Trustworthiness-Related Risks in Autonomous Cyber-Physical Production Systems – A Survey

Maryam Zahid
Mälardalen University
Eskilstuna, Sweden
Email: maryam.zahid@mdu.se

Alessio Bucaioni
Mälardalen University
Eskilstuna, Sweden
Email: alessio.bucaioni@mdu.se

Francesco Flammini
Mälardalen University
Eskilstuna, Sweden
Email: francesco.flammini@mdu.se

Abstract—**The production industry is looking for new solutions to improve the reliability, safety and efficiency of traditional processes. Current developments in artificial intelligence and machine learning have enabled a high level of autonomy in smart-manufacturing and production systems within Industry 4.0, thus paving the way towards fully Autonomous Cyber-Physical Production Systems (ACPPS). Although ACPPS can have many advantages, there still remains a concern regarding how much we can trust those systems, due to limited predictability, transparency, and explainability, as well as emerging vulnerabilities related to machine learning systems. In this paper, we present the findings of a study conducted on the possible risks related to the trustworthiness of ACPPS, and the consequences they have on the system and its environment.**

I. Introduction

The 4th industrial revolution brought forward the concept of Cyber-Physical Systems in various domains of industrial control systems (ICS), medical devices, autonomous vehicles, smart wearable devices, and smart grids [2]. These are intelligent and networked systems developed with close cooperation of their electrical, software, and mechanical components [1]. The demand for such systems is now also seen in the production or manufacturing industry due to its capabilities of simplifying and handling complex design and development challenges; hence known as Cyber-Physical Production/Manufacturing Systems (CPPS) or (CPMS). A further revolution in the industrial process brought about a new concept of Industry 5.0 [3], by having artificial intelligence (AI) technologies such as Cobots (Collaborative Robots) [4] integrated into traditional cyber-physical production systems thus transforming CPPS into autonomous cyber-physical production systems (ACPPS) (See figure 1). The use of cobots (collaborative AI agents) can help maximize production processes while addressing the varying demands of the market. ACPPS constantly requires the availability of its resources and the exchange of the required data in order to enable the safe and successful execution of operations. This in turn relies on the system to be trustworthy [10], minimizing the risks of operational disruptions or other process-related errors [5]. According to a reference taxonomy, trustworthiness can be associated with attributes such as availability, reliability, security, safety, robustness (defined as an integrated concept of resilience) [6], and ethical and legal aspects [7]. Lack of proper implementation of security policies in ACPPS can lead to intentional attacks thus posing a threat to the safety of the system and its users [8]. ACPPS being vulnerable to cyber-attacks can lead to a negative impact on the production process such that it may result in incorrect manufacturing of the parts of a product making it hazardous to its users and its environment [9]. Thus ensuring trustworthiness in ACPPS is of critical importance.

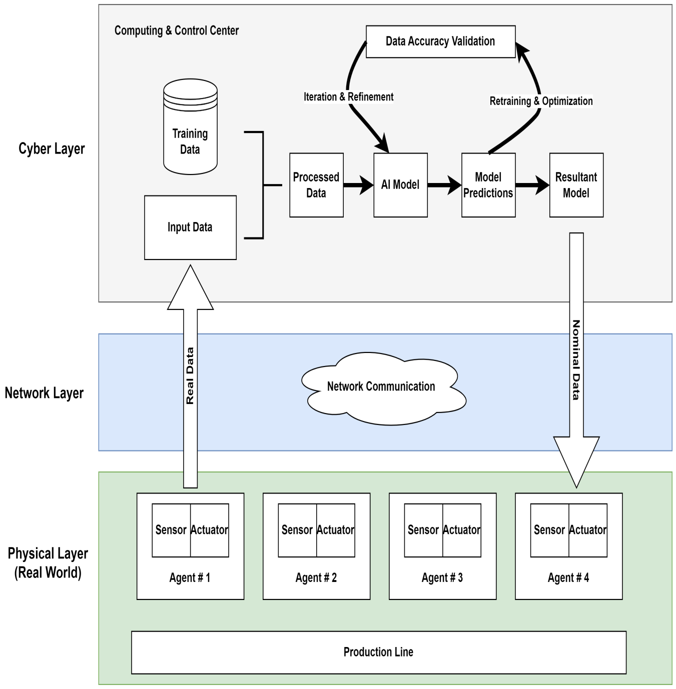

Fig. 1. Architecture of Autonomous Cyber-Physical Production System

To the best of our knowledge, there does exist a certain set of secondary and tertiary studies that discuss the importance of having attributes of trustworthiness implemented in CPPS, but there lacks a systematic study on the possible presence of risks related to trustworthiness in ACPPS, their consequences on the system and how were they observed.

The rest of the paper is structured as Section II summarizing the related work, Section III discussing the research methodology adopted for this study, Section IV presenting the results of our findings along with a brief discussion, Section V conclusion, and Section VI future work.

II. Related Work

A combination of embedded computers and communication systems known as the cyber-physical systems (CPS) has now become an integral part of various domains including the production or manufacturing domain thus known as a cyber-physical production system (CPPS) or a cyber-physical manufacturing system (CPMS) [11]. Although over the last decade, many research articles have been published on the evaluation of CPPS, very little has been done on autonomous CPPS; a type of CPPS integrated with artificial intelligence recently introduced. To the best of our knowledge [12], this study is the first of its kind presenting an analysis conducted on the evaluation of ACPPS in terms of the presence of risks related to its trustworthiness and in-specific areas of ACPPS affected by it.

A survey of surveys conducted on the security and privacy of CPPS and CPMS discuss the implementation of a risk management process such that a detection algorithm is used for identifying vulnerabilities, and as a mitigation measure apply cryptography solutions in almost all types of CPS. Our study on the other hand presents findings on the evaluation of ACPPS in terms of its trustworthiness rather than just its security and privacy [11]. A decade-wide study conducted on the security aspects in Industrial cyber-physical systems (ICPS) summarizes the identification techniques used such as attack-detection techniques to highlight the security-related risks along with possible mitigation measures [13]. Yaccoub et al. in their study provided an overview of the identified security-related vulnerabilities, threats (cyber and physical), and failures in an Industrial Internet of Things (IIOT) along with the proposed mitigation measures and their short-comings [14]. A systematic literature review conducted in the year 2019 after introducing the concept of ACPPS discusses the presence of cyber-security-related threats[12]. According to this study, the source of the cyber-attack can be categorized as internal or external in nature; for which it suggests the use of software-defined networks (SND)s and network function virtualization (NFV)s where by rapidly detecting and replacing failed components with its virtual implementation it can assist in automatic incident response. A study conducted by Geismann et al. on model-driven engineering in CPS discusses the seven specific model-based tools used for modeling and evaluation of the system at the early stages of adopted the software development life cycle [15]. The study although relevant but is focused on CPS rather than on CPPS. Another study conducted on the state-of-the-art tools used in model-driven engineering of the system related to Industry 5.0 provides an overview of the SySML modeling language-based tools used for the construction and evaluation of the AI-integrated CPS [16]. The study presented does not specify the attributes of the system being evaluated.

In general, our study presents an overview of the possible presence of trustworthiness-related risks in ACPPS, what component of ACPPS is mainly affected by the presence of such vulnerabilities and how are they evaluated.

III. Research Methodology

This section discussed the methodology adopted to conduct a literature survey [17], [18]. The process began in a systematic way consisting of the following three main phases:

- **Planning Phase:** This phase involved developing the motivation behind conducting such a survey on the risks related to trustworthiness in autonomous cyber-physical production systems, defining the research objectives and their associated research questions for the study, and finally specifying a protocol to conduct the study systematically.
- **Execution Phase:** The phase began with an automated search of peer-reviewed articles in the selected scientific databases and indexing systems. Upon collecting articles a filtration process is applied, eliminating articles that either did not fulfill the defined selection criteria or that were redundant. Furthermore, to avoid missing any related articles a backward and forward snowballing was conducted [19]. The next step of this phase involved extracting data by individually analyzing the collected set of primary studies against the defined parameters of the planned data-extraction form. The last step of this phase includes the analysis of the extracted data, as to determine the answers to the defined research questions. As a result of this phase, we end up with both vertical and orthogonal analyses of the extracted data.
- **Documentation Phase:** This phase involves documentation of the executed procedure of the study along with the findings obtained. Another role of this phase is to document and analyze any possible threat to validity that might have an impact on the conducted survey of studies.

A. Research objective and questions

The objective of this survey *is to identify and classify the trustworthiness-related risks, the targeted components of ACPPS, and the type of ACPPS under attack*. The following three research questions (RQs) are designed to tackle the defined research objective of this study:

1) What types of trustworthiness-related risks in ACPPS have been reported?
2) What components of ACPPS have been targeted for studying the effects of trustworthiness-related risks?
3) What use cases have been used to assess the effects of trustworthiness-related risks in ACPPS?

B. Search Strategy

The above research methodology was applied using the search strategy presented in table I. The set of primary studies collected for this survey was obtained using automated search in the stated electronic databases and indexing systems. These databases were selected as a source for primary studies based on their reputation as being the most reliable sources for systematic reviews in the domain of computer science and software engineering [18], [20]. The process of collecting studies began with the formulation of a search string based

TABLE I
ADOPTED SEARCH STRATEGY

Sources of Research Papers	Electronic Databases & Indexing Systems	IEEE Xplore ACM Digital Libraries Scopus Web of Knowledge
Types of Articles	Journal Article Conference Papers Workshop Papers	
Time Period	2010 - January 2023	
Language	English	

on the defined research goal and questions. This search string consisted of three components:

1) Component representing autonomous cyber-physical production: *("Cyber-Physical System" OR CPS) AND ("Manufacturing" OR "Industry 4" OR "Production") AND ("Smart" OR "Artificial Intelligent" OR "Self-Sustain" OR "Autonomous").*
2) Component capturing keywords related to trustworthiness aspects: *("Safety" OR "Security" OR "Trust" OR "Dependability" OR "Resilience" OR "Robust" OR "Self-Heal" OR "Self-Repair").*
3) Component capturing keywords focusing on the evaluation of the studies: *("Analysis" OR "Evaluation").*

We combined the above component and obtained the final search string:
("Cyber-Physical System" OR CPS) AND ("Manufacturing" OR "Industry 4" OR "Production") OR (CPPS OR CPMS) AND ("Smart" OR "Artificial Intelligent" OR "Self-Sustain" OR "Autonomous") AND ("Safety" OR "Security" OR "Trust" OR "Dependability" OR "Resilience" OR "Robust" OR "Self-Heal" OR "Self-Repair") AND ("Analysis" OR "Evaluation")

This search string not only allowed us to identify articles focusing on the implemented attributes of trustworthiness but also highlighted the risks associated with them.

C. Selection criteria

We used a well-designed set of selection criteria to obtain the most relevant set of primary studies [21]. The set of selection criteria composes of the following Inclusion Criteria (IC):

1) The article discusses the trustworthiness-related risks in autonomous cyber-physical production systems.
2) The content of the paper focuses on the affected areas of autonomous cyber-physical production systems when under attack.
3) The selected article is a peer-reviewed conference paper, journal article, or workshop paper.
4) The article is written in the English language.

In addition, the set of selection criteria composes of the following Exclusion Criteria (EC):

1) Articles that discuss the presence of trustworthiness-related risks in autonomous cyber-physical systems as a side-topic.
2) Articles that focus on systems other than autonomous cyber-physical production systems or autonomous cyber-physical manufacturing systems.
3) Articles that do not specify the type of autonomous cyber-physical production system being studied.
4) Articles that present secondary or tertiary studies.
5) Articles presenting only the keynotes of a report, editorial notes, viewpoints, opinions or discussions, tutorials, and slides of a presentation without having associated with any research article, comments, or prefaces.

To be included in the final set of primary studies, an article had to meet all the inclusion criteria and none of the exclusion criteria.

D. Data Extraction

Upon obtaining the final set of primary studies, the next step was to design a data extraction form with the aim to extract the relevant data. This form consisted of three facets each targeting their respective individual research questions (See table II). For each of these research questions, a *keyword-based* systematic process was adopted taking into consideration the characteristics of the selected final set of primary studies [22]. The resultant keywords obtained were further classified based on the process defined as a sorting mechanism for grounded theory methodology [23]. In case of coming across an irrelevant piece of information, the information was reviewed and if deemed necessary to be included was accommodated in the form but only after re-analysis based on the requirements of the updated data-extraction form. Out of *972* articles only *46* articles provided us with the answers to our research questions.

TABLE II
DESIGNED DATA EXTRACTION FORM

Facets	Cluster	Description	Value
RQ1	Trustworthiness - related Risks	Identifies the risks related to trustworthiness in ACPPS	String
RQ2	Effected Areas	Identifies the areas affected by the trustworthiness-related risks	String
RQ3	Use Cases	Identifies use cases used to study the impact of trustworthiness-related risks on ACPPS	String

E. Data Analysis

Based on the guidelines provided by Cruzes et al. [24], data from the data extraction form was collected analyzed, and finally synthesized. As a result, we came across a set of data that was better understood and helped categorize the current state of the art in the domain of trustworthy ACPPS. The outcome of this study is a quantitative analysis of the state of the art in the domain.

F. Threat to Validity

A well-established set of guidelines were followed for the execution of this study [19]. However, there still might exist certain threats to the validity of the results obtained during this study. To help minimize these risks, the following mitigation measures were adopted:

1) Threats to External Validity: The terms CPPS, trustworthiness, autonomy, and evaluation being referred to as using other terminologies can limit the coverage of our results. As a mitigation measure, we expanded our search string incorporating terms alternative to the ones mentioned in the original search string. Considering articles published in multiple languages could also pose a threat to the validity of this study; thus only those articles published in the English language were included in this study.

2) Threats to Internal Validity: A set of well-established guidelines proposed for conducting such studies in the domain of software engineering were followed to avoid coming across any threat related to the internal validity of this study. To further mitigate the threat various sanity checks on the extracted data along with a cross-analysis between the different categories defined in the data extraction form were performed.

3) Threats to Construct Validity: An automatic search was conducted on four different digital libraries and indexing systems to avoid coming across threats to construct validity of having a single source. Furthermore, a closed forward and backward snowballing was performed, followed by having the articles undergo a filtration process using the defined selection criteria.

4) Threats to Conclusion Validity: The systematic procedure adopted for this study was well documented. Well-established taxonomies were used to design the extraction form to collect values emerging from the finalized set of primary studies. All authors were involved in the execution of the defined phases for this study.

IV. Results and Discussion

This section of the paper presents a quantitative analysis of the findings obtained to answer the designed research questions.

A. RQ1 – Types of Trustworthiness-Related Risks in ACCPS

Vulnerabilities in cyber-physical systems can be categorized as either [25]:

- **Network-related vulnerabilities:** that focus on the hardware, monitoring, and configuration-related vulnerabilities.
- **Platform-related vulnerabilities:** involves vulnerabilities in hardware, software, and their configuration.
- **Management-related vulnerabilities:** are entirely based on the lack of implemented security policies.

According to the findings of this study, platform-related vulnerabilities **36.8%** were among the most reported vulnerabilities in ACPPS followed by network-related vulnerabilities **32.8%**, and management-related vulnerabilities **30.2%**.

As platform-related vulnerabilities are also known to arise due to the deficiency of protection measures [25]. Their presence can expose the system to numerous types of cyber-security threats. According to our findings, the presence of such vulnerabilities leading to cyber-security threats was mainly reported to have eventually resulted in risks related to safety, resilience, availability, holistic security, and trust as in holistic trust in ACPPS. Each of these resultant risks has its own effects on the system. Among these, for example, the presence of availability risks has been mostly associated with consequences such as operational disruption, equipment damage, compromise on product quality, violation of safety limits, and environmental pollution. According to Hackäl et al. [26], Chen et al. [39] and Matthias et al. [28], the presence of availability risks also result in various types of cyber attacks ranging from Distributed Denial of Service attacks, Man-in-the-Middle attack, Spoofing, and Data Tempering.

Every component of ACPPS being closely connected to each other via heterogeneous networks result in network-related vulnerabilities [40]. Such complexities in the overall structure of ACPPS are mostly subjected to mismatched configurations thus affecting attributes of trustworthiness such as dependability, safety, holistic security, availability, scalability, reliability, holistic trust, data confidentiality, resilience, fault-tolerance, and self-healing [30]. The consequences associated with such type of vulnerability consisted of loss of information, loss of system or sub-system control, loss of privacy, and other malicious activities resulting in operational disruption.

According to our findings, risks associated with management-related vulnerabilities overlapped the risks associated with network-related vulnerabilities.

B. RQ2 – Affected Components of ACPPS

According to Sara et al., the system can be divided into two main layers, the physical layer and its digital twin residing in the linked cloud [41]. Although the reported risks are said to have an effect mainly on either of these two layers, a deeper investigation leads us to a more specific affected area of ACPPS. The result obtained helped classify articles into three major categories namely articles reporting both cyber and physical layers of ACPPS being affected, articles focusing only on the cyber (architectural layer) of ACPPS being targeted, and lastly articles discussing the effects of trustworthiness-related risks on the physical layer of ACPPS.

Articles discussing the presence of management-related vulnerabilities or platform-related vulnerabilities within ACPPS reported having both the cyber and the physical layers of ACPPS being affected by it such that the entire system or a sub-component of the system could be compromised resulting in operational disruptions.

According to Nour et al. [29], Elias et al. [27], Marian et al. [31], and Bandyszak et al. [32], meeting the constantly evolving demands of the markets requires ACPPS to remain updated. The constant integration of newer components to ACPPS brings about contextual changes to its original architecture i.e. the cyber layer. The introduction of such heterogenous properties in ACPPS thus results in the cyber-layer of ACPPS being vulnerable to cyber-attacks.

Trustworthiness-related risks can affect not only the system as a whole; rather the presence of such unattended risks can also pose a threat to the human in the loop. Thus making such a semi-autonomous cyber-physical production system vulnerable to all types of threats [33].

Management of ACPPS's architecture as a countermeasure to avoid risks in the cyber layer of ACPPS is not enough. Failing to configure every new component being integrated into the original architecture of ACPPS can result in mismatched configuration, cyber-attacks, or other risks affecting specifically the network layer of ACPPS [34], [35], [36].

Lack of resources, limited power, limited computing capabilities of physical components, and other manufacturing vulnerabilities [37] in ACPPS are subjected to risks associated with the trustworthiness attributes such as dependability, reliability, resilience, and availability; thus compromising the physical layer of the ACPPS [38].

Based on the findings of this research question, it can be concluded that very little research has been done on the effects the trustworthiness-related risks can have specifically on the AI aspect of the ACPPS.

C. RQ3 – Use Cases

To study the effects of trustworthiness-related risks in ACPPS, authors opted for behavioral models such as Petri nets and sequence diagrams, structural models e.g., class diagrams and component diagrams, and models specifically designed for risk assessment such as fault trees, attack trees, and Bayesian networks.

Some authors opted to study the system's command processing capabilities using Logical and Functional Layered Architecture Modelling, or the existing data sets available of a particular cyber-physical production system [28].

The authors used a wide range of case studies to observe the consequences of the risks related to trustworthiness in ACPPS. Following are some examples of the use cases used:

1) **Testbeds of Smart Manufacturing Plants:** Water Treatment Testbed - SWaT [42], CNC (Computer Numerical Control)turn-mill machine [34]
2) **Model of Whole ACPPS:** Tennessee-Eastman process control system (TE-PCS) model [43], Intelligent Factory [44]
3) **Component of ACPPS:** industrial robots designed for the transport of goods within the production system [45], Platooning Application [46]
4) **Datasets:** Gas pipeline data set [47], CPS Dataset and UNSW-NB15 dataset of network traffic [29]
5) **Simulated ACPPS:** Simulation of semiconductor production process (Product of ARROWHEAD) [48], Simulation of Artificial "Print & Label" Manufacturing Process [35]

In general, all the use cases used focused mainly on the overall platform-related vulnerabilities, network-related vulnerabilities, or management-related policies. There exists very few studies on systems consisting of a Human-in-the-loop or systems purely focusing on the AI aspects of the ACPPS.

V. Conclusion

The systematic study conducted here presents a summary of recent studies conducted on the risks related to trustworthiness and their consequences within autonomous cyber-physical systems (ACPPS). During this study, a total of 972 articles published over the time period 2010 - January 2023 were identified, analyzed, and classified using a detailed data extraction, analysis, and synthesis process. From this initial set of studies we reached a final set of 46 primary studies yielding the following findings:

1) Platform-related vulnerabilities were among the highest reported type of vulnerabilities in ACPPS, with the majority of risks related to safety, security, resilience, availability, and trust as a whole.
2) Majority of the studies highlighted the cyber layer of ACPPS being the most targeted by the attackers, due to the continuous integration of heterogenous components and misconfiguration among them.
3) A variety of use cases have been used to observe the risks and their consequences in ACPPS. The authors opted to use behavioral models and structural models to develop an understanding of the effects the trustworthiness-related risks can have on ACPPS.

Based on the findings obtained, ACPPS and the implementation of trustworthiness in ACPPS is a relatively new domain. Due to this there is a lack of research on the impact of trustworthiness-related risks on the AI component of ACPPS.

Considering the findings of this study, our next step will be to explore further the possibility of trustworthiness-related risks within the AI component of the autonomous cyber-physical production systems, their impact and how can they be identified and assessed, and mitigated. Furthermore, a model-based framework will be developed to implement the risk management process specifically designed to target the AI component of autonomous cyber-physical production systems.

References

[1] Khan., A. & Turowski., K. A Perspective on Industry 4.0: From Challenges to Opportunities in Production Systems. *Proceedings Of The International Conference On Internet Of Things And Big Data - IoTBD,*. pp. 441-448 (2016)

[2] Berger, S., Bogenreuther, M., Häckel, B. & Niesel, O. Modelling availability risks of IT threats in smart factory networks–a modular Petri net approach. (2019)

[3] Commision, E. What is Industry 5.0?. (2022), https://research-and-innovation.ec.europa.eu/research-area/industry/industry-50_en1/4

[4] Lichte, D. & Wolf, K. Use Case-Based Consideration of Safety and Security in Cyber Physical Production Systems Applied to a Collaborative Robot System. *Safety And Reliability–Safe Societies In A Changing World*. pp. 1395-1401 (2018), https://www.researchgate.net/publication/325654823

[5] Berger, S., Bogenreuther, M., Häckel, B. & Niesel, O. Modelling availability risks of IT threats in smart factory networks–a modular Petri net approach. (2019)

[6] Berger, C., Eichhammer, P., Reiser, H., Domaschka, J., Hauck, F. & Habiger, G. A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms. *ACM Comput. Surv.*. **54** (2021,9), https://doi.org/10.1145/3462513

[7] Commission, E., Communications Networks, C. & Technology Ethics guidelines for trustworthy AI. (Publications Office,2019), doi/10.2759/346720

[8] Japs, S., Anacker, H. & Dumitrescu, R. SAVE: Security & safety by model-based systems engineering on the example of automotive industry. *Procedia CIRP*. **100** pp. 187-192 (2021)

[9] Yu, Z., Zhou, L., Ma, Z. & El-Meligy, M. Trustworthiness modeling and analysis of cyber-physical manufacturing systems. *IEEE Access*. **5** pp. 26076-26085 (2017)

[10] Flammini, F., Alcaraz, C., Bellini, E., Marrone, S., Lopez, J. & Bondavalli, A. Towards Trustworthy Autonomous Systems: Taxonomies and Future Perspectives. *IEEE Transactions On Emerging Topics In Computing*. pp. 1-13 (2022)

[11] Giraldo, J., Sarkar, E., Cardenas, A., Maniatakos, M. & Kantarcioglu, M. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Design & Test*. **34**, 7-17 (2017)

[12] Alcácer, V. & Cruz-Machado, V. Scanning the industry 4.0: A literature review on technologies for manufacturing systems. *Engineering Science And Technology, An International Journal*. **22**, 899-919 (2019)

[13] Agrawal, N. & Kumar, R. Security perspective analysis of industrial cyber physical systems (I-CPS): a decade-wide survey. *ISA Transactions*. **130** pp. 10-24 (2022)

[14] Yaacoub, J., Salman, O., Noura, H., Kaaniche, N., Chehab, A. & Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors And Microsystems*. **77** pp. 103201 (2020)

[15] Geismann, J. & Bodden, E. A systematic literature review of model-driven security engineering for cyber–physical systems. *Journal Of Systems And Software*. **169** pp. 110697 (2020)

[16] Gaiardelli, S., Spellini, S., Lora, M. & Fummi, F. Modeling in Industry 5.0: What Is There and What Is Missing: Special Session 1: Languages for Industry 5.0. *2021 Forum On Specification & Design Languages (FDL)*. pp. 01-08 (2021)

[17] Garousi, V., Felderer, M. & Mäntylä, M. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information And Software Technology*. **106** pp. 101-121 (2019)

[18] Kitchenham, B. & Brereton, P. A systematic review of systematic review process research in software engineering. *Information And Software Technology*. **55**, 2049-2075 (2013)

[19] Wohlin, C. Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. *Proceedings Of The 18th International Conference On Evaluation And Assessment In Software Engineering*. (2014), https://doi.org/10.1145/2601248.2601268

[20] Brereton, P., Kitchenham, B., Budgen, D., Turner, M. & Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *Journal Of Systems And Software*. **80**, 571-583 (2007)

[21] Ali, N. & Petersen, K. Evaluating strategies for study selection in systematic literature studies. *Proceedings Of The 8th ACM/IEEE International Symposium On Empirical Software Engineering And Measurement*. pp. 1-4 (2014)

[22] Petersen, K., Feldt, R., Mujtaba, S. & Mattsson, M. Systematic mapping studies in software engineering. *12th International Conference On Evaluation And Assessment In Software Engineering (EASE) 12*. pp. 1-10 (2008)

[23] Charmaz, K. & Belgrave, L. Grounded theory. The Blackwell encyclopedia of sociology. (Wiley Oxford,2007)

[24] Cruzes, D. & Dyba, T. Recommended steps for thematic synthesis in software engineering. *2011 International Symposium On Empirical Software Engineering And Measurement*. pp. 275-284 (2011)

[25] M.V, R. Cyber Physical System Security Vulnerabilities. (2021,6), https://dev.to/ruthvikraja1_mv/cyber-physical-system-security-vulnerabilities-4bak

[26] Berger, S., Bogenreuther, M., Häckel, B. & Niesel, O. Modelling availability risks of IT threats in smart factory networks–a modular Petri net approach. (2019)

[27] Chen, D., Panfilenko, D., Khabbazi, M. & Sonntag, D. A model-based approach to qualified process automation for anomaly detection and treatment. *2016 IEEE 21st International Conference On Emerging Technologies And Factory Automation (ETFA)*. pp. 1-8 (2016)

[28] Kern, M., Taspolatoglu, E., Scheytt, F., Glock, T., Liu, B., Betancourt, V., Becker, J. & Sax, E. An architecture-based modeling approach using data flows for zone concepts in industry 4.0. *2020 IEEE International Symposium On Systems Engineering (ISSE)*. pp. 1-8 (2020)

[29] Moustafa, N., Adi, E., Turnbull, B. & Hu, J. A new threat intelligence scheme for safeguarding industry 4.0 systems. *IEEE Access*. **6** pp. 32910-32924 (2018)

[30] Balzereit, K. & Niggemann, O. AutoConf: New Algorithm for Reconfiguration of Cyber-Physical Production Systems. *IEEE Transactions On Industrial Informatics*. **19**, 739-749 (2022)

[31] Daun, M., Brings, J., Weyer, T. & Tenbergen, B. Fostering concurrent engineering of cyber-physical systems a proposal for an ontological context framework. *2016 3rd International Workshop On Emerging Ideas And Trends In Engineering Of Cyber-Physical Systems (EITEC)*. pp. 5-10 (2016)

[32] Bandyszak, T., Daun, M., Tenbergen, B. & Weyer, T. Model-based documentation of context uncertainty for cyber-physical systems. *2018 IEEE 14th International Conference On Automation Science And Engineering (CASE)*. pp. 1087-1092 (2018)

[33] Fumagalli, L., Macchi, M., Colace, C., Rondi, M. & Alfieri, A. A smart maintenance tool for a safe electric arc furnace. *IFAC-PapersOnLine*. **49**, 19-24 (2016)

[34] Xin, X., Keoh, S., Sevegnani, M. & Saerbeck, M. Dynamic probabilistic model checking for sensor validation in Industry 4.0 applications. *2020 IEEE International Conference On Smart Internet Of Things (SmartIoT)*. pp. 43-50 (2020)

[35] Preuveneers, D., Joosen, W. & Ilie-Zudor, E. Robust digital twin compositions for industry 4.0 smart manufacturing systems. *2018 IEEE 22nd International Enterprise Distributed Object Computing Workshop (EDOCW)*. pp. 69-78 (2018)

[36] Bou-Harb, E., Kaisar, E. & Austin, M. On the impact of empirical attack models targeting marine transportation. *2017 5th IEEE International Conference On Models And Technologies For Intelligent Transportation Systems (MT-ITS)*. pp. 200-205 (2017)

[37] DeSmit, Z., Elhabashy, A., Wells, L. & Camelio, J. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. *Journal Of Manufacturing Systems*. **43** pp. 339-351 (2017)

[38] Alemayehu, T., Kim, J. & Cho, W. Optimal replacement model for the physical component of safety critical smart-world CPSs. *Journal Of Ambient Intelligence And Humanized Computing*. pp. 1-12 (2021)

[39] Jiang, Y., Atif, Y., Ding, J. & Wang, W. A Semantic Framework with Humans in the Loop for Vulnerability-Assessment in Cyber-Physical Production Systems. *Risks And Security Of Internet And Systems: 14th International Conference, CRiSIS 2019, Hammamet, Tunisia, October 29–31, 2019, Proceedings 14*. pp. 128-143 (2020)

[40] González, C., Varmazyar, M., Nejati, S., Briand, L. & Isasi, Y. Enabling model testing of cyber-physical systems. *Proceedings Of The 21th ACM/IEEE International Conference On Model Driven Engineering Languages And Systems*. pp. 176-186 (2018)

[41] Bazaz, S., Lohtander, M. & Varis, J. 5-dimensional definition for a manufacturing digital twin. *Procedia Manufacturing*. **38** pp. 1705-1712 (2019)

[42] Castellanos, J., Ochoa, M. & Zhou, J. Finding dependencies between cyber-physical domains for security testing of industrial control systems. *Proceedings Of The 34th Annual Computer Security Applications Conference*. pp. 582-594 (2018)

[43] Orojloo, H. & Azgomi, M. A game-theoretic approach to model and quantify the security of cyber-physical systems. *Computers In Industry*. **88** pp. 44-57 (2017)

[44] Wang, G., Li, D. & Song, H. A Formal Analytical Framework for IoT-Based Plug-And Play Manufacturing System Considering Product Life-Cycle Design Cost. *IEEE Transactions On Industrial Informatics*. **19**, 1647-1654 (2022)

[45] Pu, H., He, L., Zhao, C., Yau, D., Cheng, P. & Chen, J. Fingerprinting movements of industrial robots for replay attack detection. *IEEE Transactions On Mobile Computing*. **21**, 3629-3643 (2021)

[46] Japs, S., Anacker, H. & Dumitrescu, R. SAVE: Security & safety by model-based systems engineering on the example of automotive industry. *Procedia CIRP*. **100** pp. 187-192 (2021)

[47] Abdullahi, M., Alhussian, H., Aziz, N., Abdulkadir, S. & Baashar, Y. Deep Learning Model for Cybersecurity Attack Detection in Cyber-Physical Systems. *2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA*. pp. 1-5 (2022)

[48] Ma, Z., Hudic, A., Shaaban, A. & Plosz, S. Security viewpoint in a reference architecture model for cyber-physical production systems. *2017 IEEE European Symposium On Security And Privacy Workshops (EuroS&PW)*. pp. 153-159 (2017)