Dealing with I5.0 complexity: cyber-socio-technical systems modelling and analysis

**Antonio Javier Nakhal Akel*, Francesco Simone*,
Manuel Lombardi*, Francesco Costantino *,
Giulio Di Gravio*, Massimo Tronci*,
Marco Bortolini**, Giovanni Mazzuto***,
Riccardo Patriarca***

** Sapienza University of Rome, 00184 Rome, Italy (antonio.nakhal@uniroma1.it, francesco.simone@uniroma1.it, manuel.lombardi@uniroma1.it, giulio.digravio@uniroma1.it, massimo.tronci@uniroma1.it, riccardo.patriarca@uniroma1.it)*

*** Alma Mater Studiorum University of Bologna, 40136 Bologna, Italy (marco.bortolini3@unibo.it)*

**** Università Politecnica delle Marche, 60131 Ancona, Italy (g.mazzuto@staff.univpm.it)*

Abstract: The transition from Industry 4.0 (I4.0) to Industry 5.0 (I5.0) shifted the focus to novel challenges in industrial systems and their associated operational processes. The focus moved from digitalization towards new applications related to human-machine collaborations, human-centric settings, and cyber-physical cognitive systems. This change stressed the need to identify industrial systems as Cyber-Socio-Technical Systems (CSTS), thus emphasizing the importance of the synergies among cyber-physical technologies, social-human agents, and organizational structures in complex and dynamic contexts. In this context, operations management demands for updates, too, as it must be capable of dealing with such complex modern industrial environment, adopting a CSTS perspective. This latter must integrate relevant entities within the industrial operative context, including the plant equipment, workers and operators, and the surrounding environment, to promote safer and resilient operations. In this context, two main challenges must be addressed: how CSTS' inherent complexity could be modelled and revealed to foster safety and resilience analyses? How could safety and resilience be effectively analyzed in CSTSs applications? This paper addresses the two challenges discussing and presenting methods suitable for CSTSs modelling and analysis, with the intention to foster I5.0 implementation in modern industrial plants.

Keywords: Resilience Engineering; System theory; Knowledge management; Operations management; STAMP

1.Introduction

Over the last decade, the industrial landscape has observed a remarkable shift towards digitalization and connectivity, reflecting the advent of Industry 4.0 (I4.0) and 5.0 (I5.0). This evolution is driven by advanced technologies, such as Internet of Things (IoT), Artificial Intelligence (AI), and grownup computing system, and it has not only enhanced operations but has also introduced a heightened level of complexity. Thus, industrial systems are challenged to deal effectively with this newfound complexity, while nurturing innovation within their processes (Baxter and Sommerville, 2011; Righi and Saurin, 2015). The widespread integration of these advanced technologies into industrial processes has become pervasive, with virtually every competitive organization globally embracing the principles of I4.0. A demonstration of this transformation is evident in the increasing use of Cyber-Physical Systems (CPSs) (Drozdov et al., 2017). These systems comprise interconnected computing and control devices, facilitating seamless interaction with physical infrastructure or organizational frameworks via sensors and actuators. A distinguishing characteristic of CPSs is their ability to preserve continuous engagement with the physical systems they operate within, allowing computation, communication, and control of surrounding physical conditions or environments. Over the past few years, a rapid surge in the use of CPSs has been witnessed, including smart grids, smart factories, Industrial Control Systems (ICS), and automation-robotics (Patriarca et al., 2021). However, the incorporation of advanced technologies, in addition to offering advantages such as improved effectiveness, coordination, and enhanced overall quality, has also led to the novel classification of Cyber-Socio-Technical Systems (CSTSs) (De Nicola et al., 2023). To elucidate this definition, is it noteworthy to mention that: (i) traditional technical systems encompass physical devices, infrastructures, and machines utilized to support human activities; and (ii) socio-technical systems primarily address the symbiotic interactions between physical systems and human agents. Nevertheless, modern technical systems are defined by both cyber and physical parts. The cyber part encompasses software systems, which continuously exhibit growing autonomy and intelligence, while the physical part includes traditional technical systems, hardware infrastructures, and contemporary physical devices such as sensors and actuators, intended to collaborate with their cyber counterpart. In this paper, the concept of CSTS is used to highlight that the analysis involves those systems that deal with cyber artifacts, physical devices, and human agents together. The CSTSs underscore the intricate interplay among cyber-technical systems, humans, and organizations, acknowledging the synergies that evolve over time within these systems and the interactions among system elements into the process (Falegnami et al., 2024). However, CSTSs also introduce a whole new set of disruption scenarios with potentially disastrous impact (Hollnagel, 2012). Achieving secure and safer systems, typically pursued through risk mitigation in the forms of prevention and protection, becomes a novel challenge when dealing with CSTSs. While traditional strategies are crucial in averting extremely negative consequences, recent advancements in safety and security management indicate that not all undesired events can be entirely prevented or effectively controlled (Leveson, 2011). With the industrial landscape embracing the benefits of I4.0, and especially of I5.0, alongside the seamless integration of CPSs into operational frameworks, a parallel reality emerges, charged with security issues (Banks and Stanton, 2019; Colabianchi et al., 2023).

This paper aims to shed light on the evolution and applications of CPSs, considering them in the broader perspective of CSTS, thus accounting for their socio-technical nature, and for the critical imperative for cybersecurity measures. Within this context, cybersecurity transcends conventional data or information hacking, extending its reach to potential modifications of physical processes, thus prompting concerns about tangible damage, losses, and breakages with impact on the plant itself. The objective of this paper is to examine and address these challenges, offering insights on the delicate balance needed to secure the future of industrial systems in the I5.0 era. Accordingly, to fulfill this objective, a scoping literature review, and, subsequently, a bibliometric analysis on papers have been conducted. Thus, this paper aims to answer the following research questions: *Which modelling techniques are being employed to incorporate socio-technical elements in system models when dealing with CPSs embedded in industrial CSTSs? How do these techniques are being used to enhance safety and security of industrial CSTSs?*

The remainder of the paper is organized as follows: **Section 2** provides the systematic methodology used to review the literature in this regard. **Section 3** presents the results of the methodology being introduced; specifically, the three main approaches emerged from a review of current literature (i.e., control theory modeling, resilience engineering modelling, and information flow modelling) are covered in this section. Eventually, **Section 4** contains the conclusions to this work and a discussion on how future research may investigate modern industrial plants management.

2. Research methodology

The framework Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (David Moher et al., 2009) has been selected as a systematic technique for reviewing literature. In this context, PRISMA ensures transparency and completeness in reporting reviews, enhancing the reliability and usability of the research.

2.1 PRISMA steps

In this research, the methodological approach, consisting of 4 steps, was supported by a structured review framework implemented via dedicated spreadsheets.

2.1.1 STEP 1: identification

The first step of the review was to identify the database and define the search query. The chosen source was Scopus, as it is considered the main repository for engineering and management manuscripts. Then, the query has been structured translating the research question as it follows:

"TITLE-ABS-KEY ("cyber" AND "model*" AND ("socio* technical" OR "*man*machine")".

The search returned 183 documents.

2.1.2 STEP 2: screening

During the screening process, 106 documents (ca. 58% of the 183 documents) have been considered out of scope, being not compliant with the inclusion criteria summarized in Table 1.

Table 1: Inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Language	English	Other than English
Type	Journal articles or conference proceedings	Books, book series, editorials, errata, industrial reports, theses
Scope	Research and empirical work on socio-technical modelling in CSTSs	No focus on any modelling aspect for CSTSs
Document availability	Full-text available	Full-text not available

Table 2 describes the types of excluded documents, and the reason for their exclusion. Since the scoping review proposed here aims to investigate empirical research, 13 documents have been excluded being literature reviews. Moreover, 20 additional papers were summaries of conference proceedings. A set of 52 documents have been excluded since considered out of scope by reading the title, the abstract, and the keywords. Specifically, these papers focused on one of the following themes: organizational modelling, siloed cognitive modelling, circular economy and sustainability applications, terrorists attack through social networks data, competence engineering analysis, humanoids application, augmented reality simulations, cyber-crime and digital forensic, computer science application (e.g., software developing, security policies, and computer modelling), agriculture applications, and maturity models analyses. Finally, 21 documents have been excluded from the analysis on the grounds that they are not written in English or fall into any of the following categories: books, book series, editorials, industrial reports, or academic theses.

Table 2: Number of documents excluded in the analysis.

Motivation of exclusion	Number of documents	Percentage of documents
Out of scope	52	49,05 %
Document type and language	21	19,81 %
Summaries of conference proceedings	20	18,86 %
Literature reviews	13	12,26 %

Overall, this screening process led to the inclusion of 77 documents (ca. 42%) in the next step of the analysis.

2.1.3 STEP 3: eligibility

This round of review allowed the refinement of the sample of papers, eliminating articles that offered different interpretations of CSTSs, or were not in line with the purpose of the search: (i) 8 documents show discrepancy between the title, abstract, and keywords and the full-text, and (ii) other 12 papers were not available in full-text in any database accessible by the pool of authors. The result of this process resulted in 57 papers to be proposed in the next stages of the analysis. Please note that the results of the review have been described electively in a narrative format, but the database containing all the analyzed documents is available upon reasonable request.

2.1.4 STEP 4: inclusion and analysis

The last step of the PRISMA methodology involves detailed full-text analysis of pre-selected documents. This detailed reading was instrumental for the development of a structured spreadsheet to allow parametric analyses, as the ones exemplified in Section 3.

3. Analysis of documents and results

This section details the results from the analysis of literature. Starting with a general overview (paragraph 3.1), complemented by a domain-based analysis (paragraph 3.2), the first two paragraphs include selected descriptive findings. The analysis concludes with a brief examination of the documents related to each of the identified approaches, apt to understand in what sphere and how these methodologies are applied (paragraph 3.3).

3.1. General overview

From the full-text reading of the selected contributions, three major streams of research emerged:

- *Resilience engineering modelling*: some research manuscripts focus on the study of the CSTS adaptive capacities. They pinpoint that the main goal of the CSTS is to preserve an acceptable performance despite the adverse scenarios that may verify, embracing the resilience perspective that it is important to evaluate the ability of the system to withstand, to adapt and to recover from any unexpected event. Normal operations and related performance investigations represent the central point of these types of modelling approaches.
- *Control theory modelling*: approaches relying on modelling the CSTS adopting a control theory-inspired perspective. As such, agents within the system are studied pointing at how agents decide to modify the operations of others, and what data agents communicate to make these decisions possible. Safety and operations are here considered a control problem, i.e., control actions not performed as expected, or as planned.
- *Information flow modelling*: approaches focusing on the information exchanges within the CSTS. These models distinguish the stages within the process to then describe how information flows through the system, among the system agents. These modelling approaches characterize the kinds of data that flow through the process, capturing how and who could access them.

This general overview on the adopted modelling approaches (i.e., resilience engineering modelling, control theory modelling, and information flow modelling), enables the representation of the distribution of publications. Table 3 shows the number of documents retrieved after the screening, divided by modelling approach. In which, ca. 54% of the papers are related to control theory modelling (31 documents out of 57), the remaining are almost equally distributed between resilience engineering modelling (ca. 24%; 14 documents out of 57) and information flow modelling (ca. 21%; 12 documents out of 57).

Table 3: Document distribution by modelling approach

Modelling approach	Number of documents
Control theory	31
Resilience engineering	14
Information flow	12

A further analysis has been done with respect to the type of system being analyzed, namely: technical physical system, technical cyber system, and social system, and all the combination of them, i.e., cyber-physical system, socio-technical system, and cyber-socio-technical system. For instance, ca. 47% present investigation of a CPS (27 documents of 57); 39% of the articles focus on larger CSTSs (22 documents of 57), and the remaining documents, representing the 14% of the sample, split among some other occurrences as shown in Table 4.

Table 4: Distribution of the documents by system type

Type of system being modelled	Number of documents
Cyber-physical	27
Cyber-socio-technical	22
Socio-technical	6
Technical cyber	1
Social	1

3.2. Domain of application

Regarding the context in which each paper focuses its investigation, Table 5 reports documents by their domain of application. In addition, the number of documents has been detailed by modelling approach, too.

Table 5: Number of papers by domain of application and modelling approach

Domain of application	Number of documents		
	Control theory	Information flow	Resilience engineering
Industrial ops	13	5	7
IT	5	2	2
Automotive	3	1	2
Road	2	1	0
Railway	1	0	1
Healthcare	1	0	0
Finance	1	0	0
Aviation	1	0	0
Others	4	3	2

3.3. Application of approaches

To summarize the results of the literature review, the following sections describe the most relevant documents highlighting how they fit in the scope of this review, in terms of methodologies, domain, and system type that have been crucial to the investigation.

3.3.1 Excerpt of documents related to resilience engineering modelling

This section is intended to give an understanding of how resilience engineering modelling techniques are used. For brevity, only main articles are presented. They limited to the “Industrial operations” and “Aviation” domain of application. The former being the most coherent domain for I5.0, the latter being selected for the level of innovation being presented. Related to the “Industrial operations” domain of application, for instance, Häring I. et al. (2017) delve into a comprehensive resilience framework and management process that transcends generic risk management and functional safety standards. The proposed framework covers CSTSs, non-linear system behaviors, and various dimensions of security. The work contributes to the development of credible certification for critical infrastructure and safety-critical systems. De Nicola et al. (2023) proposes the concept of allostatic load, which is a measure that considers the repeated adaptation to stressors, to assess complex systems’ resilience. The methodology involves the use of semantic technologies, the Functional Resonance Analysis Method (FRAM), the WAx conceptual framework, and a crowd-based approach to elicit industrial knowledge. The authors validate their approach with two real case studies. In the “Aviation” domain of application, instead, the work of Köpke, C. et al. (2020) is noteworthy for the scope of this analysis. The researchers in this paper delve into airport security, focusing on vulnerabilities to combined cyber-physical threats in the context of the EU-H2020 project SATIE. Employing agent-based modeling, the obtained simulation tool represents not only technical aspects but also the social dimension of airport systems, particularly passenger interactions. The paper acknowledges the tool's current limitations, emphasizing its potential for improved threat analysis and mitigation in airport security.

3.3.2 Excerpt of documents related to control theory modelling

Similarly to the previous one, this section is intended to give an understanding of how control theory engineering modelling techniques are used. Also in this case, for brevity reasons, only the main articles are presented. They are limited to the “Industrial operations” and “IT” domain of application, being IT noteworthy for its advanced level of developments. Related to the “Industrial operations” domain of application, Nguyen (2019) states that the complex systems require collaboration across various disciplines and stakeholders throughout their lifetimes. They developed the Formal Requirements Modelling Language (FORM-L) to address dynamic phenomena in system engineering. FORM-L supports a range of activities, including scoping studies, requirements elicitation, design, optimization, and testing. While the language and methodology are well-defined, tool development is ongoing to enhance support for these activities. Furthermore, Egor (2020) in his article explores the I4.0, emphasizing the need to shift focus from technical aspects to managerial aspects in the context of digitalization within manufacturing companies. It highlights that digitalization involves integrating processes, including production, logistics, and personnel, with a strong connection between the physical and virtual environments through information and communication technologies. The evolving technologies in digital transformation are crucial for ensuring a company success and future readiness. Related to the “IT” domain of application, instead, (Hariharan et al., 2023) studied the impact of a cyber-attack on customers' perceptions in the context of an e-commerce platform by aligning the so-called STRIDE threat modeling with the Confidentiality, Integrity, and Availability (CIA) cybersecurity requirements. Findings indicate that confidentiality compromise has the highest negative impact, with 82% of respondents expressing perceived privacy risks due to a cyber-attack. The study emphasizes the importance of robust cybersecurity measures, transparent communication, customer education, and prompt response during cyber-attacks to build and maintain trust in the evolving digital economy.

3.3.3 Excerpt of documents related to information flow modelling

Analogously to previous sections, here the intention is to give an understanding of how the information flow modelling techniques are used. For brevity, the most important papers in the “Industrial operations” and “IT” domains are presented. Regarding the former, Gronau N. (2021) addresses the need for an analysis and design method for knowledge management that integrates human and machine interactions in the I4.0. It introduces KMDL3.0, an extended modeling language, as a tool to represent, analyze, and optimize knowledge processing with a focus on artificial intelligence and machine learning in both office and production environments. Instead Charitoudi K. and Blyth A. J. C. (2014) introduced a novel simulation method for estimating the impact of cyber-attacks, addressing limitations in existing approaches that often focus on individual levels such as assets or business processes. The proposed interdependency impact assessment approach emphasizes the dynamic relationships and dependencies within a supply chain, employing an agent-based socio-technical model. The model aims to enhance situational awareness for cyber defense, particularly focusing on critical information infrastructures. Cadzow, A. (2019), the authors delve into the Socio-Technical Environment of online Sextortion in the Digital Society. The paper recommends a holistic planning approach, the development of a cyber deterrence strategy by law enforcement, enhanced recording and auditing of digital evidence, expanded use of IP blocking, increased collaboration between stakeholders for cybersecurity education, and the development of software and AI tools by technology companies to proactively identify false profiles.

3.3.4 Concluding remarks on the review

The review revealed insights and limitations associated with the different types of CSTSs modeling. In the domain of resilience engineering modeling, the objective is to map the CSTS's ability to adapt and maintain their performance even in adverse scenarios. However, these models may fall short in capturing the full range of adaptive responses due to the inherent complexity of the systems under consideration. On the other hand, the control theory modeling focuses on how agents modify each operation and communicate data for decision-making. Yet, these models rely on assumptions about agent behavior and communication, and their effectiveness hinges on data quality during analysis. In contrast, the information flow modeling explains how information moves through the system at each stage. These models characterize data accessibility and identify who can retrieve it. However, they may oversimplify complex interactions by focusing on static information flow rather than dynamic system behavior. Nevertheless, a main trend in using control theory modelling approaches have been highlighted in the literature review. As such, it was decided to conduct an additional literature search on control theory modelling to highlight the most significant studies on system-theoretic modelling.

3.3.5 System theory modeling

The previous analysis revealed a large quantity of documents utilizing control theory modelling to investigate CSTSs. Consequently, it was deemed crucial to restrict the search to this domain of analysis. In particular, among control theory modelling techniques, the ones based on system theory (i.e., System-Theoretic Accident Model and Processes (STAMP) and associated techniques) were shown to be the most adopted. Such trend was confirmed also by the recent literature review on STAMP conducted by Patriarca et al. (2022). Therefore, an additional literature review was intended to analyze the contribution of system theory in CSTSs modelling in the period 2020 – 2024. Following the PRISMA methodology, and applying the same criteria as for Section 2, a total of 24 documents were obtained. The query used to obtain these papers was formalized as it follows:

"TITLE-ABS-KEY ("cyber" AND ("system* theor* accident model* process*" OR "system* theor* accident model* and process*" OR "system* theor* process analysis" OR "system* theor* process and analysis" OR ("causal analysis" AND "system* theor*")) OR "STAMP analysis") AND PUBYEAR > 2020 AND PUBYEAR < 2025"

Applying the different screening phases, the review resulted in 10 articles that were considered relevant for further analysis. These relevant articles cover various domains of application, as illustrated in Table 6. For brevity reasons, only 4 out of the 10 papers in Table 6 are detailed in the following lines. They were elected for the novelty and potential impact of obtained results with respect to CSTSs safety.

Khan and Madnick (2022) focused their attention on the cyber-attacks vulnerabilities of critical infrastructures. Their work uses the electrical generation and distribution system of an archetypal industrial facility to demonstrate the application of a STAMP-based method to identify and mitigate cyber-vulnerabilities in ICSs. The key contribution of this work is to differentiate the additional steps required to perform a holistic cybersecurity analysis for an ICS of significant size and complexity, and to present the analysis in a structured format that can be emulated for larger systems. On a similar path, Simone et al. (2023) updated the STPA-Sec (i.e., System-Theoretic Process Analysis for Security) technique presenting STPA-Sec/S which enhanced the control theory modelling approach with a quantification step based on simulation. The approach was tested on a water treatment plant targeted by various cyber-attacks showing its effectiveness in supporting decision makers in identifying the most critical scenarios. On a different stream of research, Lee and Madnick (2021) focused their attention on urban mobility. Specifically, due to the increased level of automation and connectivity in the new generation of autonomous vehicles, cybersecurity is emerging as a key threat affecting this sector. Since traditional hazard analysis methods are limited in their ability to account for interactions among organizational, sociotechnical, human and technical components, in this paper the cybersafety method, based on STPA (i.e., System-Theoretic Process Analysis) was developed to meet the growing need to holistically analyze complex socio-technical systems.

Table 6: Number of system-theoretic papers (a subset of paper on control theory), by domain of application.

Domain of application	Number of documents
Industrial operations	4
Automotive	3
Maritime (Others)	2
IT	1

The results are then compared with another promising method known as Combined Harm Analysis of Safety and Security for Information Systems (CHASSIS) and both methods were applied to the mobility-as-a-service and internet-of-vehicles use cases. In particular, cybersafety demonstrated the ability to identify hazards due to unsafe/unsecure interactions among sociotechnical components. As a different approach, Zacharaki et al. (2021) examine the widespread use of collaborative robots in industry to assist humans in manufacturing tasks. While these robots are designed to be safe, the integration of external sensors and CPSs for close cooperation with humans can introduce new safety risks and hazards. Therefore, the authors propose a method that utilizes Partially Observable Markov Decision Processes (POMDP) to combine nominal system actions with Unsafe Control Actions (UCAs) identified through STPA. The work contributes to creating a decision-making tool based on STPA hazard analysis and Markov decision processes. This tool serves as a hazard assessment monitoring tool during the operational phase, actively triggering the system to choose actions that enhance safety. The integration of STPA outcomes into a POMDP model offsets for uncertainties arising from sensor measurements and human behavior errors. Eventually, in the authors developed an integrative approach to in-time hazard detection that incorporates system-level analysis into the design of runtime monitoring architectures. Integrative approaches to runtime monitoring for hazard detection in CPS are needed to augment the technical basis for DepDevOps style methods. They demonstrated that the systematic nature of STPA is useful in deriving and refining multilevel monitoring properties related to causal factors. By developing monitors across multiple system levels, it was possible to accurately detect the origin of a hazard even when it propagates errors across different CSTS levels. In other words, when faults go undetected at their original location, monitors at other system levels can detect propagated errors, thus increasing hazard detection coverage. The authors also found that the Model Based Design and Engineering (MBDE) methods and tools significantly improve the productivity of STPA and assist in evaluating runtime monitoring schemes for hazard coverage and refinement.

4. Conclusions

The approaches to model CSTS in complex and dynamic scenarios have been illustrated in this paper, providing insights into the changing landscape of industrial operations and the challenges of joint safety and security management for operations management. The emergence of I4.0 and I5.0 paradigms has fostered the integration of advanced technologies improving their efficiency and functionality. However, this integration brought new complexities that have been acknowledged by the concept of CSTS. While traditional approaches to security and risk management have historically focused on prevention and protection strategies, the evolving nature of modern industrial systems requires a shift in thinking toward resilience modeling, control theory modeling, and information flow modeling. It is worth noting that this literature review has laid the foundation for further research and exploration in the field of CSTS modeling, providing a comprehensive overview of the current state of knowledge. This paper aims to represent a resource to advance the understanding of CSTS modeling in industry and inform strategies to ensure the future of industrial systems in an increasingly interconnected and dynamic environment. Accordingly, the knowledge in this review comprehends a view of possible approaches to deal with CSTSs complexity. In other words, this research provides some models and insights to map and examine modern CSTSs. Based on the observed results, control theory modeling appears the most widely used modeling approach. It can be inferred how control theory is considered able to model the interactions among humans and technical artifacts, both physical and computerized, approaching traditional automation control and, to some extent, transferable to human-machine or human-human control loops. Among control theory models, system theory approaches have proven effective in dealing with complex CSTS. As such, this paper concludes that systems theory is a suitable candidate to base future operations management in being more effective and efficient when acknowledging cyber-physical threats and faults.

Acknowledgement

This work has been funded by the European Union - NextGenerationEU under the National Recovery and Resilience Plan (PNRR) – Mission 4 Education and Research – Component 2 From research to business - Investment 1.1, PRIN 2022 Notice announced with DD No. 104 of 2/2/2022, entitled RESIST - RESilience management to Industrial Systems Threats, proposal code 2022YSAE2X, CUP: B53D23006650006.

This work is also part of the research activities developed by the author Manuel Lombardi, within the framework of PNRR: PhD in Industrial and Management Engineering - CUP B53C23002500006.

References

Banks VA and Stanton NA (2019) Analysis of driver roles: modelling the changing role of the driver in automated driving systems using EAST. Theoretical Issues in Ergonomics Science 20(3): 284–300.

Baxter G and Sommerville I (2011) Socio-technical systems: From design methods to systems engineering. Interacting with Computers 23(1): 4–17.

Cadzow, A. (2019) The Analysis of the Socio-Technical Environment (STE) of Online Sextortion Using Case Studies and Published Reports from a Cybersecurity Perspective. Advances in Intelligent Systems and Computing, 998, 817–833.

Charitoudi K. and Blyth A. J. C. (2014) An Agent-Based Socio-Technical Approach to Impact Assessment for Cyber Defense. Information Security Journal, 23, 125–136.

Colabianchi S, Tedeschi A and Costantino F (2023) Human-technology integration with industrial conversational agents: A conceptual architecture and a taxonomy for manufacturing. Journal of Industrial Information Integration 35: 100510.

David Moher, Alessandro Liberati, Jennifer Tetzlaff, et al. (2009) Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement.

De Nicola A, Villani ML, Sujan M, et al. (2023) Development and measurement of a resilience indicator for cyber-socio-technical systems: The allostatic load. Journal of Industrial Information Integration 35: 100489.

Drozdov D, Patil S, Dubinin V, et al. (2017) Towards formal verification for cyber-physically agnostic software: A case study. In: IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, October 2017, pp. 5509–5514. IEEE. Available at: http://ieeexplore.ieee.org/document/8216953/ (accessed 27 April 2024).

Egor P (2020) Digital Transformation of Industrial Companies: What is Management 4.0? In: 2020 The 11th International Conference on E-business, Management and Economics, Beijing China, 15 July 2020, pp. 131–138. ACM.

Falegnami A, Tomassi A, Corbelli G, et al. (2024) Managing Complexity in Socio-Technical Systems by Mimicking Emergent Simplicities in Nature: A Brief Communication. Biomimetics 9(6): 322.

Gronau N. (2021) Modeling the Handling of Knowledge for Industry 4.0. Lecture Notes in Business Information Processing, 422 LNBIP, 207–223.

Hariharan J, Sheik AT, Maple C, et al. (2023) Customers' perception of cybersecurity risks in E-commerce websites. In: International Conference on AI and the Digital Economy (CADE 2023), 2023, pp. 53–60.

Häring I., Sansavini G., Bellini E., et al. (2017) Towards a generic resilience management, quantification and development process: General definitions, requirements, methods, techniques and measures, and case studies. In NATO Science for Peace and Security Series C: Environmental Security (Vol. PartF1, pp. 21–80).

Hollnagel E (2012) Coping with complexity: past, present and future. Cognition, Technology & Work 14(3): 199–205.

Khan S and Madnick S (2022) Cybersafety: A System-Theoretic Approach to Identify Cyber-Vulnerabilities & Mitigation Requirements in Industrial Control Systems. IEEE Transactions on Dependable and Secure Computing 19(5): 3312–3328.

Köpke, C., König L., Faist K., et al. (2020) Security and Resilience for Airport Infrastructure.

Lee CW and Madnick S (2021) Cybersafety Approach to Cybersecurity Analysis and Mitigation for Mobility-as-a-Service and Internet of Vehicles. Electronics 10(10): 1220.

Leveson NG (2011) Applying systems thinking to analyze and learn from events. Safety Science 49(1): 55–64.

Nguyen T (2019) Formal Requirements and Constraints Modelling in FORM-L for the Engineering of Complex Socio-Technical Systems. In: 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), Jeju Island, Korea (South), September 2019, pp. 123–132. IEEE. Available at: https://ieeexplore.ieee.org/document/8933573/ (accessed 27 April 2024).

Patriarca R, Falegnami A, Costantino F, et al. (2021) WAx: An integrated conceptual framework for the analysis of cyber-socio-technical systems. Safety Science 136: 105142.

Patriarca R, Chatzimichailidou M, Karanikas N, et al. (2022) The past and present of System-Theoretic Accident Model And Processes (STAMP) and its associated techniques: A scoping review. Safety Science 146: 105566.

Righi AW and Saurin TA (2015) Complex socio-technical systems: Characterization and management guidelines. Applied Ergonomics 50: 19–30.

Simone F, Akel AJN, Gravio GD, et al. (2023) Thinking in Systems, Sifting Through Simulations: A Way Ahead for Cyber Resilience Assessment. IEEE Access 11: 11430–11450.

Zacharaki A, Kostavelis I and Dokas I (2021) Decision Making with STPA through Markov Decision Process, a Theoretic Framework for Safe Human-Robot Collaboration. Applied Sciences 11(11): 5212.