125]. Testbeds play an important role in the processes of cybersecurity systems verification or software validation [102], [111], [125].

2) FC2 –I4.0 SOLUTIONS AS SUPPORTIVE CI ELEMENTS

The initially identified clusters 2, 3, 4, and 6 (see Table 5) were merged into FC2 (final cluster 2) as they all pertain to the same major thematic area: implementing Industry 4.0 technologies to support critical infrastructure. It should be noted that in some of the papers, the authors observed that the main technologies of Industry 4.0 support critical infrastructure [103], [106], but in other studies technologies such as CPSs [102], (I)IoT [101], [102], cloud computing [100], [124], blockchain [101] were considered important and inseparable elements of critical infrastructure as such. In some publications, the authors explore the integration of various I4.0 technologies in the context of CI, e.g. connections (industrial) IoT, and CPSs [126]. The respective texts consider this topic at different levels, from the combination of I4.0 and CI at the level of entire economies (digital economy) [116], through smart cities [108], to the level of communication protocols enabling communication between machines (OPC Unified Architecture – OPC UA) [127]. The aspect of the relationship between I4.0 and CI that receives the most attention revolves around cybersecurity and related issues, e.g. intrusion detection [128].

3) FC3 – RELIABILITY, AND RESILIENCE OF CI

Final cluster FC3 corresponds to the initially identified cluster C5 (see Table 5). FC3 reflects maintenance strategies in the context of ensuring the continuity of operation of devices classified as critical infrastructure, e.g. refrigeration units in hospital buildings [129]. It also discusses cybersecurity capabilities that ensure the resilience of critical infrastructure [124], as well as the alignment of AI with disaster resilience management support systems [130]. An important aspect of resilience is indicated in the paper [102], which presents anomaly detection as an important category of ensuring for the security of energy CPS.

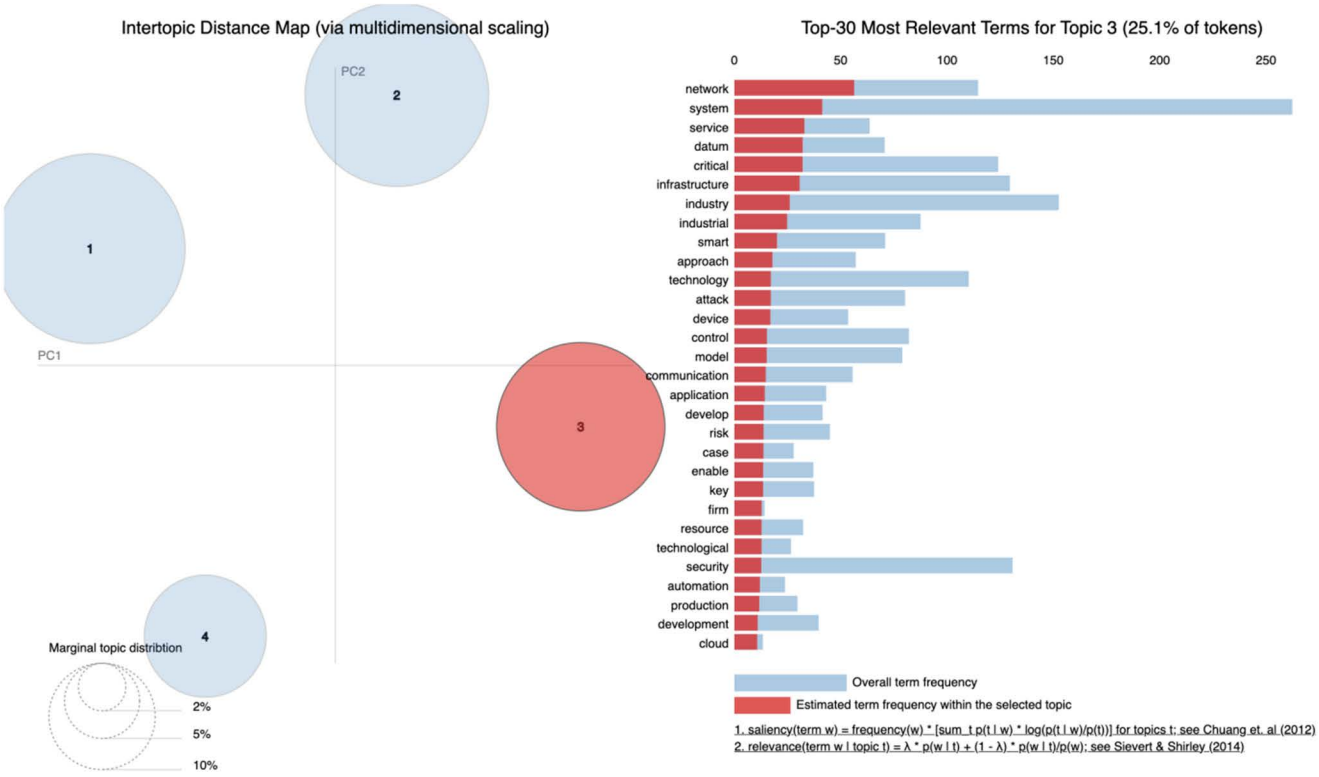

FIGURE 6. Topic three characteristics visualized with LDAvis.

C. TOPICS RESULTING FROM THE LDA ANALYSIS

The LDAvis method allowed the identification of four leading topics in the area of I4.0 usage in CI management:

- T1– network technologies as CI of industrial systems (see Fig. 4),
- T2 – security of I4.0-based CI in industrial systems (where CI framework is specific IoT, smart, CPS technologies) (see Fig. 5, Fig. 6, and Fig. 7),
- T3 – smart network services processing data in cloud computing (see Fig. 6),
- T4 – I4.0-based modeling for network technologies as industrial CI (see Fig. 7).

D. MAPPING VOSVIEWER AND LDA RESULTS

Our analysis of results from VOSviewer and LDA revealed that the findings were mutually consistent. The results from VOSviewer and LDA are mapped in Fig. 8 below.

The conducted literature review revealed that researchers and practitioners are divided as to which elements constitute Industry 4.0, how these elements are interrelated, and where Industry 4.0 specifically applies. Regardless of the definition, the idea of industry 4.0 indicates a transition from centralized production towards production that is highly flexible and self-controlled. Kolberg and Zuehlke [9] 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 [10]. This provides the opportunity to network the entire factory, creating an intelligent environment with the efficiency and capacity far exceeding the existing capabilities of manufacturing companies. While this undoubtedly creates new opportunities, one must also consider the new unknown risks that may arise in this context.

The analyzed research indicates that the issue of CI appears in the context of technologies enabling the realization of the Industry 4.0 paradigm. In particular, many papers elaborate on the uses of network technologies, cyber-physical Systems, IoT, and cloud computing. The available studies indicate that Industry 4.0 is no longer a trend of the future. For many enterprises, it has lain at the very heart of their strategic and research agenda for five or more years [131]. In this context, Industry 4.0 and the technologies enabling its implementation may soon be included in the category of CI on which the proper functioning of the economy, society, and public administration will depend.

At the same time, a substantial body of work already indicates that the technologies considered to be the foundations of I4.0 are currently widely used in systems classified as CI. Examples of the most advanced applications include IoT and CPS in the power industry, wastewater treatment systems, or systems for transporting electricity, oil, and gas.

However, there were no works discussing the applications of I4.0 technologies in systems such as food production, rescue services, medical care system, or public administration.

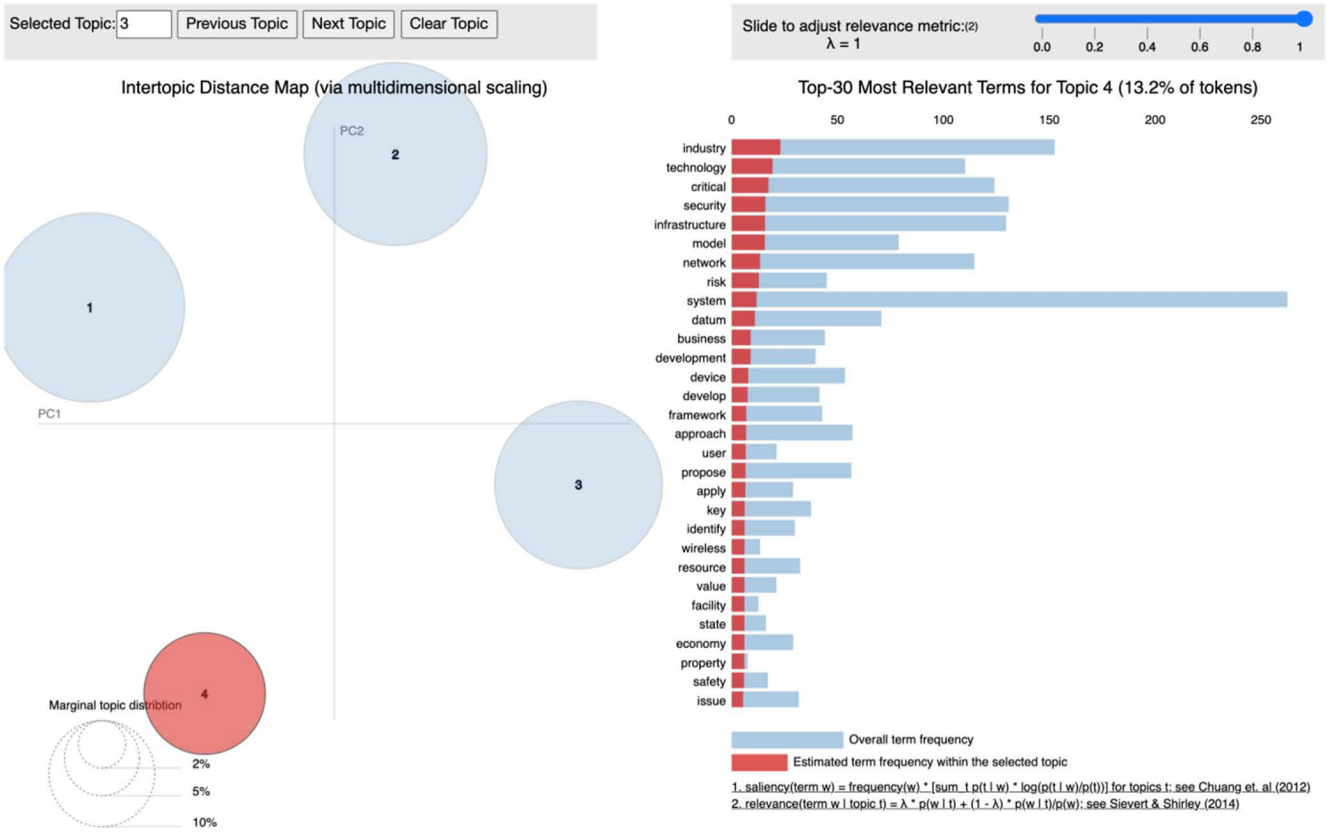

FIGURE 7. Topic four characteristics visualized with LDAVis.

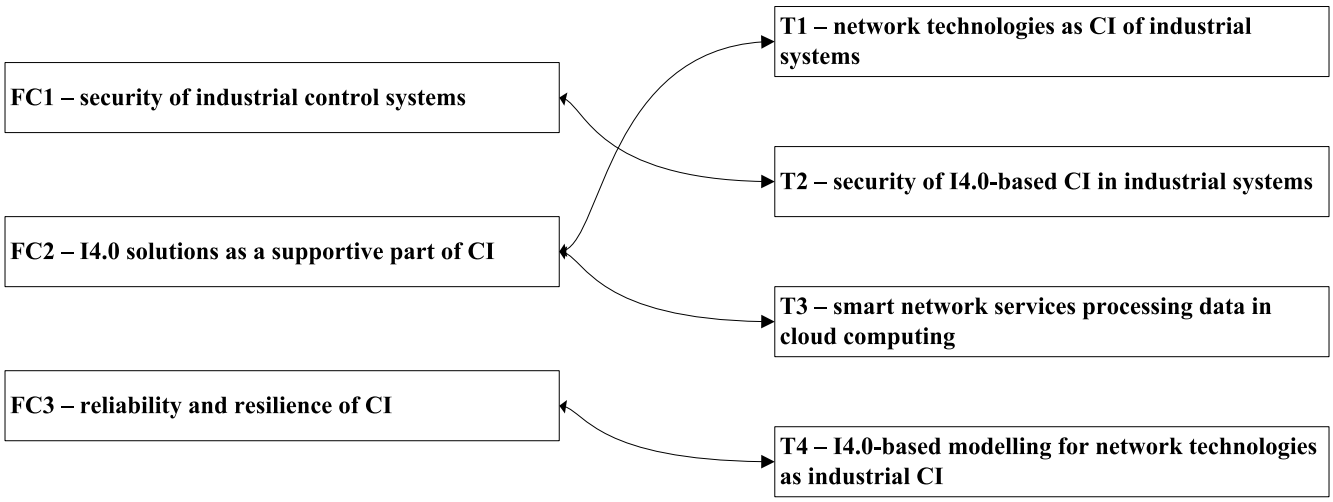

FIGURE 8. Mapping of VOSviewer and LDA results for CI and I4.0 research topics.

This is likely due to overall lack of papers focusing on non-technical CI systems. They appear in literature only as complementary elements to case studies discussing technical systems [60]. Secondly, it simply is easier to apply I4.0 technologies in CI systems of a technical nature because the problems occurring in these systems are analogous to those observed in manufacturing companies.

As follows from the literature review, the central topic of the current scientific discourse pertaining to the protection of Industry 4.0 is the issue of cybersecurity. The works analyzed

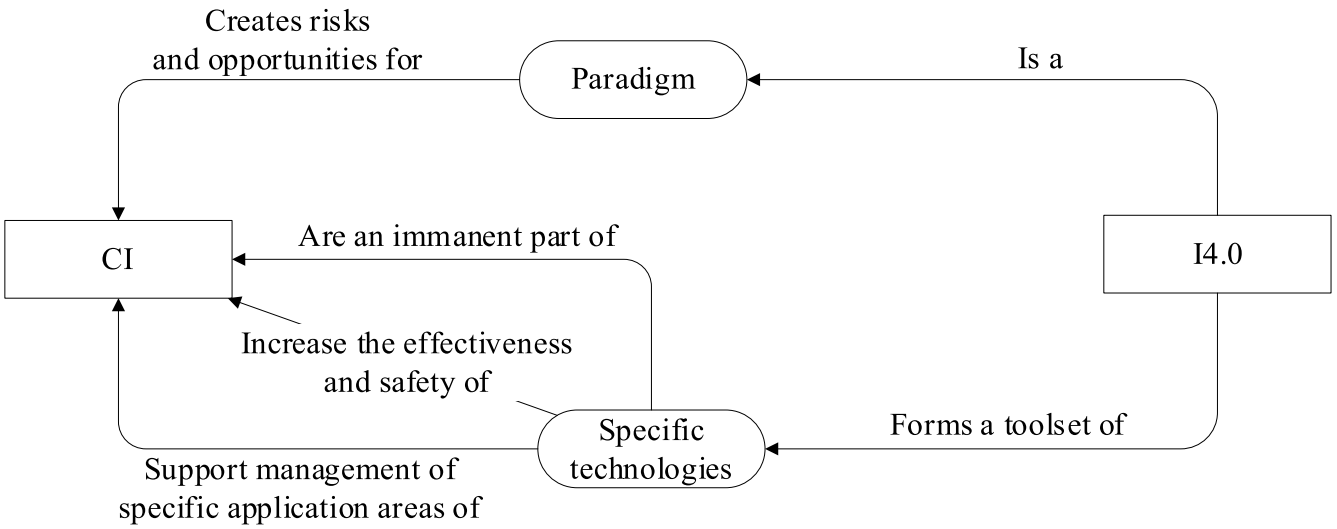

FIGURE 9. Mapping general relations between I4.0 and CI.

focused on identifying threats related to network technologies. The results revealed a field of study in its 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, deliberations on the security of elements identified as essential to Industry 4.0 do not consider all the threats to which the respective elements of Industry 4.0 are 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 are also no practical guidelines or methods to consider when dealing with different types of threats at the decision-making stage with a view to lowering risk to an acceptable level. The available works tend to provide 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. AI for minimizing cybersecurity investment and the expected cost of losses from security breaches in a supply chain [132].

Literature does not cover the impacts of CI needs on the I4.0 paradigm and technologies development. Therefore, Fig. 9 depicts only a one-directional relation between I4.0 and CI. One expects that the missing direction of interactions (CI to I4.0) ought to be covered in future research.

In general, literature delivers atomized knowledge on I4.0 technologies employed to support the management of CI and I4.0 applications as a part of CI (see relations between ''Specific technologies'' and ''CI'' entities in Fig. 9). However, research on how the full I4.0 paradigm could impact different types of CI is lacking (see relations between ''Paradigm'' and ''CI'' entities in Fig. 9).

The presented areas of research (Fig. 8) selected as a result of a literature review may be the basis of further, much more deepened research. Despite the existence of several papers in separate areas, many issues still require significant effort to researchers and practitioners.

Within FC1 and T2, future research should concern the issue of cybersecurity [51, 126] and leaking of sensitive data [46]. Blockchain technologies [21], [23], [26], [46], [101] and Digital Twin [24, 59] can be very important in this area. The development of IioT [101] will also be very important, and in particular the use of CloudEdge technology (data anonymization) [128]. Certainly, efforts will also be carried out on improving existing or creating new communication protocols, as well as the development of SCADA [125], [127].

Within FC2, T1 and T3, the development of cloud processing [100], [124] and faster processing of increasing amounts of available data (Big Data) [46], [47] can be indicated for key areas of future research. The continuous development of CPSs [55], [56], [102], [103], [112] is also significant, which currently constitute the basis for the functioning of many enterprises and enable much faster data flow or shop floor communication in real time.

Within FC3 and T4, very important works will concern issues related to the integration of systems within CI, as well as increasing their reliability and resilience [32], [36], [38], [41], [42], [45], [53], [57], [58], [59]. AI can be an important support here [51], [52], [66]. It should be noted that research are increasingly conducted on critical infrastructure facilities (e.g. hospitals, power plants), where reliability and resilience are the most important aspects [129]. Everything indicates that this trend will be maintained. An important aspect in the context of CI facility safety is to conduct a holistic research [25] considering either cyber security and physical security, technical security, legal security, personal security and business continuity.

V. CONCLUSION

There are not many works jointly covering both topics of I4.0 and CI, but there are plenty discussing each of the topics

separately. One can note the complete absence of holistic works jointly addressing CI (not specific to any domain) and I4.0 from a general perspective, where I4.0 is understood as both solutions supporting CI management and solutions constituting an intermittent part of CI itself. Moreover, the current body of literature covers only selected I4.0 elements and is often focused on specific technologies, instead of the paradigmatic I4.0 itself and its full toolset of solutions and technologies. However, not even all of the most promising I4.0 aspects have been sufficiently discussed in the context of CI. For example, there are scarcely any studies on computer simulation modeling and digital twin applications and potential. The main research directions pursued currently and likely to remain dominant in the nearest future are oriented towards security, reliability, and resilience issues of specific I4.0 technologies considered as elements of CI or as tools supporting CI management. One has to conclude that the reality has now outpaced scientific research. Therefore, two main directions for further study should be considered, 1/ including also white papers and reports published on different levels (e.g. by national agencies responsible for CI management, etc.), and 2/ computer simulation modeling of I4.0 applications in CI systems. Both aspects are currently severely lacking in our research and scientific literature. Core technologies for I4.0 not only affect CI security but are already a key component thereof. This is particularly obvious in CI systems responsible for electricity production and transmission, pipeline transport, petroleum processing, or wastewater treatment. Therefore, it is necessary to undertake research on the development of CI operation models with adequate consideration of the full I4.0 paradigm. In this context, the presented results provide the starting point for more in-depth studies and may serve as an inspiration for the scientific community. There is a need for a holistic framework of CI and I4.0, but detailed case studies are also lacking, especially in terms of simulation modeling of I4.0 and CI interactions.

REFERENCES

[1] Forschungsunion and Acatech. (2011). *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. Accessed: Sep. 3, 2021. [Online]. Available: https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/

[2] H. Kagermann, W.-D. Lukas, and W. Wahlster, "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], 13-2011 seite 2," VDI Nachrichten. [Online]. Available: http://www.wolfgang-wahlster.de/wordpress/wp-content/uploads/Industrie_4_0_Mit_dem_Internet_der_Dinge_auf_dem_Weg_zur_vierten_industriellen_Revolution_2.pdf

[3] S. Kumar, M. Suhaib, and M. Asjad, "Industry 4.0: Complex, disruptive, but inevitable," *Manage. Prod. Eng. Rev.*, vol. 11, no. 1, pp. 43–51, 2020.

[4] V. D. Majstorovic and R. Mitrovic, "Industry 4.0 programs worldwide," in *Proc. 4th Int. Conf. Ind. 4.0 Model Adv. Manuf.*, Cham, Switzerland, 2019, pp. 78–99, doi: 10.1007/978-3-030-18180-2_7.

[5] A.-W. Scheer, *CIM Computer Integrated Manufacturing: Towards the Factory of the Future*, 2nd ed. Berlin, Germany: Springer-Verlag, 1991, doi: 10.1007/978-3-642-97314-7.

[6] D. Ø. Madsen, "The emergence and rise of industry 4.0 viewed through the lens of management fashion theory," *Administ. Sci.*, vol. 9, no. 3, p. 71, Sep. 2019, doi: 10.3390/admsci9030071.

[7] T. D. Oesterreich, J. Schuir, and F. Teuteberg, "The emperor's new clothes or an enduring IT fashion? Analyzing the lifecycle of industry 4.0 through the lens of management fashion theory," *Sustainability*, vol. 12, no. 21, p. 8828, Jan. 2020, doi: 10.3390/su12218828.

[8] N. P. Melville and L. Robert, "The generative fourth industrial revolution: Features, affordances, and implications," *SSRN Electron. J.*, May 2021, doi: 10.2139/ssrn.3728052.

[9] D. Kolberg and D. Zühlke, "Lean automation enabled by industry 4.0 technologies," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 1870–1875, 2015, doi: 10.1016/j.ifacol.2015.06.359.

[10] L. D. Xu, E. L. Xu, and L. Li, "Industry 4.0: State of the art and future trends," *Int. J. Prod. Res.*, vol. 56, no. 8, pp. 2941–2962, 2018, doi: 10.1080/00207543.2018.1444806.

[11] A. Calabrese, N. L. Ghiron, and L. Tiburzi, "'Evolutions' and 'revolutions' in manufacturers' implementation of industry 4.0: A literature review, a multiple case study, and a conceptual framework," *Prod. Planning Control*, vol. 32, no. 3, pp. 213–227, Feb. 2021, doi: 10.1080/09537287.2020.1719715.

[12] Y. Liao, F. Deschamps, E. D. F. R. Loures, and L. F. P. Ramos, "Past, present and future of industry 4.0—A systematic literature review and research agenda proposal," *Int. J. Prod. Res.*, vol. 55, no. 12, pp. 3609–3629, Jun. 2017, doi: 10.1080/00207543.2017.1308576.

[13] E. Oztemel and S. Gursev, "Literature review of industry 4.0 and related technologies," *J. Intell. Manuf.*, vol. 31, no. 1, pp. 127–182, Jan. 2020, doi: 10.1007/s10845-018-1433-8.

[14] J. Grotepass, "AI in industrial automation (white paper)," ZVEI, Frankfurt am Main, Frankfurt, Germany, White Paper, 2021. Accessed: Jan. 19, 2022. [Online]. Available: https://www.zvei.org/en/press-media/publications/ai-in-industrial-automation-white-paper and https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2021/April/AI_in_Industrial_Automation/AI-in-Industrial-Automation-White-Paper-NEU.pdf

[15] K. Ejsmont, B. Gladysz, and A. Kluczek, "Impact of industry 4.0 on sustainability—Bibliometric literature review," *Sustainability*, vol. 12, no. 14, p. 5650, Jan. 2020, doi: 10.3390/su12145650.

[16] J. Leng, D. Wang, W. Shen, X. Li, Q. Liu, and X. Chen, "Digital twins-based smart manufacturing system design in industry 4.0: A review," *J. Manuf. Syst.*, vol. 60, pp. 119–137, Jul. 2021, doi: 10.1016/j.jmsy.2021.05.011.

[17] J. Leng, M. Zhou, Y. Xiao, H. Zhang, Q. Liu, W. Shen, Q. Su, and L. Li, "Digital twins-based remote semi-physical commissioning of flow-type smart manufacturing systems," *J. Cleaner Prod.*, vol. 306, Jul. 2021, Art. no. 127278, doi: 10.1016/j.jclepro.2021.127278.

[18] J. Leng, D. Yan, Q. Liu, H. Zhang, G. Zhao, L. Wei, D. Zhang, A. Yu, and X. Chen, "Digital twin-driven joint optimisation of packing and storage assignment in large-scale automated high-rise warehouse product-service system," *Int. J. Comput. Integr. Manuf.*, vol. 34, nos. 7–8, pp. 783–800, Aug. 2021, doi: 10.1080/0951192X.2019.1667032.

[19] T. van Erp, N. G. M. Rytter, F. Sieckmann, M. B. Larsen, H. Blichfeldt, and H. Kohl, "Management, design, and implementation of innovation projects: Towards a framework for improving the level of automation and digitalization in manufacturing systems," in *Proc. 9th Int. Conf. Control, Mechatronics Automat. (ICCMA)*, Nov. 2021, pp. 211–217, doi: 10.1109/ICCMA54375.2021.9646214.

[20] J. Leng, G. Ruan, P. Jiang, K. Xu, Q. Liu, X. Zhou, and C. Liu, "Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey," *Renew. Sustain. Energy Rev.*, vol. 132, Oct. 2020, Art. no. 110112, doi: 10.1016/j.rser.2020.110112.

[21] J. Leng, S. Ye, M. Zhou, J. L. Zhao, Q. Liu, W. Guo, W. Cao, and L. Fu, "Blockchain-secured smart manufacturing in industry 4.0: A survey," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 237–252, Jan. 2021, doi: 10.1109/TSMC.2020.3040789.

[22] ISA95. (2022). *Enterprise-Control System Integration–ISA*. Accessed: Jun. 28, 2022. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

[23] S. Suhail, R. Hussain, R. Jurdak, and C. S. Hong, "Trustworthy digital twins in the industrial Internet of Things with blockchain," *IEEE Internet Comput.*, vol. 26, no. 3, pp. 58–67, May 2022, doi: 10.1109/MIC.2021.3059320.

[24] J. Leng, P. Jiang, K. Xu, Q. Liu, J. L. Zhao, Y. Bian, and R. Shi, "Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing," *J. Cleaner Prod.*, vol. 234, pp. 767–778, Oct. 2019, doi: 10.1016/j.jclepro.2019.06.265.

[25] J. Leng, D. Yan, Q. Liu, K. Xu, J. Zhao, R. Shi, L. Wei, D. Zhang, and X. Chen, "Manuchain: Combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 182–192, Jan. 2020, 10.1109/TSMC.2019.2930418

[26] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Trans. Services Comput.*, early access, Nov. 25, 2022, doi: 10.1109/TSC.2020.3038641.

[27] J. Moteff and P. Parfomak, "Critical infrastructure and key assets: Definition and identification," Congressional Res. Service, Library Congr., Washington, DC, USA, CRS Rep. Congr. RL32631, Oct. 2004.

[28] European Commision. (2006). *Communication from the Commission on a European Programme for Critical Infrastructure Protection*. Accessed: Feb. 11, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52006DC0786

[29] B. Gellerbring, A. Holmgren, and A. Rinne, *Vägledning för Samhällsviktig Verksamhet: Att Identifiera Samhällsviktig Verksamhet Och Kritiska Beroenden Samt Bedöma Acceptabel Avbrottstid. Myndigheten för Samhällsskydd Och Beredskap (MSB)*, Myndigheten för samhällskydd och beredskap, Sweden, 2014.

[30] FEMA. (2021). *Historic Disasters—Hurricane Sandy | FEMA.gov*. Accessed: Sep. 6, 2021. [Online]. Available: https://www.fema.gov/disaster/historic/hurricane-sandy

[31] S. Brem, "Critical infrastructure protection from a national perspective," *Eur. J. Risk Regulation*, vol. 6, no. 2, pp. 191–199, Jun. 2015, doi: 10.1017/S1867299X00004499.

[32] J. Brassett and N. Vaughan-Williams, "Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness," *Secur. Dialogue*, vol. 46, no. 1, pp. 32–50, Feb. 2015, doi: 10.1177/0967010614555943.

[33] C. Armenakis, E. Du, S. Natesan, R. Persad, and Y. Zhang, "Flood risk assessment in urban areas based on spatial analytics and social factors," *Geosciences*, vol. 7, no. 4, p. 123, Nov. 2017, doi: 10.3390/geosciences7040123.

[34] A. Johnston, P. Slovinsky, and K. L. Yates, "Assessing the vulnerability of coastal infrastructure to sea level rise using multi-criteria analysis in scarborough, Maine (USA)," *Ocean Coastal Manage.*, vol. 95, pp. 176–188, Jul. 2014, doi: 10.1016/j.ocecoaman.2014.04.016.

[35] D. Rehak, J. Markuci, M. Hromada, and K. Barcova, "Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system," *Int. J. Crit. Infrastruct. Protection*, vol. 14, pp. 3–17, Sep. 2016, doi: 10.1016/j.ijcip.2016.06.002.

[36] C. Pursiainen, "Critical infrastructure resilience: A Nordic model in the making?" *Int. J. Disaster Risk Reduction*, vol. 27, pp. 632–641, Mar. 2018, doi: 10.1016/j.ijdrr.2017.08.006.

[37] Y. Chen and J. V. Milanovic, "Critical appraisal of tools and methodologies for studies of cascading failures in coupled critical infrastructure systems," in *Proc. IEEE 17th Int. Conf. Smart Technol. (EUROCON)*, Ohrid, Macedonia, Jul. 2017, pp. 599–604, doi: 10.1109/EUROCON.2017.8011182.

[38] R. E. Bloomfield, P. Popov, K. Salako, V. Stankovic, and D. Wright, "Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment," *Rel. Eng. Syst. Saf.*, vol. 167, pp. 198–217, Nov. 2017, doi: 10.1016/j.ress.2017.05.030.

[39] M. Eid and V. Rosato, "Critical infrastructure disruption scenarios analyses via simulation," in *Critical Infrastructure Disruption Scenarios Analyses via Simulation*, vol. 90, R. Setola, V. Rosato, E. Kyriakides, and E. Rome, Eds. Cham, Switzerland: Springer, 2016, pp. 43–61, doi: 10.1007/978-3-319-51043-9_3.

[40] G. Pescaroli and I. Kelman, "How critical infrastructure orients international relief in cascading disasters," *J. Contingencies Crisis Manage.*, vol. 25, no. 2, pp. 56–67, Jun. 2017, doi: 10.1111/1468-5973.12118.

[41] I. Tien and A. Der Kiureghian, "Reliability assessment of critical infrastructure using Bayesian networks," *J. Infrastruct. Syst.*, vol. 23, no. 4, Dec. 2017, Art. no. 04017025, doi: 10.1061/(ASCE)IS.1943-555X.0000384.

[42] B. S. Caldwell, "Framing, information alignment, and resilience in distributed human coordination of critical infrastructure event response," *Proc. Manuf.*, vol. 3, pp. 5095–5101, Jan. 2015, doi: 10.1016/j.promfg.2015.07.524.

[43] M. Häyhtiö and K. Zaerens, "A comprehensive assessment model for critical infrastructure protection," *Manage. Prod. Eng. Rev.*, vol. 8, no. 4, pp. 42–53, Dec. 2017, doi: 10.1515/mper-2017-0035.

[44] P. Maňas, "The protection of critical infrastructure objects—Technical principles," in *Durability of Critical Infrastructure, Monitoring and Testing*, A. Kravcov, E. B. Cherepetskaya, V. Pospichal, Eds. Singapore: Springer, 2017, pp. 239–248, doi: 10.1007/978-981-10-3247-9_27.

[45] T. Hatton, C. Brown, R. Kipp, E. Seville, P. Brouggy, and M. Loveday, "Developing a model and instrument to measure the resilience of critical infrastructure sector organisations," *Int. J. Crit. Infrastruct.*, vol. 14, no. 1, p. 59, 2018, doi: 10.1504/IJCIS.2018.090653.

[46] H. Hassani, X. Huang, and E. Silva, "Banking with blockchain-ed big data," *J. Manage. Anal.*, vol. 5, no. 4, pp. 256–275, Oct. 2018, doi: 10.1080/23270012.2018.1528900.

[47] P. D. Ahn and D. Wickramasinghe, "Pushing the limits of accountability: Big data analytics containing and controlling COVID-19 in South Korea," *Accounting, Auditing Accountability J.*, vol. 34, no. 6, pp. 1320–1331, Jul. 2021, doi: 10.1108/AAAJ-08-2020-4829.

[48] ICIT. (2022). *ICIT Research & Publications*. ICIT (Institute for Crit. Infrastructure Technology). Accessed: Jan. 19, 2022. [Online]. Available: https://icitech.org/publications/

[49] Z. Al Sati. (2022). *Why Energy Companies in the GCC Must Prioritize Cyber Security to Leverage Industry 4.0*. Siemens Middle East. Accessed: Jan. 19, 2022. [Online]. Available: https://new.siemens.com/mea/en/company/stories/energy/fully-benefit-from-industry-40-gccs-critical-must-ziad-al-sati.html

[50] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective," *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, Jan. 2017, doi: 10.1080/23742917.2016.1252211.

[51] P. Laplante and B. Amaba, "Artificial intelligence in critical infrastructure systems," *Computer*, vol. 54, no. 10, pp. 14–24, Oct. 2021, doi: 10.1109/MC.2021.3055892.

[52] A. Guzman, S. Ishida, E. Choi, and A. Aoyama, "Artificial intelligence improving safety and risk analysis: A comparative analysis for critical infrastructure," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Dec. 2016, pp. 471–475, doi: 10.1109/IEEM.2016.7797920.

[53] S. G. González, S. Dormido Canto, and J. Sánchez Moreno, "Obtaining high preventive and resilience capacities in critical infrastructure by industrial automation cells," *Int. J. Crit. Infrastruct. Protection*, vol. 29, Jun. 2020, Art. no. 100355, doi: 10.1016/j.ijcip.2020.100355.

[54] A. Shukla and H. Karki, "Application of robotics in offshore oil and gas industry—A review Part II," *Robot. Auton. Syst.*, vol. 75, pp. 508–524, Jan. 2016, doi: 10.1016/j.robot.2015.09.013.

[55] J. Isern, F. Barranco, D. Deniz, J. Lesonen, J. Hannuksela, and R. R. Carrillo, "Reconfigurable cyber-physical system for critical infrastructure protection in smart cities via smart video-surveillance," *Pattern Recognit. Lett.*, vol. 140, pp. 303–309, Dec. 2020, doi: 10.1016/j.patrec.2020.11.004.

[56] J. Ding, Y. Atif, S. F. Andler, B. Lindström, and M. Jeusfeld, "CPS-based threat modeling for critical infrastructure protection," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 45, no. 2, pp. 129–132, Oct. 2017, doi: 10.1145/3152042.3152080.

[57] L. Russell, R. Goubran, F. Kwamena, and F. Knoefel, "Agile IoT for critical infrastructure resilience: Cross-modal sensing as part of a situational awareness approach," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4454–4465, Dec. 2018, doi: 10.1109/JIOT.2018.2818113.

[58] E. Brucherseifer, H. Winter, A. Mentges, M. Mühlhäuser, and M. Hellmann, "Digital twin conceptual framework for improving critical infrastructure resilience," *At-Automatisierungstechnik*, vol. 69, no. 12, pp. 1062–1080, Dec. 2021, doi: 10.1515/auto-2021-0104.

[59] S. Rautio, I. Valtonen, and R. Pirinen, "Enhancing the technical resilience of critical infrastructure with additive manufacturing," in *Proc. 30th Annu. NOFOMA Conf.*, 2018, pp. 705–720.

[60] M. Wisniewski, "The role of integral model of critical infrastructure safety in industry 4.0," *Eur. Res. Stud. J.*, vol. XXIV, no. 3, pp. 1153–1188, Aug. 2021.

[61] N. J. van Eck and L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," *Scientometrics*, vol. 84, no. 2, pp. 523–538, 2010, doi: 10.1007/s11192-009-0146-3.

[62] N. Jan van Eck and L. Waltman, "Text mining and visualization using VOSviewer," 2011, *arXiv:1109.2058*.

[63] VOSviewer. (2022). *VOSviewer—Visualizing Scientific Landscapes*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.vosviewer.com//

[64] X. Li and L. Lei, "A bibliometric analysis of topic modelling studies (2000–2017)," *J. Inf. Sci.*, vol. 47, no. 2, pp. 161–175, Apr. 2021, doi: 10.1177/0165551519877049.
[65] A. Kontostathis, L. M. Galitsky, W. M. Pottenger, S. Roy, and D. J. Phelps, "A survey of emerging trend detection in textual data mining," in *Survey of Text Mining: Clustering, Classification, and Retrieval*, M. W. Berry, Ed. New York, NY, USA: Springer, 2004, pp. 185–224, doi: 10.1007/978-1-4757-4305-0_9.
[66] R. Buchkremer, A. Demund, S. Ebener, F. Gampfer, and D. Jägering, "The application of artificial intelligence technologies as a substitute for reading and to support and enhance the authoring of scientific review articles," *IEEE Access*, vol. 7, pp. 65263–65276, 2019, doi: 10.1109/ACCESS.2019.2917719.
[67] A. Joshi, "Comparison between Scopus and ISI web of science," *J. Global Values*, vol. 7, p. 2016, Jul. 2017.
[68] K. R. Powell and S. R. Peterson, "Coverage and quality: A comparison of Web of science and scopus databases for reporting faculty nursing publication metrics," *Nursing Outlook*, vol. 65, no. 5, pp. 572–578, Sep. 2017, doi: 10.1016/j.outlook.2017.03.004.
[69] M. Visser, N. J. van Eck, and L. Waltman, "Large-scale comparison of bibliographic data sources: Scopus, Web of science, dimensions, crossref, and Microsoft Academic," *Quant. Sci. Stud.*, vol. 2, pp. 1–37, Jan. 2021, doi: 10.1162/qss_a_00112.
[70] F. Strozzi, C. Colicchia, A. Creazza, and C. Noè, "Literature review on the 'smart factory' concept using bibliometric tools," *Int. J. Prod. Res.*, vol. 55, no. 22, pp. 6572–6591, Nov. 2017, doi: 10.1080/00207543.2017.1326643.
[71] S. Stahlschmidt and D. Stephen, "From indexation policies through citation networks to normalized citation impacts: Web of science, scopus, and dimensions as varying resonance chambers," 2021, *arXiv:2106.01695*.
[72] K. Chew, M. Schoenborn, J. Stemper, and C. Lilyard, "E-journal metrics for collection management: Exploring disciplinary usage differences in scopus and web of science," *Evidence Based Library Inf. Pract.*, vol. 11, no. 2, p. 97, Jun. 2016, doi: 10.18438/B85P87.
[73] S. Tabacaru. (Apr. 2019). *Web of Science Versus Scopus: Journal Coverage Overlap Analysis*. Texas A&M Univ. Libraries. Accessed: Sep. 3, 2021. [Online]. Available: https://oaktrust.library.tamu.edu/handle/1969.1/175137
[74] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333–339, Nov. 2019, doi: 10.1016/j.jbusres.2019.07.039.
[75] B. Arvidsson, J. Johansson, and N. Guldåker, "Critical infrastructure, geographical information science and risk governance: A systematic cross-field review," *Rel. Eng. Syst. Saf.*, vol. 213, Sep. 2021, Art. no. 107741, doi: 10.1016/j.ress.2021.107741.
[76] A. Boin and A. McConnell, "Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience," *J. Contingencies Crisis Manage.*, vol. 15, no. 1, pp. 50–59, Mar. 2007, doi: 10.1111/j.1468-5973.2007.00504.x.
[77] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Syst.*, vol. 21, no. 6, pp. 11–25, Dec. 2001, doi: 10.1109/37.969131.
[78] S. Wang, X. Gu, S. Luan, and M. Zhao, "Resilience analysis of interdependent critical infrastructure systems considering deep learning and network theory," *Int. J. Crit. Infrastruct. Protection*, vol. 35, Dec. 2021, Art. no. 100459, doi: 10.1016/j.ijcip.2021.100459.
[79] G. Culot, G. Nassimbeni, G. Orzes, and M. Sartor, "Behind the definition of industry 4.0: Analysis and open questions," *Int. J. Prod. Econ.*, vol. 226, Aug. 2020, Art. no. 107617, doi: 10.1016/j.ijpe.2020.107617.
[80] S. S. Kamble, A. Gunasekaran, and S. A. Gawankar, "Sustainable industry 4.0 framework: A systematic literature review identifying the current trends and future perspectives," *Process Saf. Environ. Protection*, vol. 117, pp. 408–425, Jul. 2018, doi: 10.1016/j.psep.2018.05.009.
[81] H. Arksey and L. O'Malley, "Scoping studies: Towards a methodological framework," *Int. J. Social Res. Methodol.*, vol. 8, no. 1, pp. 19–32, Feb. 2005, doi: 10.1080/1364557032000119616.
[82] H. M. Daudt, C. van Mossel, and S. J. Scott, "Enhancing the scoping study methodology: A large, inter-professional team's experience with Arksey and O'Malley's framework," *BMC Med. Res. Methodol.*, vol. 13, no. 1, p. 48, Mar. 2013, doi: 10.1186/1471-2288-13-48.
[83] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *BMJ*, vol. 339, p. b2535, Jul. 2009, doi: 10.1136/bmj.b2535.
[84] T. McDaniels, S. Chang, K. Peterson, J. Mikawoz, and D. Reed, "Empirical framework for characterizing infrastructure failure interdependencies," *J. Infrastruct. Syst.*, vol. 13, no. 3, pp. 175–184, Sep. 2007, doi: 10.1061/(ASCE)1076-0342(2007)13:3(175).
[85] A. Kusiak, "Smart manufacturing," *Int. J. Prod. Res.*, vol. 56, nos. 1–2, pp. 508–517, 2018, doi: 10.1080/00207543.2017.1351644.
[86] D. Knoke and S. Yang, *Social Network Analysis*. Thousand Oaks, CA, USA: Sage, 2008, doi: 10.4135/9781412985864.
[87] T. A. Morris, "Structural relationships within medical informatics," in *Proc. AMIA Symp.*, 2000, pp. 590–594.
[88] W. Lou and J. Qiu, "Semantic information retrieval research based on co-occurrence analysis," *Online Inf. Rev.*, vol. 38, no. 1, pp. 4–23, Jan. 2014, doi: 10.1108/OIR-11-2012-0203.
[89] L.-M. González, X. García-Massó, A. Pardo-Ibañez, F. Peset, and J. Devís-Devís, "An author keyword analysis for mapping sport sciences," *PLoS ONE*, vol. 13, no. 8, Aug. 2018, Art. no. e0201435, doi: 10.1371/journal.pone.0201435.
[90] A. Lis, "Keywords co-occurrence analysis of research on sustainable enterprise and sustainable organisation," *J. Corporate Responsibility Leadership*, vol. 5, no. 2, pp. 47–66, 2018. [Online]. Available: https://apcz.umk.pl/JCRL/article/view/JCRL.2018.011/17065, doi: 10.12775/JCRL.2018.011.
[91] H. Jelodar, Y. Wang, C. Yuan, X. Feng, X. Jiang, Y. Li, and L. Zhao, "Latent Dirichlet allocation (LDA) and topic modeling: Models, applications, a survey," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15169–15211, Jun. 2019, doi: 10.1007/s11042-018-6894-4.
[92] N. Horn, F. Gampfer, and R. Buchkremer, "Latent Dirichlet allocation and T-distributed stochastic neighbor embedding enhance scientific reading comprehension of articles related to enterprise architecture," *AI*, vol. 2, no. 2, pp. 179–194, Apr. 2021, doi: 10.3390/ai2020011.
[93] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," *J. Mach. Learn. Res.*, vol. 3, pp. 993–1022, Mar. 2003.
[94] J. Chuang, C. D. Manning, and J. Heer, "Termite: Visualization techniques for assessing textual topic models," in *Proc. Int. Work. Conf. Adv. Vis. Interfaces (AVI)*, New York, NY, USA, 2012, pp. 74–77, doi: 10.1145/2254556.2254572.
[95] C. Sievert and K. Shirley, "LDAvis: A method for visualizing and interpreting topics," in *Proc. Workshop Interact. Lang. Learn., Vis., Interfaces*, Baltimore, MD, USA, 2014, pp. 63–70, doi: 10.3115/v1/W14-3110.
[96] A. Moez. (Apr. 2020). *PyCaret: An Open Source, Low-Code Machine Learning Library in Python*. PyCaret. Accessed: Nov. 4, 2021. [Online]. Available: https://www.pycaret.org
[97] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," 2018, *arXiv:1810.04805*.
[98] SpaCy. (2022). *spaCy · Industrial-strength Natural Language Processing in Python*. Accessed: Jan. 25, 2022. [Online]. Available: https://spacy.io/
[99] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd Annu. Design Autom. Conf.*, New York, NY, USA, Jun. 2015, pp. 1–6, doi: 10.1145/2744769.2747942.
[100] C. O. Klingenberg, M. A. V. Borges, and J. A. V. Antunes, Jr., "Industry 4.0 as a data-driven paradigm: A systematic literature review on technologies," *J. Manuf. Technol. Manage.*, vol. 32, no. 3, pp. 570–592, Jun. 2019, doi: 10.1108/JMTM-09-2018-0325.
[101] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021, doi: 10.1109/JIOT.2020.3025916.
[102] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.
[103] N. H. Carreras Guzman, M. Wied, I. Kozine, and M. A. Lundteigen, "Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis," *Syst. Eng.*, vol. 23, no. 2, pp. 189–210, 2020, doi: 10.1002/sys.21509.
[104] E. G. Popkova, E. N. Egorova, E. Popova, and U. A. Pozdnyakova, "The model of state management of economy on the basis of the Internet of Things," in *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*, E. G. Popkova, Ed. Cham, Switzerland: Springer, 2019, pp. 1137–1144, doi: 10.1007/978-3-030-13397-9_116.

[105] J. M. Müller, "Business model innovation in small- and medium-sized enterprises: Strategies for industry 4.0 providers and users," *J. Manuf. Technol. Manage.*, vol. 30, no. 8, pp. 1127–1142, Dec. 2019, doi: 10.1108/JMTM-01-2018-0008.

[106] D. Serpanos, "The cyber-physical systems revolution," *Computer*, vol. 51, no. 3, pp. 70–73, Mar. 2018, doi: 10.1109/MC.2018.1731058.

[107] D. Kiel, C. Arnold, M. Collisi, and K.-I. Voigt, "The impact of the industrial Internet of Things on established business models," in *Proc. 25th Int. Assoc. Manage. Technol.*, 2016, pp. 673–695.

[108] S. K. Singh, Y.-S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart city," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102252, doi: 10.1016/j.scs.2020.102252.

[109] J. Yun, E. Jeong, Y. Lee, and K. Kim, "The effect of open innovation on technology value and technology transfer: A comparative analysis of the automotive, robotics, and aviation industries of Korea," *Sustainability*, vol. 10, no. 7, p. 2459, Jul. 2018, doi: 10.3390/su10072459.

[110] S. Bag, G. Yadav, P. Dhamija, and K. K. Kataria, "Key resources for industry 4.0 adoption and its effect on sustainable production and circular economy: An empirical study," *J. Cleaner Prod.*, vol. 281, Jan. 2021, Art. no. 125233, doi: 10.1016/j.jclepro.2020.125233.

[111] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019, doi: 10.1109/ACCESS.2019.2920763.

[112] K. Kobara, "Cyber physical security for industrial control systems and IoT," *IEICE Trans. Inf. Syst.*, vol. 99, no. 4, pp. 787–795, 2016, doi: 10.1587/transinf.2015ICI0001.

[113] M. P. Ciano, R. Pozzi, T. Rossi, and F. Strozzi, "How IJPR has addressed 'lean': A literature review using bibliometric tools," *Int. J. Prod. Res.*, vol. 57, nos. 15–16, pp. 5284–5317, Aug. 2019, doi: 10.1080/00207543.2019.1566667.

[114] K. Ejsmont, B. Gladysz, D. Corti, F. Castaño, W. M. Mohammed, and J. L. Martinez Lastra, "Towards 'lean industry 4.0'—Current trends and future perspectives," *Cogent Bus. Manage.*, vol. 7, no. 1, Jan. 2020, Art. no. 1781995, doi: 10.1080/23311975.2020.1781995.

[115] L. Waltman, N. J. van Eck, and E. C. M. Noyons, "A unified approach to mapping and clustering of bibliometric networks," *J. Informetrics*, vol. 4, no. 4, pp. 629–635, Oct. 2010, doi: 10.1016/j.joi.2010.07.002.

[116] S. M. Tagirov, Z. K. Omarova, and N. G. Omarova, "Scenarios of region's development in the conditions of the digital economy and priorities of state and corporate management," in *State and Corporate Management of Region's Development in the Conditions of the Digital Economy*, Y. G. Buchaev, S. G. Abdulmanapov, A. S. Abdulkadyrov, and A. A. Khachaturyan, Eds. Cham, Switzerland: Springer, vol. 2021, pp. 121–125, doi: 10.1007/978-3-030-46394-6_21.

[117] T. Limba, A. Stankevičius, and A. Andrulevičius, "Industry 4.0 and national security: The phenomenon of disruptive technology," *Entrepreneurship Sustainability Issues*, vol. 6, no. 3, pp. 1528–1535, Mar. 2019, doi: 10.9770/jesi.2019.6.3(33).

[118] A. Andrulevicius, A. Stankevičius, T. Limba, and K. Driaunys, "Cryptocurrence and national security: Pecularities of interaction," *Transformations Bus. Econ.*, vol. 19, p. 138, Jun. 2020.

[119] J. Montalban, E. Iradier, P. Angueira, O. Seijo, and I. Val, "NOMA-based 802.11n for industrial automation," *IEEE Access*, vol. 8, pp. 168546–168557, 2020, doi: 10.1109/ACCESS.2020.3023275.

[120] I. Forenbacher, S. Husnjak, I. Jovović, and M. Bobić, "Throughput of an IEEE 802.11 wireless network in the presence of wireless audio transmission: A laboratory analysis," *Sensors*, vol. 21, no. 8, p. 2620, Apr. 2021, doi: 10.3390/s21082620.

[121] P. Kasinathan and J. Cuellar, "Securing emergent IoT applications," in *ngineering Trustworthy Software Systems: 4th International School (SETSS)* J. P. Bowen, Z. Liu, and Z. Zhang, Eds. Cham: Springer, Apr. 2019, pp. 99–147, doi: 10.1007/978-3-030-17601-3_3.

[122] R. Beerens, S. C. N. Thissen, W. C. M. Pancras, T. M. P. Gommans, N. van de Wouw, and W. P. M. H. Heemels, "Control allocation for an industrial high-precision transportation and positioning system," *IEEE Trans. Control Syst. Technol.*, vol. 29, no. 2, pp. 876–883, Mar. 2021, doi: 10.1109/TCST.2019.2956899.

[123] X. Jiang, Z. Pang, M. Luvisotto, R. Candell, D. Dzung, and C. Fischione, "Delay optimization for industrial wireless control systems based on channel characterization," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5855–5865, Sep. 2020, doi: 10.1109/TII.2019.2958708.

[124] M. Malatji, A. L. Marnewick, and S. Von Solms, "Cybersecurity capabilities for critical infrastructure resilience," *Inf. Comput. Secur.*, vol. 30, no. 2, pp. 255–279, Mar. 2022, doi: 10.1108/ICS-06-2021-0091.

[125] S. Kim, Y. Won, I.-H. Park, Y. Eun, and K.-J. Park, "Cyber-physical vulnerability analysis of communication-based train control," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6353–6362, Aug. 2019, doi: 10.1109/JIOT.2019.2919066.

[126] H. Khujamatov, E. Reypnazarov, D. Khasanov, and N. Akhmedov, "IoT, IIoT, and cyber-physical systems integration," in *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*, K. K. Singh, A. Nayyar, S. Tanwar, and M. Abouhawwash, Eds. Cham, Switzerland: Springer, 2021, pp. 31–50, doi: 10.1007/978-3-030-66222-6_3.

[127] J. M. Gutierrez-Guerrero and J. A. Holgado-Terriza, "Automatic configuration of OPC UA for industrial Internet of Things environments," *Electronics*, vol. 8, no. 6, p. 600, May 2019, doi: 10.3390/electronics8060600.

[128] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey," *J. Cloud Comput.*, vol. 7, no. 1, p. 21, Dec. 2018, doi: 10.1186/s13677-018-0123-6.

[129] F. Rota, A. Maldarella, C. Talamo, and G. Paganin, "A condition-based maintenance strategy in support of risk management for hospital buildings refrigeration units," 2020, p. 3773. [Online]. Available: http://rpsonline.com.sg/proceedings/9789811485930/html/4420.xml, doi: 10.3850/978-981-14-8593-0_4420-cd.

[130] A. M. J. Skulimowski and V. A. Bañuls, "AI alignment of disaster resilience management support systems," in *Artificial Intelligence and Soft Computing*, Cham, Switzerland: Springer, 2021, pp. 354–366, doi: 10.1007/978-3-030-87897-9_32.

[131] C. G. Machado, M. Winroth, D. Carlsson, P. Almström, V. Centerholt, and M. Hallin, "Industry 4.0 readiness in manufacturing companies: Challenges and enablers towards increased digitalization," *Proc. CIRP*, vol. 81, pp. 1113–1118, Jan. 2019, doi: 10.1016/j.procir.2019.03.262.

[132] T. Sawik, "A linear model for optimal cybersecurity investment in Industry 4.0 supply chains," *Int. J. Prod. Res.*, vol. 60, no. 4, pp. 1368–1385, Dec. 2020, doi: 10.1080/00207543.2020.1856442.