Digital Forensic Investigations on Cyber Physical Production Systems: A Systematic Literature Survey

Norman Nelufule, Pertunia Senamela, Hunadi Mawela, Molebogeng Latakgomo
Council for Scientific and Industrial Research (CSIR)
Information and Cybersecurity Centre (ICSC)
Brummeria, Pretoria, South Africa, 0184
nnelufule@csir.co.za

***Abstract*—Cyber Physical Production systems are complex systems in nature, consisting of several physical and cyber components communicating through sensing and data communication protocols. These systems have played a crucial role in maximizing production and maximized efficiency because of their control, which occurs via a network communication protocol. With such massive advantages, new threats have also emerged, especially in cybersecurity and digital forensics investigations. This article presents a systematic review of the literature on forensic investigation approaches used in physical cyber production systems. The objective is to understand the landscape, challenges, risks, limitations, and opportunities within the forensic investigative processes of cyber physical production systems.**

Keywords—Digital Forensic, Electronic Evidence, Cyber-Physical Systems, Cyber-Physical Production Systems, Internet of Things, Industrial Internet of Things.

I. INTRODUCTION

The era of Industry 4.0 technologies has transformed many industries in terms of increasing production and efficiency [1]. This was precipitated by the nature and functionalities of the emerging technologies employed in Industry 4.0 which are characterized by high-speed data acquisition and data processing. Such characteristics include cloud and edge computing technology, Internet of Things (IoT), Industrial Internet of Things (IIoT), Big Data analytics, Cyber Physical Systems, Smart Systems and etc, as depicted in Fig. 1 [2], [3].

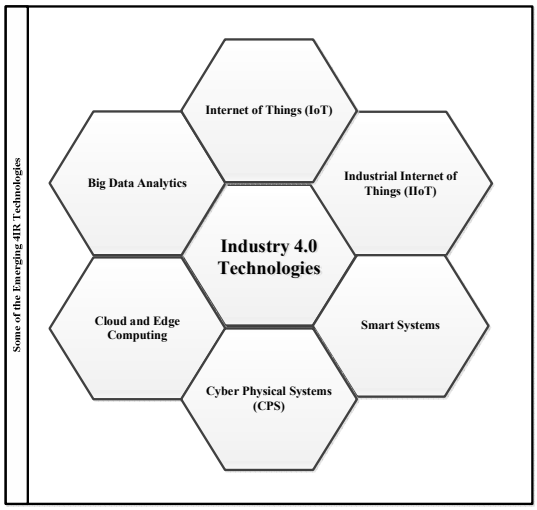

Fig. 1. An overview of some of the key industry 4.0 technologies

This work was financially supported by the Department of Science and Innovation (DSI) of South Africa.

The field of cyber-physical systems (CPS) also emerged from Industry 4.0 technologies as IoT technologies were gaining momentum in their usage by various industries. The CPS incorporates all the mentioned properties of Industry 4.0 technologies into one system by merging the cyber component, the physical component and the human factor component as depicted in Fig. 2 [4]. The cyber components has the responsibility to run software, the physical components ensure that physical activities are conducted and products can be produced, while the human components ensure that there is synergy between the two components [5]-[7].

The main components of cyber components are usually known to consist of a data communication network protocol, which ensures that there is swift and smooth connectivity and data communication; computing and data control centers which ensure that there is efficiency in data production and storage in a safe manner [7]-[9]. The physical components consisting of physical sensors and physical actuators which also have a software component embedded on them to enable them to communicate with the human component and cyber component as depicted in Fig. 2 [10].

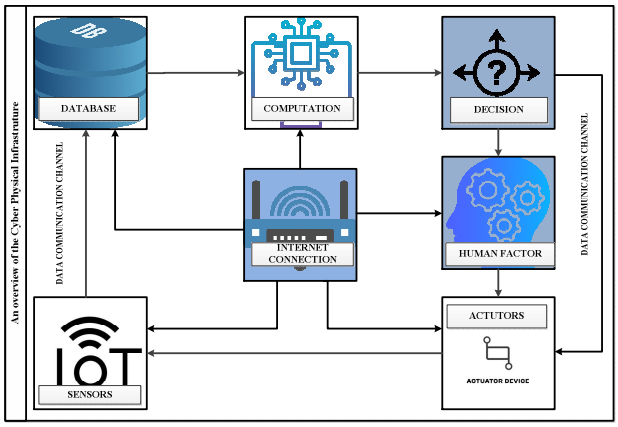

Fig. 2. A pictorial representation of a cyber-physical system [11]

Despite the increase in production and efficiency, cyberphysical production systems (CPPSs) face serious challenges especially with this era of systems security vulnerabilities [12],[13]. The smarter the system is, the more vulnerable it becomes due to the many smart components required to complete the systems efficiently. One of the main concerns of these systems is protecting the entire system against sophisticated cyber threats and sophisticated cyber-attacks [11],[14]. Safeguarding the CPPS comes with numerous challenges due to the complex nature of the system.

979-8-3503-5469-0/24/$31.00 ©2024 IEEE

According to Duo *et al.,* [11], there are several cyber-attacks that emerge at various components of the CPPS. Such threats can be either time-oriented or even oriented or both occurring together [11]. Harkat, *et al.,* [9] have presented a systematic review of cyber physical system security, to identify the main challenges and major concerns. In [6], a review of CPS and cybersecurity systems in smart grid was presented. The main objective was to review the existing standards, protocols, and constraints and recommend the appropriate framework for protecting such structures [6]. Hu *et al.,* [15] also presented a review of the concepts, models, and implementation of CPS, with the aim of analysing the robustness of these models.

Another challenge is to carry out digital forensic investigation in CPPS, due to the variety of sensors required to produce and manipulate data. Mahomed *et al.,* [16] is of the view that every CPS should ensure that security is implemented in such a way that forensic capabilities can be supported in case of breach. In this era of industrialization, it is crucial to ensure that data are stored in the cloud. Sonia, *et al.,* [17] however presented the challenges of forensic investigations on the cloud, due to data accessibility and data privacy. Some of these forensic challenges can also be attributed to legal and ethical challenges, as discussed in [18].

In this article, the main objective is to study the landscape, impact, and opportunities of conducting digital forensics in CPPS. Since the field of CPS is broad and can span several industries, this work is limited to CPPS. To achieve this objective, several research questions that guide this study have been identified. These questions include:

- RQ1: What are the conditions and requirements for forensic investigation in CPPS?
- RQ2: What are the main challenges posed to forensic investigations in CPPS?
- RQ3: What are the opportunities or benefits of conducting forensic investigations on CPPS?
- RQ4: What types of risk / attack could exploit current vulnerabilities in CPPSs?

The remaining work of this paper has been organized as follows: Section II presents the background and literature survey, Section III presents the methodology and research materials, Section IV presents the discussion and analysis, and Section V concludes the work.

II. Background and Literature Survey

A. Internet of Things (IoT)

IoT is the core of industry 4.0 and industry 5.0 technologies. The functioning of CPS and CPPS is based on the effectiveness of IoT connectivity and communications [19]. It important to ensure that a proper security framework of IoT-based CPPS is envisaged. Yang *et al.,* [20] has presented a review of security and forensic investigation challenges on IoT-based CPPS. Rani *et al.,* [21] has expressed that a software defined network security framework using blockchain technologies is most efficient [21]. This is beneficial because blockchain technologies can preserve data integrity and can also be used to maintain the chain of custody in forensic investigations. Another major challenge of IoT is privacy, legal and ethical concerns [22]-[24]. Relating to forensic on IoT, a generic forensic framework has been presented in [25]-[27].

B. Industrial Internet of Things

IIoT is an extension of IoT, which enables the industrial setup to function effectively and efficiently [28]. There are several security concerns in IIoT as presented in a survey by [29], [30]. One way to address such challenges is to employ a digital twin-driven secured edge private cloud [31]. The advantages of using IIoT is through the use of decentralized and adaptive data access control offered by multi-party data sharing [32].

C. Cyber Physical Systems (CPS)

The CPS are being widely adopted, and their complex structure has been studied across the globe [4]. The configurations, and perspectives on their security and forensic investigative process have also been highlighted in [4]. Monostori *e al.,* [7] presented the importance of CPS in manufacturing and the challenges they pose to emerging cyber threats. In [33], it was argued that the main foundational components should be the design of the embedded system that connects the IoT devices [33]. There are also several smart agents that play a crucial role in the functioning of a CPS [34]. Such smartness also pose several challenges in terms of digitization and control of industrial CPS [35].

D. Cyber Physical Production Systems (CPPS)

The CPPS is an extension of the CPS, which operates in almost the same way. According to [13], CPPS have been discovered to have several characteristics, which exposes several research and development challenges [13]. Fraccaroli and Vinco, [36] were of the view that the main challenge is the modelling of a particular CPPS, and propose an analog mixed signal (AMS) because they support device heterogeneity [36]. Another concern with regards to CPPS is the unexpected delays caused by hardware or software and network problems. This can be resolved by implementing domain-specific language (DSL) to avoid ambiguity [37]. The understanding of several classifications of CPPS in terms of their application is also crucial. An analysis of a framework in this regard has been conducted and presented in [38]. The integration of process planning and scheduling also has some bearing implications [39]. Jiang *et al.,* [40] was of the view that dynamic schedule can be effective on a multi-agent CPPS. It is important to impose a connective framework to support the life cycle of CPPS [41]. Transitioning from standard automation to CPPS can also pose several challenges. Some of the critical challenges of the concept of CPPS and their technical and operational challenges have been presented in [42]. Eckhart, *et al.,* [43] presented automated quality driven approach for the analysis of security risks in CPPS. This is crucial to ensure that digital evidence can be retrieved with ease. Hastbacka *et al.,* [44] has expressed that implementing a dynamic edge and cloud services can also improve the monitoring systems. Otto *et al.,* [45] also mentioned that the use of automatic parameter estimation for reusable cyber components can be effective.

E. Digtal Forensics

Digital forensic is a process of identifying digital evidence, extracting such evidence, processing and analyzing the evidence, present the analysis report while maintaining the chain of custody [46], [47]. This field has been adopted in many fields and has a variety of applications, including questioned document examination, computer forensic, network forensic, cloud forensic, mobile forensic, IoT forensic, and cyber physical system forensic [48]-[50]. In

many instances, the procedure to conduct forensic investigation is similar, however the tools can vary depending on the location of the digital evidence [51]. Bangemann *et al.,* [10] also expressed that the main challenge in CPS is the integration of classical components into the CPS [10]. Some of the challenges may also emerge from the engineering methods and tools deployed to automate CPS [52],[53]. Thakur *et al.,* [54] has expressed that heterogeneous smart CPS for industry 5.0 demands the existence of emerging architectures. This becomes a challenge if the old architectures are deployed on newer technologies, which can increase non-heterogeneity between sensors and other IoT devices [54]. Napoleone *et al.,* [55] also presented a review of the characteristics of CPS for smart factories, concentrating on the application and their effectiveness. Chae *et al.,* [56] also presented a survey on the perspective on Industrial CPS when being transformed to AI augmented CPS [56]. Malik *et al.,* [57] discussed the security and forensic challenges on Industry 4.0 SCADA systems. In [58], similar challenges were identified and discussed.

III. Methodology and Research Materials

A. PRISMA Framework

The main survey framework adopted in this article is the preferred reporting items for systematic reviews and Meta-Analyses (PRISMA) as depicted in Fig. 3 [59], [60]. To effectively exploit this framework, it is also important to consider other systematic literature surveys such those discussed in [61]-[63]. The principles discussed in the mentioned literature outline steps such as planning, search strategy, article selection criteria, quality assessment, and analysis, and presented in detail in the next bullet sections.

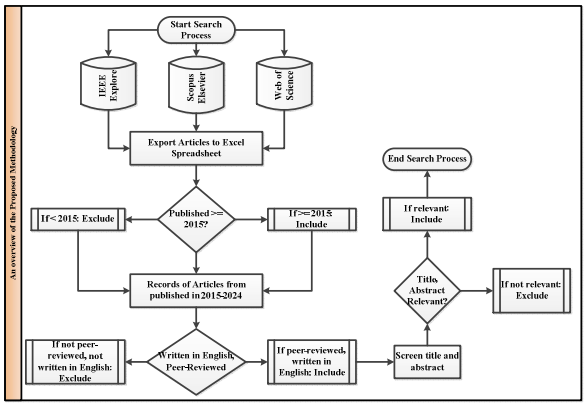

Fig. 3. A Schematic representation of a PRISMA framework

B. Planning

Planning involves prescribing the required scope and materials required. This includes the identification of sources such as indexing databases and the formulation of research questions. The required articles were targeted from Scopus, IEEE, and Web of Science because they index high-quality peer-reviewed articles. Google scholar was not used because it was assumed that all the articles which can be found in these three indexing databases may have been published on Google scholar. Another reason was that some of the articles in Google Scholar may have not been peer reviewed.

C. Search strategy

This involves the combination of search keywords and search phrases which can produce maximum results. The main idea of building is the search strategy is to produce maximum hits of articles, which can be found in each indexing database used. The search strategy and the different hits produced by each search strategy used in shown in Table 1.

TABLE 1: SEARCH STRATEGY

Search Strategy	Hits
(TITLE-ABS-KEY (cyber W/5 physical W/5 production W/5 system*) AND TITLE-ABS-KEY (cybersecurity))	32
(((TITLE-ABS-KEY (cyber W/5 physical W/5 production W/5 system*) AND TITLE-ABS-KEY (cyber AND security))) OR ((TITLE-ABS-KEY (cyber W/5 physical W/5 production W/5 system*) AND TITLE-ABS-KEY (cybersecurity)))) AND NOT ((TITLE-ABS-KEY (cyber W/5 physical W/5 production W/5 system*) AND TITLE-ABS-KEY (cybersecurity)))	85
(TITLE-ABS-KEY (physical* W/5 infrastructure*) AND TITLE-ABS-KEY (digital* W/5 forensic*))	12

D. Selection Criteria

Article selection criteria were based on the publication language, of which the preferred language was English. The articles should also be available as full texts without paying a subscription. The articles were also limited to those published in Engineering or Computer Science literatures. The summarized exclusion and inclusion criteria is presented in Table 2.

TABLE 2: A SUMMARY OF EXCLUSION AND INCLUSION CRITERIA

Exclusion Criteria (EC)	
EC	Articles not published in English language
EC	Articles outside the scope of cyber physical systems and digital forensics
EC	Duplicates from the other indexing databases
Inclusion Criteria (IC)	
IC	Articles relevant to cyber physical systems and digital forensics
IC	Articles published from 2025 to date
IC	Articles published in English
IC	Articles with full text
IC	Articles published in engineering and computer science related disciplines

E. Quality Assessment

The titles and abstracts were reviewed to assess the quality of the content of the required research materials. Duplicate articles were also removed using the Excel tool.

IV. Discussion and Analysis

In this article, several published works have been analyzed and compared against this work in terms of the features used for comparative analysis. Table 3 shows some of the analyzed reviewed research articles analyzed.

TABLE 3: AN ANALYSIS AND COMPARISON OF REVIEWED RESEARCH ARTICLES

Authors	***Contribution***	***A***	***B***	***C***	***D***	***E***
Zhang et al, 2023 [4]	Overview and perspectives of the advances in Industrial Cyber-Physical Systems	☑	☒	☑	☒	☒
Lyu et al, 2019 [64]	Safety and security risks assessment in cyberphysical systems	☑	☑	☑	☒	☒
Fraccaroli and Vinco, 2023 [65]	Modelling Cyberphysical Production Systems with SystemC_AMS	☑	☑	☒	☒	☒
Vogel-Heuser et al, 2021 [37]	Redeployment of Smart Algorithms in Cyber-Physical Production System using DSL4hDNCS	☑	☑	☑	☒	☒
Zhu and Zhang, 2018 [66]	A Cyber-Physical Production System Framework of Smart CNC Machining Monitoring System	☑	☑	☑	☒	☒
Uhlemann et al, 2017 [67]	The Digital Twin: Realizing the Cyber-Physical Production System for Industry 4.0	☑	☑	☑	☒	☒
Harrison et al, [41]	A Connective Framework to Support the Lifecycle of Cyber-Physical Production Systems	☑	☑	☑	☑	☒
Eckhart et al, [43]	QualSec: An Automated Quality-Driven Approach for Security Risk Identification in Cyber-Physical Production Systems	☑	☑	☒	☑	☒
Hastbacka et al, [68]	Dynamic Edge and Cloud Service Integration for Industrial IoT and Production Monitoring Applications of Industrial Cyber-Physical Systems	☑	☑	☒	☑	☒
Robiero and Bjorkman 2018 [42]	Transitioning from Standard Automation Solutions to Cyber-Physical Production Systems: An Assessment of Critical Conceptual and Technical Challenges	☑	☑	☒	☑	☑
Mercan et al, 2020 [69]	Security, Privacy and Ethical Concerns of IoT Implementations in Hospitality Domain	☑	☒	☑	☒	☒
Mahomed et al, 2020 [16]	Cyber-Physical Systems Forensics	☑	☒	☒	☑	☑
Kayan et al, 2022 [70]	Cybersecurity of Industrial Cyber-Physical Systems: A Review	☑	☑	☑	☒	☒
Hasan et al, 2023 [71]	Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations	☑	☑	☑	☑	☒
Wang et al, 2022 [72]	Digital Workers in Cyber-Physical-Social Systems for PCB Manufacturing	☑	☑	☑	☒	☒
Xing and Shen, 2024 [73]	Security Control of Cyber–Physical Systems Under Cyber Attacks: A Survey	☑	☑	☑	☒	☒
Lyu et al, 2019 [64]	Safety and security risk assessment in cyberphysical systems	☑	☑	☑	☒	☒
Mahomed et al, 2020 [74]	Cyber–physical systems forensics: Today and tomorrow	☑	☒	☑	☑	☑
Kim et al, 2023 [75]	Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey	☑	☑	☒	☑	☑
Harkat et al, 2024 [76]	Cyber-physical systems security: A systematic review	☑	☑	☑	☒	☒
Leitao et al, 2016 [77]	Smart Agents in Industrial Cyber-Physical Systems	☑	☑	☑	☒	☒
Grady et al, 2021 [78]	When Smart Systems Fail: The Ethics of Cyber–Physical Critical Infrastructure Risk	☑	☑	☑	☒	☒
Canonico and Sperli, 2023 [79]	Industrial cyber-physical systems protection: A methodological review	☑	☑	☑	☒	☒
This article	*A comprehensive analysis of challenges and opportunities within the forensic investigative processes of cyber physical production systems*	☑	☑	☑	☑	☑

Note: A: Security and Privacy B: Frameworks, C: Legal and Ethical, D: Evidence Acquisition, E: Evidence Analysis, ☑: discussed, ☒: Not discussed.

A. Findings of the Research

The findings of the systematic literature review indicate that while there has been significant progress in developing digital forensic technologies and frameworks applicable to CPPS, there are several gaps which remain unresolved. Some of the missing gas is the lack of standardized frameworks, and this limits the ability to conduct comprehensive digital forensic investigation.

Another challenge is the limitation in the integration of real-time forensic capabilities because the dynamic nature of CPPS requires real-time data acquisition and processing. The CPPS forensics investigation encompasses the investigation of cyber incidents which may affect some portion or the entire physical production systems. The findings of this review have revealed that there is growing interest in data-driven research forensic investigations.

Several challenges were identified which hamper comprehensive and successful forensic investigation, and such challenges include complexity of CPS, the need for real-time data acquisition and analysis, maintaining the integrity of evidence through chain of custody, and the integration of diverse non-heterogeneous technologies. Some of these complex CPS application technologies are depicted in Fig. 4.

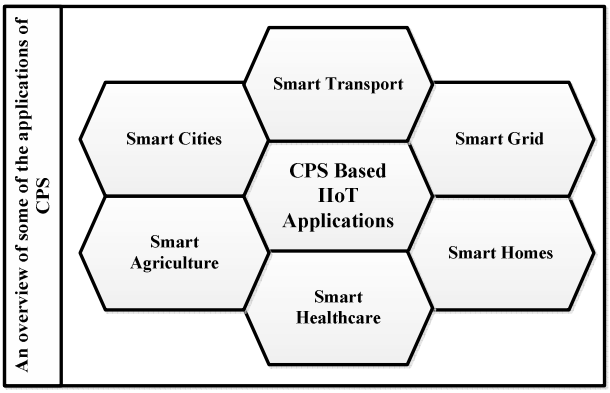

Fig. 4. Some applications of CPS where emerging cyberthreats are rife and enormous and forensic investigations are complex.

The findings presented here were based on the analysis of research articles between 2015 and 2025. As per Fig. 5, at the time of search there were only two articles published in 2015, but the research reached its first peak in 2018, and the articles reached the first peak at 57 articles. In 2021, the articles reached the second peak at 76 articles.

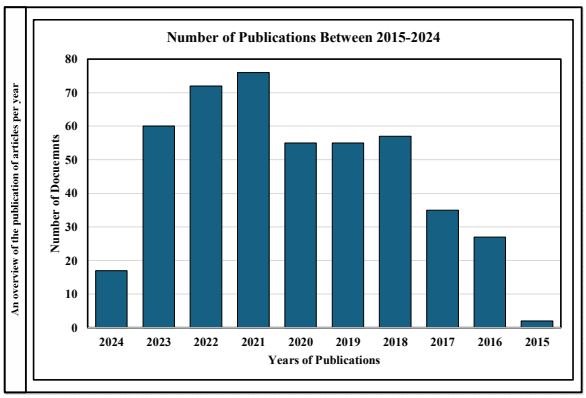

Fig. 5. An illustration of published articles per year

B. Recommendations and Limitations

To address the identified gaps and limitations of existing technologies, the following recommendations are proposed:

- **Standardization:**

Researchers should collaborate with technologists to develop standardized forensic frameworks customized for CPS to ensure consistency and reliability in investigations.

- **Real-Time Forensics:**

There is a need for real-time data acquisition, analysis, and processing. This will also need the use of advanced big data analytics, AI and ML techniques.

- **Interdisciplinary Collaboration:**

Worldwide collaboration is required between cybersecurity professionals, legal experts, forensic specialists, and industry practitioners to address the multifaceted challenges of CPPS forensics. This will also enhance the sharing of real-world data sets to facilitate the development and testing of forensic tools.

C. Limitations

The primary limitations of this research encompass the scope of literature that covered articles from only three databases with articles published between 2015 and 2024. The selected indexing databases were limited to IEEE Xplore, Scopus, and Web of Science, which may not cover all relevant literature, potentially leading to a biased overview. There is also an element of rapid technological advancement, especially in the space of CPS, and this may also render the findings in this research obsolete.

D. Answering Research Questions

The identified research questions, has been summarised in Table 4.

TABLE 4: TABLE OF RESEARCH QUESTIONS AND SOLUTIONS

Research Question	Research Solution
RQ1: What are the conditions and requirements for forensic investigation in CPPS?	The security technologies should be designed to aid forensic investigation work
RQ2: What are the main challenges posed to forensic investigations in CPPS?	Heterogeneity of connected devices. Technologies such as DSL can be because they naturally support heterogeneity
RQ3: What are the opportunities or benefits of conducting forensic investigations on CPPS?	Data can be hosted on the cloud, and since it is a production system, data logs are saved for the purpose of inspections
RQ4: What types of risk / attack could exploit current vulnerabilities in CPPSs?	The main attacks relates to data breach, malware to interpret production system.

V. Conclusion and Future Work

The presented systematic review of the literature has highlighted that CPPS requires the use of ML technologies to detect, process, and analyze digital evidence. This study also presented some of the bottlenecks such as the lack of standardized frameworks and the lack of data availability to train the newly developed technologies.

Digital forensic investigations in CPPS are crucial for ensuring the security and resilience of modern production systems. This systematic literature survey provides a foundation for future research, highlighting current trends, challenges, and opportunities in this evolving field. By addressing the identified gaps and following the proposed recommendations, the field of CPPS forensics can advance significantly, contributing to the overall security and efficiency of Industry 4.0.

Future research will be extended to the development of standardized forensic methodologies and technologies which will enhance real-time forensic capabilities. This systematic literature survey provides a foundation for future research, highlighting current trends, existing challenges, and opportunities. Another active area worth exploring is AI and Blockchain technology for privacy preservation and maintaining the chain of custody by making use of distributed ledger technology.

Acknowledgment

The authors acknowledge the Department of Science and Innovation (DSI), South Africa, for their funding contribution towards this research initiative.

References

[1] E. L. Alvarez-Aros and C. A. Bernal-Torres, "Technological competitiveness and emerging technologies in industry 4.0 and industry 5.0," *An Acad Bras Cienc*, vol. 93, no. 1, 2021, doi: 10.1590/0001-3765202120191290.

[2] M. T. Okano, "IOT and Industry 4.0: The Industrial New Revolution," *ICMIS-17 - International Conference on Management and Information Systems*, no. September, 2017.

[3] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, "Industry 4.0 and Industry 5.0—Inception, conception and perception," *J Manuf Syst*, vol. 61, pp. 530–535, Oct. 2021, doi: 10.1016/j.jmsy.2021.10.006.

[4] K. Zhang, Y. Shi, S. Karnouskos, T. Sauter, H. Fang, and A. W. Colombo, "Advancements in Industrial Cyber-Physical Systems: An Overview and Perspectives," Jan. 01, 2023, *IEEE Computer Society*. doi: 10.1109/TII.2022.3199481.

[5] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap, "Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review," *ACM Comput Surv*, vol. 55, no. 10, pp. 1–36, Oct. 2023, doi: 10.1145/3565570.

[6] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," Jan. 01, 2023, *Academic Press*. doi: 10.1016/j.jnca.2022.103540.

[7] L. Monostori *et al.*, "Cyber-physical systems in manufacturing," *CIRP Annals*, vol. 65, no. 2, pp. 621–641, 2016, doi: 10.1016/j.cirp.2016.06.005.

[8] "Cyber-Physical Security and Critical Infrastructure," 2023.

[9] H. Harkat, L. M. Camarinha-Matos, J. Goes, and H. F. T. Ahmed, "Cyber-physical systems security: A systematic review," *Comput Ind Eng*, vol. 188, Feb. 2024, doi: 10.1016/j.cie.2024.109891.

[10] T. Bangemann, M. Riedl, M. Thron, and C. Diedrich, "Integration of Classical Components into Industrial Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 947–959, May 2016, doi: 10.1109/JPROC.2015.2510981.

[11] W. Duo, M. C. Zhou, and A. Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges," May 01, 2022, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/JAS.2022.105548.

[12] N. Nelufule, T. Singano, and M. Masango, "A Comprehensive Exploration of Digital Forensics Investigations in Embedded Systems, Ubiquitous Computing, Fog Computing, and Edge Computing," in *2024 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/icABCD62167.2024.10645254.

[13] L. Monostori, "Cyber-physical production systems: Roots, expectations and R&D challenges," in *Procedia CIRP*, Elsevier B.V., 2014, pp. 9–13. doi: 10.1016/j.procir.2014.03.115.

[14] D. Zhang, Q. G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," *ISA Trans*, vol. 116, pp. 1–16, Oct. 2021, doi: 10.1016/j.isatra.2021.01.036.

[15] F. Hu *et al.*, "Robust Cyber-Physical Systems: Concept, models, and implementation," *Future Generation Computer Systems*, vol. 56, pp. 449–475, Mar. 2016, doi: 10.1016/j.future.2015.06.006.

[16] N. Mahomed, J. Al-Jaroodi, and I. Jawhar, "Cyber-Physical Systems Forensics," in *2020 IEEE Systems Security Symposium (SSS)*, USA: IEEE, Aug. 2020, p. 17.

[17] S. Sonia Akter and M. Shahriar Rahman, "Cloud Forensic: Issues, Challenges and Solution Models," *ArXiv*, pp. 2–23, 2023.

[18] M. M. Losavio, K. P. Chow, A. Koltay, and J. James, "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security," *SECURITY AND PRIVACY*, vol. 1, no. 3, May 2018, doi: 10.1002/spy2.23.

[19] K. Kaushik, S. Dahiya, A. Bhardwaj, and Y. Maleh, *Internet of Things and Cyber Physical Systems*. CRC Press, 2022. doi: 10.1201/9781003283003.

[20] W. Yang, M. N. Johnstone, L. F. Sikos, and S. Wang, "Security and Forensics in the Internet of Things: Research Advances and Challenges," in *Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT 2020*, Institute of Electrical and Electronics Engineers Inc., Apr. 2020, pp. 12–17. doi: 10.1109/ETSecIoT50046.2020.00007.

[21] S. Rani, H. Babbar, G. Srivastava, T. R. Gadekallu, and G. Dhiman, "Security Framework for Internet-of-Things-Based Software-Defined Networks Using Blockchain," *IEEE Internet Things J*, vol. 10, no. 7, pp. 6074–6081, Apr. 2023, doi: 10.1109/JIOT.2022.3223576.

[22] E. Shaikh, I. Mohiuddin, and A. Manzoor, "Internet of Things (IoT): Security and Privacy Threats," in *2nd International Conference on Computer Applications & Information Security (ICCAIS' 2019)* , Daudi Arabia: IEEE, 2019, pp. 1–6.

[23] G. Baldini, M. Botterman, R. Neisse, and M. Tallacchini, "Ethical Design in the Internet of Things," *Sci Eng Ethics*, vol. 24, no. 3, pp. 905–925, Jun. 2018, doi: 10.1007/s11948-016-9754-5.

[24] M. El-Khoury and C. L. Arikan, "From the internet of things toward the internet of bodies: Ethical and legal considerations," *Strategic Change*, vol. 30, no. 3, pp. 307–314, May 2021, doi: 10.1002/jsc.2411.

[25] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, Institute of Electrical and Electronics Engineers Inc., Sep. 2016, pp. 356–362. doi: 10.1109/FiCloud.2016.57.

[26] A. P. Renold, "Survey of Evidence Collection Methods for Internet of Things Forensics," in *Proceedings of the 1st IEEE International Conference on Networking and Communications 2023, ICNWC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICNWC57852.2023.10127407.

[27] N. Koroniotis, N. Moustafa, and E. Sitnikova, "Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions," 2019, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2019.2916717.

[28] V. R. Kebande, "Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0," *Forensic Science International: Reports*, vol. 5, Jul. 2022, doi: 10.1016/j.fsir.2022.100257.

[29] T. Gebremichael *et al.*, "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges,"

IEEE Access, vol. 8, pp. 152351–152366, 2020, doi: 10.1109/ACCESS.2020.3016937.

[30] G. De La Torre Parra, P. Rad, and K. K. R. Choo, "Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities," 2019. doi: 10.1016/j.jnca.2019.02.022.

[31] M. Al-Hawawreh and M. S. Hossain, "Digital twin-driven secured edge-private cloud Industrial Internet of Things (IIoT) framework," *Journal of Network and Computer Applications*, vol. 226, Jun. 2024, doi: 10.1016/j.jnca.2024.103888.

[32] R. Saha, G. Kumar, M. Conti, T. Devgun, and J. J. P. C. Rodrigues, "AALMOND: Decentralized Adaptive Access Control of Multi-Party Data Sharing in Industrial Networks," *IEEE Internet Things J*, 2024, doi: 10.1109/JIOT.2024.3392933.

[33] P. Marwedel, *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things*, Fourth Edition., vol. 4. Germany: Springer, 2021. [Online]. Available: http://www.springer.com/series/8563

[34] P. Leitão, S. Karnouskos, L. Ribeiro, J. Lee, T. Strasser, and A. W. Colombo, "Smart Agents in Industrial Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1086–1101, May 2016, doi: 10.1109/JPROC.2016.2521931.

[35] O. Cardin, W. Derigent, and D. Trentesaux, *Digitalization and Control of Industrial Cyber-Physical Systems*, 1st ed., vol. 1. United Kingdom: WILEY, 2022.

[36] E. Fraccaroli and S. Vinco, "Modeling Cyber-Physical Production Systems with SystemC-AMS," *IEEE Transactions on Computers*, vol. 72, no. 7, pp. 2039–2051, Jul. 2023, doi: 10.1109/TC.2022.3226567.

[37] B. Vogel-Heuser, E. Trunzer, D. Hujo, and M. Sollfrank, "(Re)deployment of Smart Algorithms in Cyber-Physical Production Systems Using DSL4hDNCS," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 542–555, Apr. 2021, doi: 10.1109/JPROC.2021.3050860.

[38] O. Cardin, "Classification of cyber-physical production systems applications: Proposition of an analysis framework," *Comput Ind*, vol. 104, pp. 11–21, Jan. 2019, doi: 10.1016/j.compind.2018.10.002.

[39] H. Meissner and J. C. Aurich, "Implications of cyber-physical production systems on integrated process planning and scheduling," in *Procedia Manufacturing*, Elsevier B.V., 2019, pp. 167–173. doi: 10.1016/j.promfg.2018.12.027.

[40] Z. Jiang, Y. Jin, E. Mingcheng, and Q. Li, "Distributed Dynamic Scheduling for Cyber-Physical Production Systems Based on a Multi-Agent System," *IEEE Access*, vol. 6, pp. 1855–1869, Dec. 2017, doi: 10.1109/ACCESS.2017.2780321.

[41] R. Harrison, D. A. Vera, and B. Ahmad, "A Connective Framework to Support the Lifecycle of Cyber-Physical Production Systems," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 568–581, Apr. 2021, doi: 10.1109/JPROC.2020.3046525.

[42] L. Ribeiro and M. Bjorkman, "Transitioning from Standard Automation Solutions to Cyber-Physical Production Systems: An Assessment of Critical Conceptual and Technical Challenges," *IEEE Syst J*, vol. 12, no. 4, pp. 3816–3827, Dec. 2018, doi: 10.1109/JSYST.2017.2771139.

[43] M. Eckhart, A. Ekelhart, S. Biffl, A. Luder, and E. Weippl, "QualSec: An Automated Quality-Driven Approach for Security Risk Identification in Cyber-Physical Production Systems," *IEEE Trans Industr Inform*, vol. 19, no. 4, pp. 5870–5881, Apr. 2023, doi: 10.1109/TII.2022.3193119.

[44] D. Hastbacka *et al.*, "Dynamic Edge and Cloud Service Integration for Industrial IoT and Production Monitoring Applications of Industrial Cyber-Physical Systems," *IEEE Trans Industr Inform*, vol. 18, no. 1, pp. 498–508, Jan. 2022, doi: 10.1109/TII.2021.3071509.

[45] J. Otto, B. Vogel-Heuser, and O. Niggemann, "Automatic Parameter Estimation for Reusable Software Components of Modular and Reconfigurable Cyber-Physical Production Systems in the Domain of Discrete Manufacturing," *IEEE Trans Industr Inform*, vol. 14, no. 1, pp. 275–282, Jan. 2018, doi: 10.1109/TII.2017.2718729.

[46] M. Pollitt, M. Caloyannides, J. Novotny, and S. Shenoi, "Digital Forensics: Operational, Legal and Research Issues.," in *Springer*, vol. XVII, Springer, 2004, pp. 1–11.

[47] G. W. Manes and E. D. Avansic, "Digital Forensics," *IEEE Security & Privacy*, pp. 1–4, Mar. 2009. [Online]. Available: www.thekesslernotebook.com,

[48] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations," Aug. 01, 2022, *Elsevier B.V.* doi: 10.1016/j.iot.2022.100544.

[49] H. I. Mohd Abdullah *et al.*, "Smart Grid Digital Forensics Investigation Framework," in *2020 8th International Conference on Information Technology and Multimedia, ICIMU 2020*, 2020. doi: 10.1109/ICIMU49871.2020.9243536.

[50] F. Casino *et al.*, "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," 2022, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2022.3154059.

[51] S. Sachdeva, B. L. Raina, and A. Sharma, "Analysis of Digital Forensic Tools," *J Comput Theor Nanosci*, vol. 17, no. 6, 2020, doi: 10.1166/jctn.2020.8916.

[52] R. Harrison, D. Vera, and B. Ahmad, "Engineering Methods and Tools for Cyber-Physical Automation Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 973–985, May 2016, doi: 10.1109/JPROC.2015.2510665.

[53] L. Wang, M. Törngren, and M. Onori, "Current status and advancement of cyber-physical systems in manufacturing," *J Manuf Syst*, vol. 37, pp. 517–527, Oct. 2015, doi: 10.1016/j.jmsy.2015.04.008.

[54] P. Thakur and V. Kumar Sehgal, "Emerging architecture for heterogeneous smart cyber-physical systems for industry 5.0," *Comput Ind Eng*, vol. 162, Dec. 2021, doi: 10.1016/j.cie.2021.107750.

[55] A. Napoleone, M. Macchi, and A. Pozzetti, "A review on the characteristics of cyber-physical systems for the future smart factories," Jan. 01, 2020, *Elsevier B.V.* doi: 10.1016/j.jmsy.2020.01.007.

[56] J. Chae, S. Lee, J. Jang, S. Hong, and K.-J. Park, "A Survey and Perspective on Industrial Cyber-Physical Systems (ICPS): From ICPS to AI-Augmented ICPS," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 257–272, Oct. 2023, doi: 10.1109/ticps.2023.3323600.

[57] V. R. Malik, K. Gobinath, S. Khadsare, A. Lakra, and S. V. Akulwar, "Security Challenges in Industry 4.0 SCADA Systems-A Digital Forensic Prospective," in *ICAICST 2021 - 2021 International Conference on Artificial Intelligence and Computer Science Technology*, Institute of Electrical and Electronics Engineers Inc., Jun. 2021, pp. 229–233. doi: 10.1109/ICAICST53116.2021.9497829.

[58] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," *Journal of Information Security and Applications*, vol. 52, Jun. 2020, doi: 10.1016/j.jisa.2020.102500.

[59] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," 2021. doi: 10.1136/bmj.n71.

[60] M. J. Page *et al.*, "PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews," Mar. 29, 2021, *BMJ Publishing Group*. doi: 10.1136/bmj.n160.

[61] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," Jan. 2009. doi: 10.1016/j.infsof.2008.09.009.

[62] K. S. Khan, R. Kunz, J. Kleijnen, and G. Antes, "Five steps to conducting a systematic review," *J R Soc Med*, vol. 96, pp. 118–121, Mar. 2003, [Online]. Available: http://www.ncbi.nlm.nih.gov/entrez/query/

[63] C. Okoli, "A Guide to Conducting a Standalone Systematic Literature Review," *Communications of the Association for Information Systems*, vol. 37, pp. 1–33, Nov. 2015, [Online]. Available: http://aisel.aisnet.org/cais/vol37/iss1/43

[64] X. Lyu, Y. Ding, and S. H. Yang, "Safety and security risk assessment in cyberphysical systems," Sep. 01, 2019, *Institution of Engineering and Technology*. doi: 10.1049/iet-cps.2018.5068.

[65] E. Fraccaroli and S. Vinco, "Modeling Cyber-Physical Production Systems with SystemC-AMS," *IEEE Transactions on Computers*, vol. 72, no. 7, pp. 2039–2051, Jul. 2023, doi: 10.1109/TC.2022.3226567.

[66] K. Zhu and Y. Zhang, "A Cyber-Physical Production System Framework of Smart CNC Machining Monitoring System," *IEEE/ASME Transactions on Mechatronics*, vol. 23, no. 6, pp. 2579–2586, Dec. 2018, doi: 10.1109/TMECH.2018.2834622.

[67] T. H. J. Uhlemann, C. Lehmann, and R. Steinhilper, "The Digital Twin: Realizing the Cyber-Physical Production System for Industry 4.0," in *Procedia CIRP*, Elsevier B.V., 2017, pp. 335–340. doi: 10.1016/j.procir.2016.11.152.

[68] D. Hastbacka *et al.*, "Dynamic Edge and Cloud Service Integration for Industrial IoT and Production Monitoring Applications of Industrial Cyber-Physical Systems," *IEEE Trans Industr Inform*, vol. 18, no. 1, pp. 498–508, Jan. 2022, doi: 10.1109/TII.2021.3071509.

[69] S. Mercan, K. Akkaya, L. Cain, and J. Thomas, "Security, Privacy and Ethical Concerns of IoT Implementations in Hospitality Domain," in *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, IEEE, Nov. 2020, pp. 198–203. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00048.

[70] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, "Cybersecurity of Industrial Cyber-Physical Systems: A Review," *ACM Comput Surv*, vol. 54, no. 11s, Sep. 2022, doi: 10.1145/3510410.

[71] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," Jan. 01, 2023, *Academic Press*. doi: 10.1016/j.jnca.2022.103540.

[72] Y. Wang, J. Wang, Y. Tian, X. Wang, and F. Y. Wang, "Digital Workers in Cyber-Physical-Social Systems for PCB Manufacturing," *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 688–692, 2022, doi: 10.1109/JRFID.2022.3212782.

[73] W. Xing and J. Shen, "Security Control of Cyber–Physical Systems under Cyber Attacks: A Survey," Jun. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/s24123815.

[74] N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "Cyber–physical systems forensics: Today and tomorrow," *Journal of Sensor and Actuator Networks*, vol. 9, no. 3, Aug. 2020, doi: 10.3390/JSAN9030037.

[75] K. Kim, I. M. Alshenaifi, S. Ramachandran, J. Kim, T. Zia, and A. Almorjan, "Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey," Apr. 01, 2023, *MDPI*. doi: 10.3390/s23073681.

[76] H. Harkat, L. M. Camarinha-Matos, J. Goes, and H. F. T. Ahmed, "Cyber-physical systems security: A systematic review," *Comput Ind Eng*, vol. 188, Feb. 2024, doi: 10.1016/j.cie.2024.109891.

[77] P. Leitão, S. Karnouskos, L. Ribeiro, J. Lee, T. Strasser, and A. W. Colombo, "Smart Agents in Industrial Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1086–1101, May 2016, doi: 10.1109/JPROC.2016.2521931.

[78] C. Grady, S. Rajtmajer, and L. Dennis, "When Smart Systems Fail: The Ethics of Cyber–Physical Critical Infrastructure Risk," *IEEE Transactions on Technology and Society*, vol. 2, no. 1, pp. 6–14, Feb. 2021, doi: 10.1109/tts.2021.3058605.

[79] R. Canonico and G. Sperlì, "Industrial cyber-physical systems protection: A methodological review," *Comput Secur*, vol. 135, Dec. 2023, doi: 10.1016/j.cose.2023.103531.