SN Computer Science (2023) 4:825
https://doi.org/10.1007/s42979-023-02268-0

ORIGINAL RESEARCH

A Review and Analysis of the Characteristics of Cyber-physical Systems in Industry 4.0

Yasamin Eslami[1] · Chiara Franciosi[2] · Sahand Ashouri[3] · Mario Lezoche[2]

Received: 18 April 2023 / Accepted: 22 August 2023

Abstract

Industry 4.0 (I4.0) creates more efficient production processes by providing an interconnected environment between man and machine. Cyber-physical systems (CPS) are one of the many technologies that enable I4.0 by building a bridge between the physical and the virtual objects in production systems. Nonetheless, CPSs are dealing with a complex system with various emergent behaviours. CPS must be defined by features and characteristics that can adapt to the changes in real-time and derive knowledge through the gathered abundant information it receives. In this respect, this study focuses on an analysis and a review of CPS and its characteristics to explore the essence of knowledge representation in CPS metamodels. This study aims to answer the following research questions: how are CPS metamodels described and characterized? How is Knowledge represented in CPS metamodels? To respond to the research questions and achieve the purpose of this study, first a literature review was conducted to identify relevant papers, then Formal Concept Analysis (FCA) as a clustering technique is used to make a more thorough investigation of the topic, to analyse CPS characteristics, and to discover any hidden relationship between them. The analysis conducted led to an understanding of CPS's characteristics and the discovery of any hidden relationship among them. Among all characteristics (e.g., safety, fault-tolerant, redundancy), "resiliency" was the most frequent characteristic. Consequently, with the help of the hidden bonds found by FCA among the most frequent and the most observed characteristics, a hierarchy of highly ranked CPS characteristics as a road map to reach "resiliency" is proposed. The paper presented a review and an analysis of Cyber-physical systems and their representative characteristics. A new set of definitions for the highly ranked characteristics is also introduced. The proposed definitions can help the future CPS metamodel designs so that they take a path more aligned with the concept of Industry 4.0.

Keywords Cyber-physical systems · Meta-models · Industry 4.0 · Formal concept analysis

Introduction

Cyber-physical systems (CPS) represent more than networking and information technology: information and knowledge are integrated into physical objects. By integrating perception, communication, learning, behaviour generation, and reasoning into such systems, a new generation of intelligent and autonomous systems are to be developed.

A large-scale CPS can be envisioned as millions of networked, smart devices, sensors, and actuators being embedded in the physical world, which can sense, process, and communicate the data all over the network. The proliferation of technology-mediated social interactions via these highly featured and networked smart devices has allowed many individuals to contribute to the size of the Big Data available. The data generated by CPSs are contextualised, which helps transform data into information. This makes CPSs,

This article is part of the topical collection "Innovative Intelligent Industrial Production and Logistics 2022" guest edited by Alexander Smirnov, Kurosh Madani, Hervé Panetto and Georg Weichhart.

✉ Yasamin Eslami
yasamin.eslami@ec-nantes.fr

Chiara Franciosi
chiara.franciosi@univ-lorraine.fr

Sahand Ashouri
sahand.ashouri.68@gmail.com

Mario Lezoche
mario.lezoche@univ-lorraine.fr

[1] Ecole Centrale de Nantes, LS2N, 44300 Nantes, France

[2] Université de Lorraine, CNRS, CRAN, 54000 Nancy, France

[3] Independent Researcher, Milan, Italy

Published online: 28 October 2023

in the context of Industry 4.0, a huge source of information that includes, often implicitly, relationships about the environment and the working domain. This information and relationships are a potential source of knowledge that needs to be extracted, formalised and, potentially, reused. To be able to implement this knowledge extraction, it is necessary to study in depth the characteristics that the systems under examination must and can have to characterize the methods according to their potential. To this point, this study, completes the work of the same authors [1] on CPS characteristics and their frequency of appearance in literature to detect trends and gather the current opinion of researchers regarding CPS characteristics. Consequently, this work focuses on the various meta-models presented in the literature to extract the most-studied characteristics while presenting a metamodel that can satisfy all modelling needs.

The work is structured as follows: (a) the following section describes the adopted methodology in detail; (b) previous surveys in the context of CPS metamodels are examined in "Previous studies on CPS metamodels and their applications in real world"; (c) a descriptive background on formal concept analysis (FCA) will be presented in "Background" together with a discussion on the CPS characteristics; (d) "Clustering assessment on characteristics using the formal concept analysis method" presents an analysis of the characteristics through the help of FCA, which enabled the clustering of the inspected CPS characteristics; (f) The subsequent section presents the discussion on the results of the analysis; (g) finally, the conclusion and future works are presented in "Conclusions".

Methodology

The methodology of this study has two main sections. It starts with a state-of-the-art based on cyber-physical systems metamodels, and the CPS characteristics represented in the scientific papers. Then, a formal concept analysis (FCA) will run on the results of the state of the art to reveal and discover any hidden relationship among the characteristics.

The focus of the state-of-the-art was based on CPS knowledge representation in different scientific papers. To do so, a sequence of questions have been answered throughout the work:

- RQ (1) 'How CPS metamodels are described and characterized?'
- RQ (2) 'How is Knowledge represented in CPS metamodels?'

Consequently, papers were identified through a structured keyword search on major databases and publisher websites (Scopus, Elsevier and ScienceDirect). The research statement was set by using the keywords "Cyber (-) Physical system" AND ("Metamodel" OR "Meta-model") to have the first pool of the articles. All the searches were applied in the "Title, Keyword, Abstract" field.

As the first step, articles were categorised as included and excluded. In this step, the articles abstract, title and keyword were screened, and they were decided to be included or excluded from the study based on the exclusion criteria (EC) below:

- EC(1): entire conference proceedings
- EC(2): articles that do not develop a (meta) model of CPS
- EC(3): articles that do not represent or study a CPS characteristic

In the second step, a content analysis was conducted, in which the full text of the included articles was read. In this phase articles were excluded based on the following exclusion criteria:

- EC(4): non-English articles
- EC(5): articles whose full-texts were not available.

A systematic analysis was run to assess the included articles in terms of what CPS characteristics are discussed explicitly or implicitly. Consequently, a snowball analysis was done through reference scanning of the included articles to identify articles with CPS characteristics discussed. A schematic view of the literature review is shown in Fig. 1.

Previous Studies on CPS Metamodels and Their Applications in Real World

CPSs have been widely discussed in the literature [2] thoroughly discusses the characteristics and architecture of CPS and then investigates different research on the information processing of CPS, CPS Software Systems, CPS System Security and CPS System Testbed. Studying all, they conclude that the biggest challenge in the development of CPS is the limitation on existing theory and technology of computation, communications, and control technology. After an investigation of the structure of CPS, [3] makes a comprehensive search of different domain applications of CPS such as handling energy, network security and data transmission and management. Afterwards, they briefly explored the models and methods driven for the development of CPSs, domain-specific modelling (DSM), prominent model-driven development (MDD) and model-integrated computing are a few to mention. Adversely, the importance of smart healthcare cyber-physical systems (SHCPS) is discussed in [4] as the COVID-pandemic in 2020 has shown the urge for

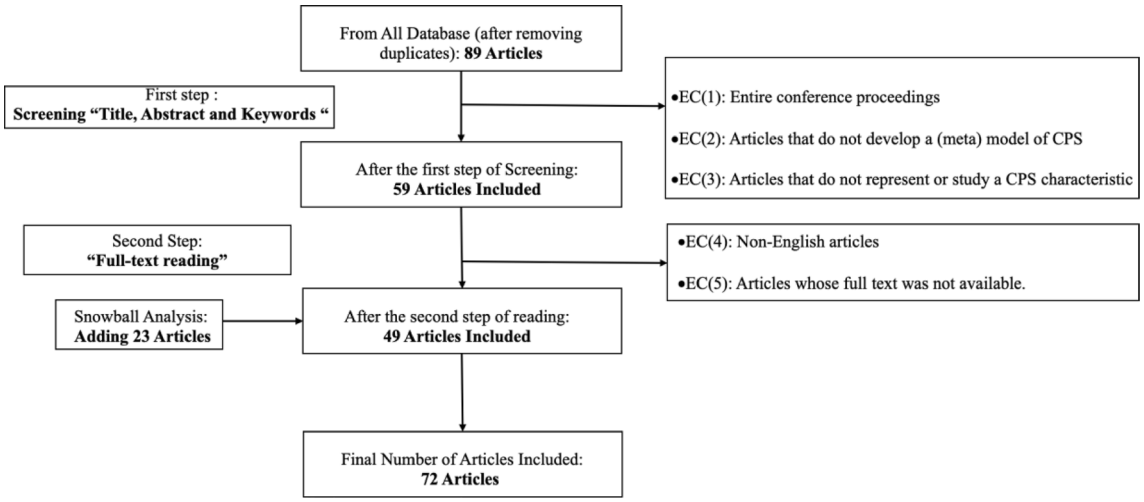

Fig. 1 Literature review process

continuous communication and information exchange of physiological data through efficient external monitoring and control of patients and medical equipment. They have defined five different levels of healthcare cyber-physical systems: (1) Unit level, which is the basic level for HCPS that can provide monitoring and control for patients in intensive care units or at the hospital level; (2) integration level, which integrates hospital and smart homes to provide remote healthcare and monitoring to the patients; (3) system level, which forms a smart city healthcare by CPS through several autonomous CPSs. It creates a smart grid with smart homes, smart hospital, smart ambulance and even smart manufacturing units to provide a smart quality healthcare system to patients; (4) acceptance level, where coordinates different researchers, technologists, engineers, health experts, academicians to help define effective policies and implement a successful ecosystem; and (5) evolutionary level, with self-adaptability and self-management characteristics that can learn from the past data in the healthcare system and behave in current scenarios. In general, due to the structure of the SHCPS, characteristics like level of autonomy, security and reliability are discussed since they construct the backbone of the healthcare systems and are desired by the CPS structure. In another work, cyber-physical Production Systems (CPPS), their design and application are the focal point of the study ran by [5]. The 5C architecture of CPS (Smart Connection Level, Data-to-Information Conversion Level, Cyber Level, Cognition Level and Configuration Level) is also deeply discussed regarding the CPPS. Considering CPPS again, [6] presents a metamodel-based CPPS trying to integrate information from different software into comprehensive models of CPPS. The integration benefits from flexible interoperability alignments among networks. The created integration inside the networks consequently effectuates collaboration of production systems avoiding time-consuming and deadlock-prone semantic standardization efforts.

On the other hand, [7] categorizes the application domain of CPS into 10 main categories and discusses the work done in each category. Agriculture, education, energy management, environmental monitoring, medical devices and systems, process control, security, smart city and smart home, smart manufacturing and transportation systems are the 10 groups CPSs discussed in the mentioned work. To name a few of the many examples, they mention the work of [8] through which a "Rat Detection system" (RDS) was developed to help monitor rats in the agriculture field. This CPS-based system reduces the costs of rat control, crop waste and environmental contamination. In the energy management sector, they pointed out the work of [9] who designed a CPS application for the Energy Management Framework (EMF). The designed CPS collects the real-time power consumption demand and status from an autonomous electric vehicle (AEV) and the charging station in a smart grid. This EMF hierarchical network architecture minimizes the energy consumption of wireless sensor networks (WSNs) for optimizing the power supply and distribution. In the process control field, [10] offer a control-theoretic software to monitor solutions for coordinating time predictability and memory utilization in runtime monitoring of systems that interact with the physical world. In the other category, smart manufacturing, the work of [11] has been mentioned, in which they try to develop a flexible, modular and distributed control architecture for automated warehouse systems using Function Blocks and a CPS perspective in the category of intelligent transportation, the work of [12, 13] in traffic management in transport engineering is introduced. Thanks to the intelligent cyber-physical road systems the automatic collection of traffic data was possible so they could measure

the number of vehicles traveling from one geographical location to another.

Background

Background on Formal Concept Analysis

Formal concept analysis (FCA) is based on the lattice theory [14] and was proposed by a German mathematician, Wille [30] in 1982. FCA is a formal context to represent the relationship among concepts and attributes. It is indeed a mathematical theory for handling concepts and their hierarchies [15]. FCA is best used for knowledge representation, data analysis, and information management. It detects conceptual structures in data and consequently extraction of dependencies within the data by forming a collection of objects and their properties known as attributes [16, 17].

The concept lattice involves different nodes where each node is a formal concept consisting of two parts: an extent and an intent. An extent is described as an object set in the concept domain while an intent is the set of attributes that are shared by the objects in the object set. Accordingly, a formal concept is a collection of objects with some common attributes, to that point, what is called finding formal concepts in a lattice is in fact clustering the objects within the object set [15].

Formal context is a triple $K=(U, M, I)$, where U is a set of objects (or samples), M is a set of attributes (or features), and $I \subseteq U \times M$ is a binary relation called indices incidence that expresses which object has what attribute. For any $x \in U$ and $m \in M$, $(x, m) \in I$ represent that the object x has the attribute m.

A formal context can be easily represented by a table (see Table 1), where the rows are headed by the object names (here as x_i) and the columns headed by the attribute names (hereasm_j). For example, a cross in row 2 and column 3 means that x_2 has the attribute m_3.

To discover any hidden relationship among the attributes, FCA employs association rule mining (ARM). FCA first constructs the formal contexts by the sets of objectives and their attributes. Using this formal context, it extracts underlying information with the creation of the concept lattice and then by applying ARM, it detects regularities between attributes in large data sets and tries to introduce patterns for attributes which has been seen together frequently [18].

Let $I = \{i_1, i_2, ..., i_n\}$ be a set of n binary attributes called items. Let $D = \{t_1, t_2, ..., t_m\}$ be a set of transactions called the database. Each transaction in D has a unique transaction ID and contains a subset of the items in the I. A rule is defined as an implication of the form $X \Rightarrow Y$ where $X, Y \subseteq I$ and $X \cap Y = \emptyset$. The sets of items (for short itemsets) X and Y are called antecedent and consequent of the rule [19]. The defined rule can mean that if X is chosen then it is likely that Y is also selected.

To better extract rules, some measures are defined in the FCA-based ARM. The best-known measures are Support and Confidence, which are the main measures employed in the present study.

The support supp(X) of an itemset X is defined as "the proportion of transactions in the data set which contain the itemset". For example, if the support of itemset X is 0.4 it means that the itemset occurs in 40% of all transactions. On the other hand, the confidence of a rule is defined $\text{conf}(X \Rightarrow Y) = \text{supp}(X \cup Y)/\text{supp}(X)$ and can be interpreted as "an estimate of the probability $P(Y|X)$, the probability of finding the antecedent of the rule in transactions under the condition that these transactions also contain the consequent". For example, if the $\text{conf}(X \Rightarrow Y) = 0.5$, it means the rule $X \Rightarrow Y$ is correct in 50% of the transactions containing X and Y [19].

FCA-based ARM can be a very helpful method in recognising the patterns as it: (1) extracts all the association rules from a given data without redundancies; (2) generates the rules faster and more efficiently; and (3) discovers more significant rules [18].

Background and Study on CPS Characteristics

CPSs are often engineered systems and are differentiated from other types of engineered systems as they are built on the integration of cyber and physical components. It is, therefore, agreed upon that CPS functionalities come from the tight integration of the cyber and physical sides and create CPS characteristics in different terms. On the other hand, CPSs should be characterized by well-defined components. They should provide components with well-known characteristics described using standardized semantics and syntax. Therefore, defining and shaping key characteristics of CPSs will pave the path to better development and implementation management within and across various domains of CPS applications [20]. Considering the above, and exploring how CPS metamodels are characterized and defined, the focus point of the present study has been put on exploring the CPS characterises in various domains in scientific papers.

Napoleone et al. [21] discussed the technological characteristics of CPSs in manufacturing emergent from existing

Table 1 An example of a formal context K

U	m_1	m_2	m_3	m_4	m_5
x_1	×	×		×	
x_2		×	×	×	×
x_3	×		×	×	×
x_4	×	×			×

Table 2 Studied CPS characteristics and their definition in the literature

Characteristics	Definition	References
Resiliency	Resilience is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation	[22]
Redundancy	Redundancy is the duplication of critical components or functions of a system. It is the ability of providers to have different alternatives	[22]
Complexity	The complexity of CPSs is due to the different nature of their elements. CPSs are often equipped with embedded systems (software and hardware) able to generate, communicate, and evaluate huge amounts of data about the ongoing production processes	[23]
Heterogeneity encapsulation	CPSs are heterogeneous because they integrate several different systems together with standard communication and information	[24]
Interoperability	Interoperability is the capability of system components to connect, communicate, and operate with each other. Interoperability allows CPSs to exchange mutually intelligible information exchange	[24–26]
Connectivity	CPSs consist of entities that are connected, based on the context, within and across all levels of production activities, from machine operation, process control, up to entire production and logistics networks	[27, 28]
Networking capability	CPSs should be composed of interconnected clusters of processing elements and physical elements in large-scale wired and wireless networks through a variety of sensors and actuators, aiming at constructing intelligence across different fields. Connecting these fields usually relies on the Internet; dynamic participation in the network is herein possible	[29–31]
Modularity	Modularity is the capability of a CPS to be modularized, flexibly changed, and reconfigured in response to rapidly changing customer needs and product changes	[25, 32]
Autonomy	Autonomy is the capacity of CPS to independently learn and adapt to the environment	[33]
Self-capabilities	Different types of self-capabilities: self-adaptivity	[34]
	Self-reconfiguration, self-organization	[23]
	Self-awareness	[35]
	Self-learning	[36]
	Self-diagnosis	[37]
	Self-healing	[38]
	Self-optimization	[39]
	Self-protection, and self-explaining	[40]
Integration	CPSs are the integration of computation and physical processes	[41–43]
Virtualization	Virtualization consists of creating a virtual copy of the real physical world and remaining connected to it over time	[24]
Real-time capability	Real-time capability is the ability of CPSs to acquire and analyse real-time data on equipment, quality and raw materials and provide the derived insights immediately	[25, 35, 44]
Computational capability	The cyber parts of CPSs should be able to perform a significant amount of computation and control work previously performed by a human, and today also strengthened by the possibility to share data and interact with each other	[45, 46]
Intelligence/smartness	CPS can use sensors and actuators to collect information about the physical operations in real-time and conduct intelligent control over physical systems to adapt to changing conditions and environment	[28]
Cooperation	Cooperation is the capability of a distributed system with autonomous subsystems to dynamically decide which components will carry out a certain task to optimize performances such as the response time	[47]
Collaboration	Collaboration relies on the ability to share information between different stakeholders at different locations	[41]
Reconfigurability	Reconfigurability refers to the characteristic that enables quick responsiveness to market changes and disturbances	[48]
Adaptability	Adaptability is the ability of CPSs to adapt to quickly changing situations and new requirements (such as new products or product variants) through dynamic reorganization/reconfiguration	[24, 49]
Scalability	It refers to the ability of complex CPSs to change during their life cycle, due to either a growing or shrinking number of "nodes" (nodes could be either participating or managed physical systems, sub-systems or components of the CPSs)	[40]
Diagnosability	The ability to autonomously detect and diagnose the root cause of product defects or otherwise actively support users in their identification; moreover, they should operate in a traceable way	[50, 51]

Table 2 (continued)

Characteristics	Definition	References
Predictability	Predictability is the ability to predict CPSs' behaviour, supporting the detection of unexpected events and the root cause analysis in case of a failure	[40]
Uncertainty	Uncertainty can be defined as the lack of "knowledge" about the internal behaviour of a CPS and its composed physical units, and its operating environment	[45]
Fault-tolerant	Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of (one or more faults within) some of its components	[52]
Composability	Understanding and mitigating interactions (among components and applications) require that CPS be designed as open as a composable system	[53]
Reliability	System reliability is the ability of a system to perform its intended function under a given set of environmental and operational conditions for a given period of time	[54]
Safety and security	Safety is aimed at protecting the systems from accidental failures to avoid hazards, while security is focused on protecting the systems from intentional attacks	[55]
Stability	Stability means the CPS can achieve a stable sensing-actuation close-loop control even though the inputs (sensing data) have noise or attacks	[56]

literature in detail. They carried out a structured review to investigate the CPS characteristics that have been studied in scientific papers. In the end, they came up with the 19 most cited lower-order characteristics and then provided their literature-based descriptions and, explaining their reasoning, aggregated them to eight higher-order characteristics. A base CPS characteristic list was considered on account of their work aiming at delineating CPS metamodels. Therefore, the choice of content analysis for our work was established as deductive. However, during the procedure of analysing the papers and digging deeper into the study, the list of the characteristics that were gone through for the analysis was modified to what can be seen in Table 2.

Clustering Assessment on Characteristics Using the Formal Concept Analysis Method

To answer the two research questions, "How CPS metamodels are described and characterized?" and "How is Knowledge represented in CPS metamodels?", scientific papers were gone through whether they discuss, implicitly or explicitly, the CPS characteristics given in the last section. Hence, formal concept analysis (FCA), as a clustering technique, was chosen to help us first to describe the CPS metamodels and then scrutinize the CPS characteristics and the hidden relationship between them in the chosen papers.

FCA has been discussed previously in the background section. It has been mentioned that it detects conceptual structures in data and consequently extraction of dependencies within the data by forming a collection of objects and their properties [17]. The FCA method starts with a formal context as shown in Table 1 where the input data will form a matrix, in which each row represents an object from the domain of interest, and each column represents one of the defined attributes. In the present study, the formal contexts are formed by including articles as the objects and the CPS characteristics as attributes. If an article has, implicitly or explicitly, investigated the CPS characteristics in their metamodel a "×" is input in the cell. Otherwise, the cell remains empty. Table 3 represents the formal context prepared for the analysis in this work.

In general, FCA results in two sets of output data: a hierarchical relationship of all the established concepts in the form of a Hasse diagram called a concept lattice and a list of all interdependencies found among attributes in the formal context. The latter is what was used for the analysis of the CPS characteristics in this work. As explained previously, FCA uses the formal context to extract information and detect regularities between attributes so that it can introduce patterns for attributes which has been seen together frequently. In the present study, FCA resulted in regularities among CPS characteristics, detecting what characteristics that have been studied more frequently (single clustering) and also the characteristics that have been regularly studied or used together (double clustering).

Figure 2 represents the result of FCA on single clustering of CPS characteristics. As it is seen, "Resiliency" was the one characteristic that stood on the top of the list, with a noticeable difference from the rest, as the most reflected characteristic in the literature whether to be explicitly or implicitly mentioned. Characteristics like "Fault-Tolerant", "Diagnosability", "Redundancy" and "Safety and Security" come next in the list with a noticeable difference from Resiliency and ignorable divergence among themselves. On the other hand, characteristics like Reconfigurability, Collaboration, Controllability, and Self-capabilities are at the end of the list, which does not refer to the lack of importance on the characteristics though. The main reason might mostly be that they are the characteristics that are fundamental and taken for granted in the design and application of CPSs.

Table 3 The formal context

References	Resiliency	Stability	Fault-Tolerant	Uncertainty	Redundancy	Composability	Complexity	Stochastic	Heterogeneity encapsulation	Interoperability	Standardization	Communication	Connectivity	Networking capability	Modularity	Reusability	Replaceability	Inheritance
[22]	×				×													
[57]																		
[58]						×	×								×	×	×	×
[59]				×			×		×	×								
[60]			×				×			×				×				
[61]	×		×															
[62]									×	×								
[63]							×			×								
[64]									×							×		
[65]			×				×					×						
[66]										×			×	×				
[67]							×		×	×			×		×	×		
[68]							×	×	×	×			×					
[69]				×			×											
[70]	×																	
[71]	×		×			×												
[72]										×								
[60]									×	×								
[73]																		
[74]																×		
[75]																		
[76]										×			×		×			
[77]																		
[78]									×	×		×						
[79]																		
[80]									×									
[81]																		
[82]										×		×						
[83]												×						
[84]	×		×		×													
[85]												×						
[86]							×					×						
[87]			×						×	×			×					
[88]							×			×								

Table 3 (continued)

References	Resiliency	Stability	Fault-Tolerant	Uncertainty	Redundancy	Composability	Complexity	Stochastic	Heterogeneity encapsulation	Interoperability	Standardization	Communication	Connectivity	Networking capability	Modularity	Reusability	Replaceability	Inheritance
[89]	×		×			×	×					×						
[90]										×			×					
[91]	×		×	×	×		×		×							×		
[92]	×	×	×	×		×			×	×				×				
[93]		×		×			×											
[94]	×											×	×					
[95]	×		×		×													
[96]	×	×								×		×	×					
[97]	×											×	×					
[98]	×	×																
[99]	×	×										×				×		
[100]	×	×										×						
[101]	×	×										×						
[102]	×											×	×					
[11]													×		×			
[103]	×		×		×													
[104]	×			×	×				×			×						
[105]	×				×					×			×					
[106]							×											
[107]	×	×																
[108]	×		×		×													
[109]	×																	
[110]	×		×															
[111]	×				×													
[112]	×				×							×						
[113]	×	×			×							×	×					
[114]	×	×	×		×													
[115]	×	×																
[116]	×				×													
[117]	×		×		×													
[118]	×		×		×													
[119]	×				×													
[120]	×			×					×									

Table 3 (continued)

References	Resiliency	Stability	Fault-Tolerant	Uncertainty	Redundancy	Composability	Complexity	Stochastic	Heterogeneity encapsulation	Interoperability	Standardization	Communication	Connectivity	Networking capability	Modularity	Reusability	Replaceability	Inheritance
[121]	×		×		×													
[122]	×		×		×													
[123]	×		×		×													
[124]	×				×													

References	Continuity	Autonomy	Self-Capabilities	Integration	Virtualization	Real-time capability	Computational capability	Intelligence/smartness	Cooperation	Collaboration	Controllability	Reconfigurability	Reliability	Adaptability	Scalability	Safety and Security	Diagnosable	Predictability
[22]																		
[57]																		
[58]	×	×	×		×													
[59]																		
[60]				×			×											
[61]			×				×	×						×			×	
[62]								×										
[63]																		
[64]																		
[65]																		
[66]																	×	×
[67]				×														
[68]							×											
[69]																		
[70]																	×	
[71]						×		×							×		×	
[72]																		×
[60]																		
[73]																		×
[74]																		
[75]						×												
[76]								×										
[77]		×																
[78]				×														
[79]				×														

Table 3 (continued)

References	Continuity	Autonomy	Self-Capabilities	Integration	Virtualization	Real-time capability	Computational capability	Intelligence/smartness	Cooperation	Collaboration	Controllability	Reconfigurability	Reliability	Adaptability	Scalability	Safety and Security	Diagnosable	Predictability
[80]				×				×				×					×	
[81]		×		×			×											
[82]				×		×	×						×					
[83]							×											
[84]				×												×		×
[85]							×									×		
[86]							×				×							
[87]		×	×			×		×										
[88]				×														
[89]													×					×
[90]									×	×								
[91]						×										×	×	
[92]				×			×											×
[93]																		
[94]			×					×		×								×
[95]				×		×		×					×		×			×
[96]							×						×			×		
[97]																×		
[98]																×		
[99]		×		×									×			×	×	×
[100]							×									×		
[101]													×					
[102]						×	×									×		×
[11]												×						
[103]													×			×	×	×
[104]							×				×					×	×	
[105]						×												
[106]																		
[107]				×		×										×		×
[108]																×	×	
[109]											×					×		×
[110]				×							×		×			×	×	×
[111]														×			×	

Table 3 (continued)

References	Continuity	Autonomy	Self-Capabilities	Integration	Virtualization	Real-time capability	Computational capability	Intelligence/smartness	Cooperation	Collaboration	Controllability	Reconfigurability	Reliability	Adaptability	Scalability	Safety and Security	Diagnosable	Predictability
[112]		×															×	
[113]						×							×					
[114]													×					
[115]						×										×	×	
[116]																×	×	
[117]													×			×	×	
[118]													×			×	×	
[119]																×		
[120]		×				×										×		
[121]						×											×	
[122]						×											×	
[123]																×	×	
[124]													×			×		

Figure 3 shows what was extracted from the coupling demonstration of characteristics in the analysed papers through FCA. Going through the results, the combination of Resiliency with other characteristics is the one observed the most, which was somehow predictable by the analysis of the single characteristics. However, the pair of {Resiliency; Redundancy}, {Resiliency; safety and security}, {Resiliency; Fault-Tolerant} and {Resiliency; diagnosability} are at the top ranking, respectively which one way or another can show a close relationship between the concepts; the outcome that establishes the backbone of the upcoming discussion.

As discussed previously, FCA uses association rules to help detect patterns among regular attributes. Moreover, the measures of support and confidence have been introduced to check the reliability of the detected patterns and also their probability of appearance.

To serve this purpose, the software LATTICE MINER 2.0 was adopted as the result of the analysis done. The association rules between the selected CPS characteristics were extracted considering the minimum support level as 20% and minimum confidence level as 20% as shown in Table 4. The minimum levels were defined by a try-and-error procedure.

Looking through the association rules, the probability of achieving resiliency through fault tolerant, diagnosability, safety and security and finally redundancy goes over 84% which itself confirms the result for the first step in FCA. It is also worth noting that, resiliency is in all the itemsets that have support levels above 20% and a confidence of 50% and above.

Discussion on the Results

Concerning the results of FCA achieved in the previous part, resiliency draws the most attention to itself among other characteristics. Different terms were used and established in the literature for a CPS that has "resilience" such as survivable [104] or Fail-safe [114].

Furthermore, the present study investigated the concept, whether it was explicitly or implicitly discussed in scientific papers. To name a few, [22] tried to reach resiliency by modelling the functions and also the links between the components of the metamodel with the help of FCA. Looking at the hierarchical inclusion of the CPS metamodel and thanks to the created lattice, they could find control over redundancy and therefore elevate the resiliency of the system. Sangiovanni-Vincentelli et al. [91] addressed the systems engineering of cyber-physical contract-based design by employing structured and formal design methodologies to finally increase the reliability and consequently the resiliency of the CPS metamodel. Although [71] did not mention resiliency directly as an objective of their study, they have had it implicitly targeted through an integration of the physical layer, the

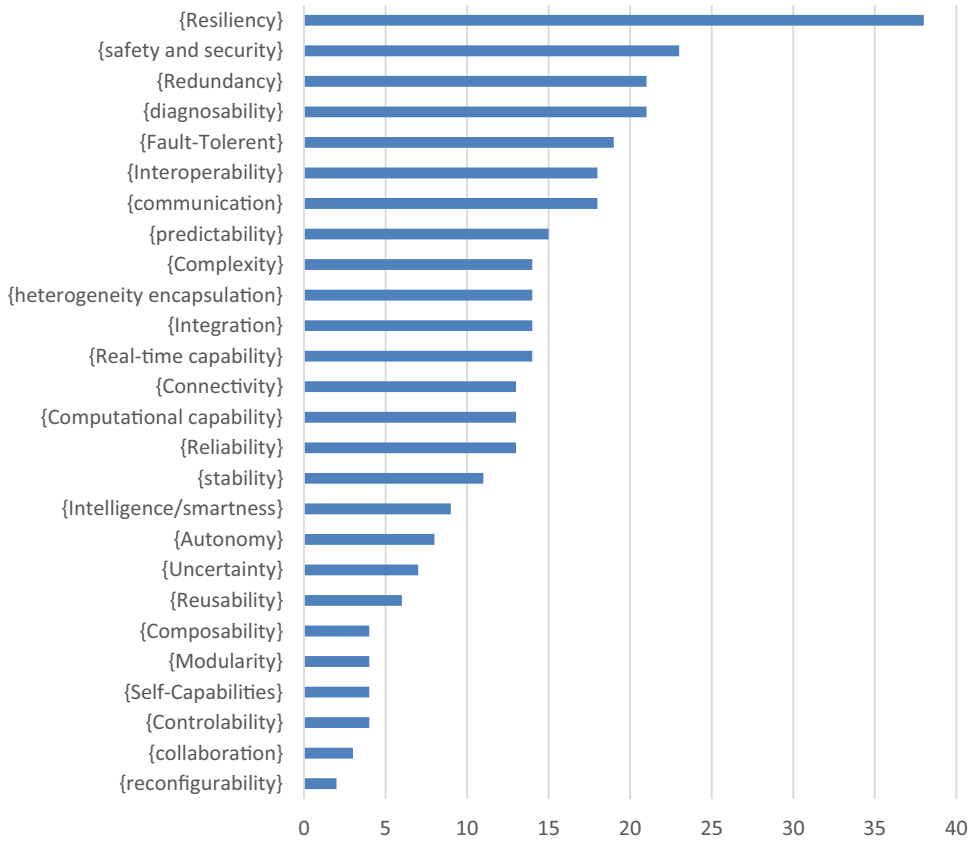

Fig. 2 Single clustering of CPS characteristics

network layer and the business layer. The integration at the end leads to a better investigation of the hardware status information, software, patches and other information for perception, acquisition and control. The integration results in a platform by which the controllability, diagnosability and fault-tolerant of the CPS are increased which will be directed to more survivability of the system.

Given the importance of the concept, different paths were taken to reach and increase the resiliency of a CPS. Due to the results observed, the main two tracks were used more frequently than the two characteristics: 'safety and security' and 'fault-tolerance'. For example, [124] believes that only by unifying safety, security and resiliency it is possible to reach adaptable and dynamic design patterns that can take into account the intended functions of a system. [114] explored fault tolerant control systems (FTCS) and mentioned that they can withstand the failures and errors of the components of the system itself and preserve the system performance to the maximum, therefore, they can survive and be resilient.

Digging a bit deeper, the resiliency of a system was thrown together with recognizing different challenges and risks along with defining proper metrics to protect the endangered system and estimating plant states despite attacks [22, 112]. Observing the trend illustrates different efforts to elevate the resiliency of the system: through characteristics like predictability and diagnosability which also stood at the high ranks of the FCA double clustering.

Redundancy and reliability were also the characteristics that coupled well with resiliency in FCA and were also discussed closely with the concept in the literature. As mentioned by [112], redundancy is the principle that can be advantageous in estimating resiliency in the majority of systems. On the other hand, the intention of redundancy in the system can be to increase its reliability since it relies on employing multi-pronged solutions rather than a single technique which also improves the security and resiliency of the system [22].

In addition to all, stability was also a characteristic that was paid attention to in reaching safety, security and consequently the resiliency of the system since fast reconfiguration of attacks can lead to maintaining the stability of the system which keeps it safe and helps it retain normal operation [99].

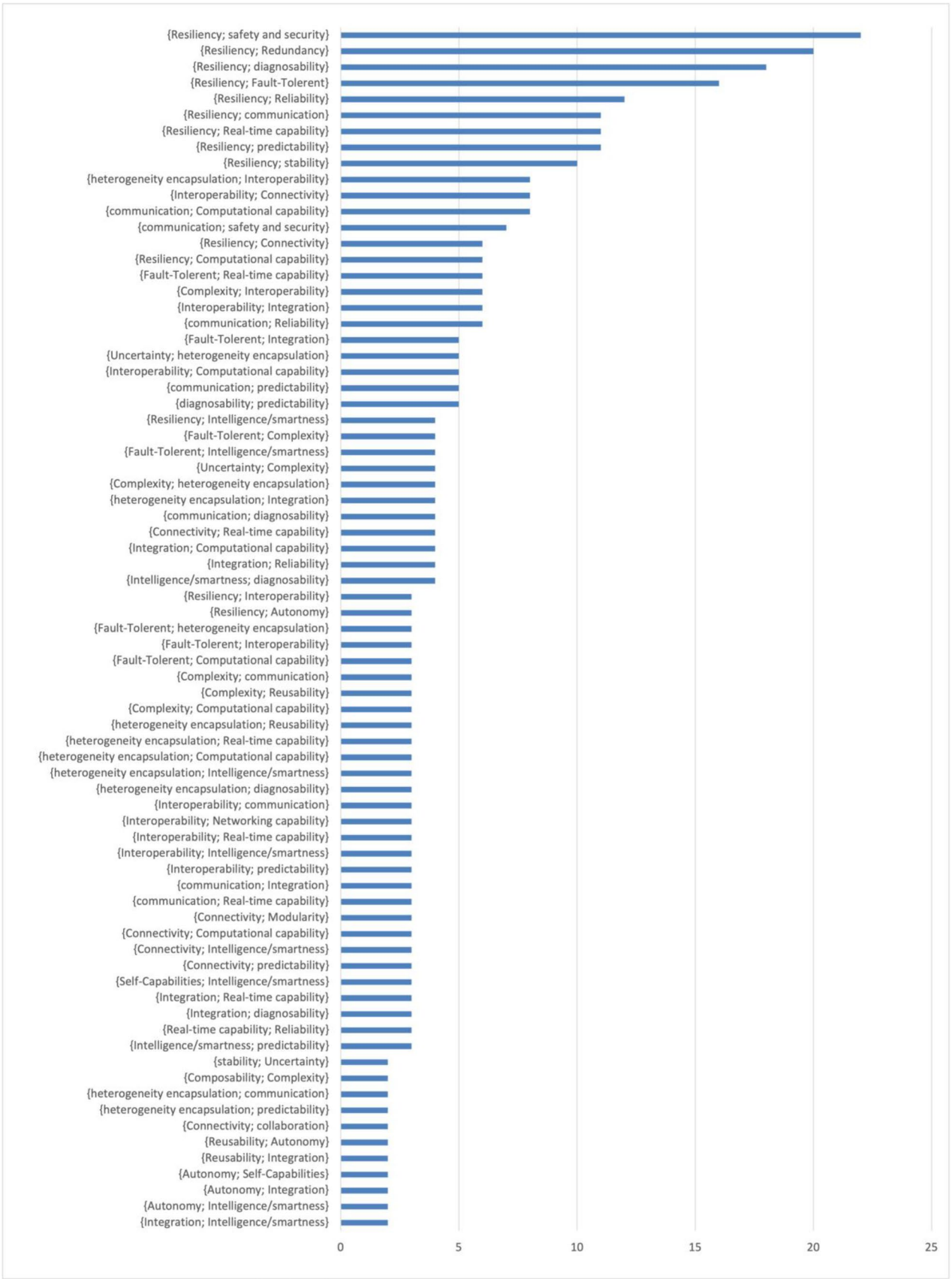

Fig. 3 Double clustering of CPS characteristics

Table 4 Association rules between the CPS characteristics

#	Antecedent	= >	Consequence	Support	Confidence
1	Resiliency	= >	Redundancy	27.02%	52.63%
2	Resiliency	= >	diagnosability	24.32%	47.36%
3	Resiliency	= >	Fault-Tolerant	21.62%	42.10%
4	Resiliency	= >	safety and security	29.72%	57.89%
5	Fault-tolerant	= >	Resiliency	21.62%	84.21%
6	Diagnosability	= >	Resiliency	24.32%	85.71%
7	Safety and security	= >	Resiliency	29.72%	95.65%
8	Redundancy	= >	Resiliency	27.02%	100.00%

A Schematic Hierarchy of the CPS Characteristics

Based on the observations and the FCA outcomes, the characteristics "resiliency" was chosen as the most used and applied among the others. Therefore, we used the discovered implicit relationships among the characteristics (thanks to FCA-based ARM) to design a hierarchy of characteristics to map achieving resiliency of a CPS. The hierarchy illustrates different levels of characteristics that directly or indirectly influence resiliency, from built-in characteristics that cannot be ignored in the design of a CPS to the ones that have a non-breakable effect on the top level.

As depicted in Fig. 4, the hierarchy represents 4 different levels:

- the top level (Level 1) is dedicated to the characteristics that were used the most frequently among the ones investigated in the scientific papers, i.e., resiliency.
- Level 2 is representing the second-graded characteristics that have a linear connection with characteristics in Level 1 and a direct influence on it, i.e., Safety and Security and Fault-tolerance.
- Level 3 portrays the characteristics that helped the CPS reach the second-graded ones in Level 2 and consequently to resiliency as in the first level.
- Level 4 illustrates the bottom-line characteristics that were not directly led to elevating resiliency but are fundamental to forming a CPS, without which the system might not function efficiently.

As mentioned above, the hierarchy resulted from the study of the hidden relationship among the characteristics of CPS and how they are related to each other. Regarding the FCA results and the consequent association rules (ARM), resiliency was the characteristic that appeared the most while searching for solutions for the survival of the CPS meta-models and a more efficient performance. The proposed hierarchy maps the road of observed characteristics to achieve resiliency in a CPS meta-model from the built-in characters to the top.

Following the results of FCA, the higher-level characteristics in the hierarchy have been redefined using other characteristics that seem to be related to them. The relationship comes from FCA analysis and their positioning in the hierarchy, therefore, the related characteristics contribute to acts, behaviours and consequently definition of the main characteristic. Table 5 captures the connected terms in the redefinition of the selected characteristics.

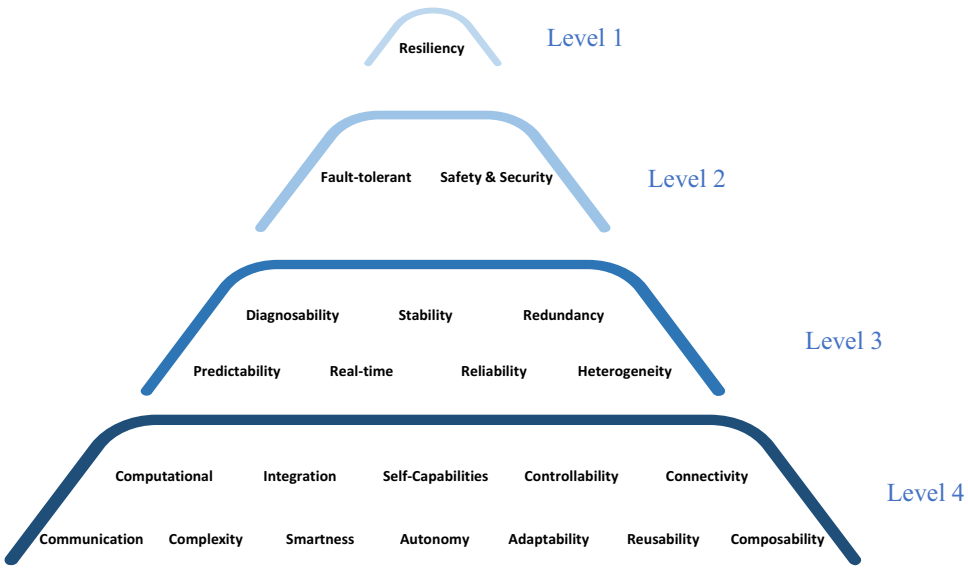

Fig. 4 Hierarchy of characteristics to reach resiliency

Table 5 Characteristics redefinition due to the hierarchy

Characteristic	Definition	Related characteristics													
		Intelligence smartness	Reliability	Diagnosability	Connectivity	Redundancy	Real-time	Predictability	Fault-tolerant	Resiliency	Uncertainty	Adaptability	Integration	Safety and Security	Stability
Resiliency	Resiliency is the capability to keep the stability, safety and quality of the service in the time of (un) predicted faults and threats and accommodate the networking system with different alternatives to help it operate with no interruption	✓	✓	✓	✓	✓	✓	✓	✓					✓	

Table 5 (continued)

Characteristic	Definition	Related characteristics														
		Intelligence smartness	Reliability	Diagnosability	Connectivity	Redundancy	Real-time	Predictability	Fault-tolerant	Resiliency	Uncertainty	Adaptability	Integration	Safety and Security	Stability
Safety and Security	Safety is aimed at keeping the systems resilient and safe in times of unpredicted faults to avoid failure, while security is focused on protecting the systems from intentional attacks						✓	✓	✓	✓					

Table 5 (continued)

Characteristic	Definition	Related characteristics													
		Intelligence smartness	Reliability	Diagnosability	Connectivity	Redundancy	Real-time	Predictability	Fault-tolerant	Resiliency	Uncertainty	Adaptability	Integration	Safety and Security	Stability
Fault-Tolerant	Fault-tolerant is the capability of the system to keep the system resilient after a failure has occurred and protects the system from accidental failures or intentional attacks. The capability mainly comes from the combination of redundant system elements, diagnosing and correcting procedures	✓				✓	✓			✓	✓	✓		✓	

Table 5 (continued)

Characteristic	Definition	Related characteristics													
		Intelligence smartness	Reliability	Diagnosability	Connectivity	Redundancy	Real-time	Predictability	Fault-tolerant	Resiliency	Uncertainty	Adaptability	Integration	Safety and Security	Stability
Redundancy	Redundancy is the capability that can provide the system with alternatives which helps the system retain its normal operation and keeps the quality and stability of the system without accidental failures in times of fault, (un) predicted events and intentional attacks									✓					

Table 5 (continued)

Characteristic	Definition	Related characteristics													
		Intelligence smartness	Reliability	Diagnosability	Connectivity	Redundancy	Real-time	Predictability	Fault-tolerant	Resiliency	Uncertainty	Adaptability	Integration	Safety and Security	Stability
Diagnosability	Diagnosability is the capability of the real-time identification of specific states that may correspond to system malfunction due to a fault or an attack to keep the system operating	✓					✓			✓					

Table 5 (continued)

Characteristic	Definition	Related characteristics													
		Intelligence smartness	Reliability	Diagnosability	Connectivity	Redundancy	Real-time	Predictability	Fault-tolerant	Resiliency	Uncertainty	Adaptability	Integration	Safety and Security	Stability
Predictability	Predictability is the ability to predict CPSs' behaviour, supporting the detection of unexpected events and the root cause analysis in case of a failure to keep the system resilient									✓			✓	✓	
Reliability	Reliability is the capability to correspond to and tolerate system random malfunction due to a fault or an attack to keep the system operating and stable							✓	✓	✓					✓

Table 5 (continued)

Characteristic	Definition	Related characteristics													
		Intelligence smartness	Reliability	Diagnosability	Connectivity	Redundancy	Real-time	Predictability	Fault-tolerant	Resiliency	Uncertainty	Adaptability	Integration	Safety and Security	Stability
Stability	Stability is the capability to achieve a stable sensing actuation control and tolerate system random malfunction in times of accidental failures or intentional attacks		✓						✓	✓					

Table 5 (continued)

Characteristic	Definition	Related characteristics													
		Intelligence smartness	Reliability	Diagnosability	Connectivity	Redundancy	Real-time	Predictability	Fault-tolerant	Resiliency	Uncertainty	Adaptability	Integration	Safety and Security	Stability
Real-time	Real-time capability is the ability of CPSs to acquire and analyse real-time data on equipment, quality and raw materials and provide the derived insights immediately. The aim is to detect unexpected events in real-time to make sure the system is stable and can tolerate system random malfunction due to a fault or an attack		✓					✓	✓	✓					✓

Subsequently, resiliency, as the most frequent characteristic, has been put in words as the capability to keep the safety, stability, and quality of the service in the time of (un)predicted faults and threats and accommodate the networking system with different alternatives to help it operate with no interruption. The definition relates closely to the other two characters pursuing resiliency, safety and security and fault tolerance. As disclosed above, CPS engineering is mostly leaning on keeping the system safe, secure and stable at the time of predicted or sudden attacks or threats. This aim can be reached through having functional or operational alternatives, real-time identification and detection of failures or faults by considering the fundamental characteristics of the CPS located at the bottom order.

Conclusions

The paper continues the previous work of the authors on studying cyber-physical systems and their representative characteristics in the literature. Two research questions were put as the principal of the search, i.e., 'How CPS metamodels are described and characterized?', 'How is Knowledge represented in CPS metamodels?', through which CPS metamodels were investigated regarding what characteristics they are designed to mirror. A literature review was done focusing on the two research questions to investigate the current opinion in the literature on what characteristics to target more frequently in studying a CPS meta-model. Therefore, articles in the literature were selected based on two main criteria: (1) they study CPS metamodels and (2) they refer to one or some CPS characteristics in their metamodel study. After a two-step literature review, CPS characteristics, implicitly or explicitly discussed, were extracted. Afterwards, Formal Concept Analysis (FCA) as the clustering technique was applied to detect any hidden relationship among the most used characteristics in the articles. Due to the results, "Resiliency" was the characteristic that was targeted the most frequent, implicitly or explicitly, in the scientific papers. "Fault-Tolerant", "Diagnosability", "Redundancy" and "Safety and Security" were the ones that followed resiliency in the list but with a noticeable difference.

Thanks to FCA, the implicit bonds between characteristics in the literature were also disclosed which led to a hierarchy of CPS characteristics aiming at reaching resiliency in the metamodels. A new set of definitions for the highly ranked characteristics was also introduced that sheds light on future CPS metamodel designs regarding what characteristics to target and what path to take to be more aligned with the concept of Industry 4.0.

This study was focused on what has been observed in the literature from different researchers in the field and it aims at reporting trends and themes on CPS characteristics. However, there is still a gap in the literature on the cyber-physical systems on whether we can define any dominant characteristic in the development of a CPS metamodel. As a future work, the result of this study can help in the development of measures or indicators in significance assessment of any CPS characteristics.

Data availability The data related to the study are all present in the article. No excess data ia available to share.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Eslami Y, Ashouri S, Franciosi C, Lezoche M. Knowledge extraction in cyber-physical systems meta-models: A formal concept analysis application. In: Proceedings of the 3rd International Conference on Innovative Intelligent Industrial Production and Logistics - IN4PL; ISBN 978-989-758-612-5; ISSN 2184-9285. SciTePress;2022. pp. 129-136. https://doi.org/10.5220/0011536700003329.
2. Liu Y, Peng Y, Wang B, Yao S, Liu Z. Review on cyber-physical systems. IEEE/CAA J Autom Sin. 2017;4:27–40. https://doi.org/10.1109/JAS.2017.7510349.
3. Someswara Rao C, Shiva Shankar R, Murthy KVS (2020) Cyber-Physical System—An Overview. In: Satapathy S, Bhateja V, Mohanty J, Udgata S (eds) Smart Intelligent Computing and Applications . Smart Innovation, Systems and Technologies, vol 160. Singapore: Springer. https://doi.org/10.1007/978-981-32-9690-9_54.
4. Verma R. Smart city healthcare cyber physical system: characteristics, technologies and challenges. Wirel Pers Commun. 2022;122:1413–33. https://doi.org/10.1007/s11277-021-08955-6.
5. Wu X, Goepp V, Siadat A. Cyber physical production systems: a review of design and implementation approaches. 2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Macao, China, 2019. pp. 1588-1592. https://doi.org/10.1109/IEEM44572.2019.8978654.
6. Juhlin P, Schlake JC, Janka D, Hawlitschek A. Metamodeling of Cyber-Physical Production Systems using AutomationML for Collaborative Innovation. 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vasteras, Sweden, 2021. pp. 1-4. https://doi.org/10.1109/ETFA45728.2021.9613560.
7. Chen H. Applications of cyber-physical system: a literature review. J Ind Integr Manag. 2017. https://doi.org/10.1142/S2424862217500129.
8. Mehdipour F. Smart field monitoring: an application of cyber-physical systems in agriculture (work in progress). Proceedings—2014 IIAI 3rd international conference on advanced applied informatics, IIAI-AAI 2014. 2014. p. 181–84. https://doi.org/10.1109/IIAI-AAI.2014.46.
9. Wan J, Yan H, Li D, Zhou K, Zeng L. Cyber-physical systems for optimal energy management scheme of autonomous electric vehicle. Comput J. 2013;56:947–56. https://doi.org/10.1093/comjnl/bxt043.

10. Medhat R, Bonakdarpour B, Kumar D, Fischmeister S. Runtime monitoring of cyber-physical systems under timing and memory constraints. ACM Trans Embed Comput Syst. 2015;14:79:1-79:29. https://doi.org/10.1145/2744196.
11. Basile F, Chiacchio P, Coppola J, Gerbasio D. Automated warehouse systems: a cyber-physical system perspective. In: 2015 IEEE 20th conference on emerging technologies factory automation (ETFA). 2015. p. 1–4. https://doi.org/10.1109/ETFA.2015.7301597.
12. Zhou Y, Xiao Q, Mo Z, Chen S, Yin Y. Privacy-preserving point-to-point transportation traffic measurement through bit array masking in intelligent cyber-physical road systems. 2013. p. 826–33. https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.146.
13. Zhou Y, Mo Z, Xiao Q, Chen S, Yin Y. Privacy-preserving transportation traffic measurement in intelligent cyber-physical road systems. IEEE Trans Veh Technol. 2015;65:1–1. https://doi.org/10.1109/TVT.2015.2436395.
14. Wille R. Restructuring Lattice Theory: An Approach Based on Hierarchies of Concepts. In: Rival I, editor. Ordered Sets. NATO Advanced Study Institutes Series, vol 83. Springer; Dordrecht: 1982. https://doi.org/10.1007/978-94-009-7798-3_15.
15. Hu Q, Yuan Z, Qin K, Zhang J. A novel outlier detection approach based on formal concept analysis. Knowl Based Syst. 2023;268: 110486. https://doi.org/10.1016/j.knosys.2023.110486.
16. Mezni H, Sellami M. Multi-cloud service composition using formal concept analysis. J Syst Softw. 2017;134:138–52. https://doi.org/10.1016/j.jss.2017.08.016.
17. Wajnberg M, Lezoche M, Massé BA, Valtchev P, Panetto H. Complex system tacit knowledge extraction trough a formal method. INSIGHT Int Counc Syst Eng (INCOSE). 2017;20:23–6. https://doi.org/10.1002/inst.12176.
18. Kim E-H, Kim H-G, Hwang S-H, Lee S-I. FARM: an FCA-based association rule miner. Knowl Based Syst. 2015;85:277–97. https://doi.org/10.1016/j.knosys.2015.05.013.
19. Hornik K, Grün B, Hahsler M. arules—a computational environment for mining association rules and frequent item sets. J Stat Softw. 2005. https://doi.org/10.18637/jss.v014.i15.
20. Griffor ER, Greer C, Wollman DA, Burns MJ. Framework for cyber-physical systems: volume 1, overview. Gaithersburg: National Institute of Standards and Technology; 2017. https://doi.org/10.6028/NIST.SP.1500-201.
21. Napoleone A, Macchi M, Pozzetti A. A review on the characteristics of cyber-physical systems for the future smart factories. J Manuf Syst. 2020;54:305–35. https://doi.org/10.1016/j.jmsy.2020.01.007.
22. Lezoche M, Panetto H. Cyber-physical systems, a new formal paradigm to model redundancy and resiliency. Enterp Inf Syst. 2018. https://doi.org/10.1080/17517575.2018.1536807.
23. Ilsen R, Meissner H, Aurich JC. Optimizing energy consumption in a decentralized manufacturing system. J Comput Inf Sci Eng. 2017. https://doi.org/10.1115/1.4034585.
24. Yuan X, Anumba CJ, Parfitt KM. Review of the potential for a cyber-physical system approach to temporary structures monitoring. Int J Archit Res. 2015. https://doi.org/10.26687/archnet-ijar.v9i3.841.
25. Rosenberg EH. Smart architecture-bots & Industry 4.0 principles for architecture. In: Martens B, Wurzer G, Grasl T, Lorenz WE, Schaffranek R, editors. Real time—proceedings of the 33rd ECAADe conference—volume 2. Vienna: Vienna University of Technology, 16–18 September 2015. CUMINCAD, 2015. p. 251–59. http://papers.cumincad.org/cgi-bin/works/BasketShow&editable=1/Show?ecaade2015_155. Accessed 25 Apr 2020.
26. Ghobakhloo M. The future of manufacturing industry: a strategic roadmap toward Industry 4.0. J Manuf Technol Manag. 2018;29:910–36. https://doi.org/10.1108/JMTM-02-2018-0057.
27. Upasani K, Bakshi M, Pandhare V, Lad BK. Distributed maintenance planning in manufacturing industries. Comput Ind Eng. 2017;108:1–14. https://doi.org/10.1016/j.cie.2017.03.027.
28. Tu M, Lim MK, Yang M-F. IoT-based production logistics and supply chain system—part 2: IoT-based cyber-physical system: a framework and evaluation. Ind Manag Data Syst. 2018;118:96–125. https://doi.org/10.1108/IMDS-11-2016-0504.
29. Rajkumar R, Lee I, Sha L, Stankovic J. Cyber-physical systems: the next computing revolution. In: Proceedings of the 47th design automation conference, association for computing machinery. Anaheim, California; 2010. p. 731–36. https://doi.org/10.1145/1837274.1837461.
30. Wu F-J, Kao Y-F, Tseng Y-C. From wireless sensor networks towards cyber physical systems. Pervasive Mob Comput. 2011;7:397–413. https://doi.org/10.1016/j.pmcj.2011.03.003.
31. Wang L, Haghighi A. Combined strength of holons, agents and function blocks in cyber-physical systems. J Manuf Syst. 2016;40:25–34. https://doi.org/10.1016/j.jmsy.2016.05.002.
32. Lee H, Ryu K, Cho Y. A framework of a smart injection molding system based on real-time data. Procedia Manuf. 2017;11:1004–11. https://doi.org/10.1016/j.promfg.2017.07.206.
33. Fettermann DC, Cavalcante CGS, de Almeida TD, Tortorella GL. How does Industry 4.0 contribute to operations management? J Ind Prod Eng. 2018;35:255–68. https://doi.org/10.1080/21681015.2018.1462863.
34. Chen B, Wan J, Shu L, Li P, Mukherjee M, Yin B. Smart factory of industry 4.0: key technologies, application case, and challenges. IEEE Access. 2018;6:6505–19. https://doi.org/10.1109/ACCESS.2017.2783682.
35. Lee J, Jin C, Bagheri B. Cyber physical systems for predictive production systems. Prod Eng Res Dev. 2017;11:155–65. https://doi.org/10.1007/s11740-017-0729-4.
36. Scholze S, Barata J, Stokic D. Holistic context-sensitivity for run-time optimization of flexible manufacturing systems. Sensors. 2017;17:455. https://doi.org/10.3390/s17030455.
37. Leitão P, Barbosa J, Papadopoulou M-E, Venieris IS. Standardization in cyber-physical systems: the ARUM case, in. IEEE Int Conf Ind Technol (ICIT). 2015;2015:2988–93. https://doi.org/10.1109/ICIT.2015.7125539.
38. Yu Z, Ouyang J, Li S, Peng X. Formal modeling and control of cyber-physical manufacturing systems. Adv Mech Eng. 2017. https://doi.org/10.1177/1687814017725472.
39. Schuh G, Gartzen T, Rodenhauser T, Marks A. Promoting Work-based Learning through INDUSTRY 4.0. Procedia CIRP. 2015;32:82–7. https://doi.org/10.1016/j.procir.2015.02.213.
40. Heiss M, Oertl A, Sturm M, Palensky P, Vielguth S, Nadler F. Platforms for industrial cyber-physical systems integration: contradicting requirements as drivers for innovation. In: 2015 Workshop on modeling and simulation of cyber-physical energy systems (MSCPES). 2015. p. 1–8. https://doi.org/10.1109/MSCPES.2015.7115405.
41. Wang L, Törngren M, Onori M. Current status and advancement of cyber-physical systems in manufacturing. J Manuf Syst. 2015;37:517–27. https://doi.org/10.1016/j.jmsy.2015.04.008.
42. Lee EA. Cyber-physical systems-are computing foundations adequate, position paper for NSF workshop on cyber-physical systems: research motivation, techniques and roadmap. 2006.
43. Mourtzis D, Vlachou E. Cloud-based cyber-physical systems and quality of services. TQM J. 2016;28:704–33. https://doi.org/10.1108/TQM-10-2015-0133.

44. Hofmann E, Rüsch M. Industry 4.0 and the current status as well as future prospects on logistics. Comput Ind. 2017;89:23–34. https://doi.org/10.1016/j.compind.2017.04.002.
45. Zhang H, Peng C, Sun H, Du D. Adaptive state estimation for cyber physical systems under sparse attacks. Trans Inst Meas Control. 2019;41:1571–9. https://doi.org/10.1177/0142331217730123.
46. Mora H, Colom JF, Gil D, Jimeno-Morenilla A. Distributed computational model for shared processing on cyber-physical system environments. Comput Commun. 2017;111:68–83. https://doi.org/10.1016/j.comcom.2017.07.009.
47. Etxeberria-Agiriano I, Calvo I, Noguero A, Zulueta E. Configurable cooperative middleware for the next generation of CPS. In: 2012 9th international conference on remote engineering and virtual instrumentation (REV). 2012. p. 1–5. https://doi.org/10.1109/REV.2012.6293154.
48. Morgan J, O'Donnell GE. Enabling a ubiquitous and cloud manufacturing foundation with field-level service-oriented architecture. Int J Comput Integr Manuf. 2017;30:442–58. https://doi.org/10.1080/0951192X.2015.1032355.
49. Otto J, Vogel-Heuser B, Niggemann O. Automatic parameter estimation for reusable software components of modular and reconfigurable cyber-physical production systems in the domain of discrete manufacturing. IEEE Trans Ind Inf. 2018;14:275–82. https://doi.org/10.1109/TII.2017.2718729.
50. Ribeiro L, Hochwallner M. On the design complexity of cyber-physical production systems. Complexity. 2018;2018: e4632195. https://doi.org/10.1155/2018/4632195.
51. Ribeiro L, Björkman M. Transitioning from standard automation solutions to cyber-physical production systems: an assessment of critical conceptual and technical challenges. IEEE Syst J. 2018;12:3816–27. https://doi.org/10.1109/JSYST.2017.2771139.
52. Basu S. Plant hazard analysis and safety instrumentation systems. Cambridge: Academic Press; 2016.
53. Gujrati S, Zhu H, Singh G. Composable algorithms for interdependent cyber physical systems. In: 2015 resilience week (RWS). 2015. p. 1–6. https://doi.org/10.1109/RWEEK.2015.7287431.
54. Lazarova-Molnar S, Mohamed N, Shaker HR. Reliability modeling of cyber-physical systems: a holistic overview and challenges. In: 2017 workshop on modeling and simulation of cyber-physical energy systems (MSCPES). 2017. p. 1–6. https://doi.org/10.1109/MSCPES.2017.8064536.
55. Sabaliauskaite G, Mathur AP. Aligning cyber-physical system safety and security. In: Cardin M-A, Krob D, Lui PC, Tan YH, Wood K, editors. Complex systems design and management Asia. Cham: Springer International Publishing; 2015. p. 41–53. https://doi.org/10.1007/978-3-319-12544-2_4.
56. Mahmoud MS, Xia Y. Networked control systems: cloud control and secure control. New York: Butterworth-Heinemann; 2019.
57. Morozov D, Lezoche M, Panetto H. Multi-paradigm modelling of cyber-physical systems. IFAC PapersOnLine. 2018;51:1385–90. https://doi.org/10.1016/j.ifacol.2018.08.334.
58. Cobos Méndez R, de Oliveira Filho J, Dresscher D, Broenink J. A bond-graph metamodel:: physics-based interconnection of software components, lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). 12018 LNCS. 2020. p. 87–105. https://doi.org/10.1007/978-3-030-40914-2_5.
59. Jeon J, Chun I, Kim W. Metamodel-based CPS modeling tool. In: Park JH, Jeong Y-S, Park SO, Chen H-C, editors. Embedded and Multimedia computing technology and service. Dordrecht: Springer; 2012. p. 285–91. https://doi.org/10.1007/978-94-007-5076-0_33.
60. Mezhuyev V, Samet R. Geometrical meta-metamodel for cyber-physical modelling. In: 2013 international conference on cyberworlds. 2013. p. 89–93. https://doi.org/10.1109/CW.2013.14.
61. Tavčar J, Duhovnik J, Horváth I. From Validation of medical devices towards validation of adaptive cyber-physical systems. J Integr Des Process Sci. 2020;23:37–59. https://doi.org/10.3233/JID190008.
62. Cossentino M, Lopes S, Renda G, Sabatucci L, Zaffora F. A Metamodel of a Multi-Paradigm Approach to Smart Cyber-Physical Systems Development. In WOA. 2019. pp. 35–41.
63. Yilma BA, Panetto H, Naudet Y. A meta-model of cyber-physical-social system: the CPSS paradigm to support human-machine collaboration in industry 4.0. IFIP Adv Inf Commun Technol. 2019;568:11–20. https://doi.org/10.1007/978-3-030-28464-0_2.
64. Baar T. A metamodel-based approach for adding modularization to KeYmaera's input syntax, lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). 11964 LNCS. 2019. p. 125–139. https://doi.org/10.1007/978-3-030-37487-7_11.
65. Fatehah M, Mezhuyev V. Design and process metamodels for modelling and verification of safety-related software applications in smart building systems. ICIT 2018: Proceedings of the 6th International Conference on Information Technology: IoT and Smart City. 2018. pp. 60-64. https://doi.org/10.1145/3301551.3301577.
66. Alrimawi F, Pasquale L, Mehta D, Nuseibeh B. I've seen this before: Sharing cyber-physical incident knowledge. 2018 IEEE/ACM 1st International Workshop on Security Awareness from Design to Deployment (SEAD). Gothenburg, Sweden: 2018. pp. 33-40. https://doi.org/10.1145/3194707.3194714.
67. Merschak S, Hehenberger P, Witters M, Gadeyne K. A hierarchical meta-model for the design of cyber-physical production systems. 2018 19th International Conference on Research and Education in Mechatronics (REM). Delft, Netherlands: 2018. pp. 36-41. https://doi.org/10.1109/REM.2018.8421784.
68. Huang P, Jiang K, Guan C, Du D. Towards modeling cyber-physical systems with SysML/MARTE/pCCSL. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Tokyo, Japan: 2018. pp. 264-269. https://doi.org/10.1109/COMPSAC.2018.00042.
69. Zhang M, Selic B, Ali S, Yue T, Okariz O, Norgren R. Understanding uncertainty in cyber-physical systems: a conceptual model, lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics, 9764. 2016; p. 247–64. https://doi.org/10.1007/978-3-319-42061-5_16.
70. Athinaiou M, Mouratidis H, Fotis T, Pavlidis M, Panaousis E. Towards the definition of a security incident response modelling language, lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). 11033 LNCS. 2018. p. 198–212. https://doi.org/10.1007/978-3-319-98385-1_14.
71. Zhao Y, Rao Y. A CPS-based intelligence-awareness platform for IT service management. 2017. p. 6668–73. https://doi.org/10.1109/CAC.2017.8243978.
72. Carmen Cheh, Ken Keefe, Brett Feddersen, Binbin Chen, William G. Temple, and William H. Sanders. 2017. Developing Models for Physical Attacks in Cyber-Physical Systems. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS '17). Association for Computing Machinery, New York, NY, USA, 49–55. https://doi.org/10.1145/3140241.3140249.
73. M. Tuo, X. Zhou, G. Yang and N. Fu, "An Approach for Safety Analysis of Cyber-Physical System Based on Model Transformation," 2016 IEEE International Conference 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), Chengdu, China, 2016, pp. 636-639. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.140.
74. Islam N, Azim A. Feature characterization for CPS software reuse. In: Proceedings of the 10th ACM/IEEE international conference on cyber-physical systems, association for computing machinery. 2019; Montreal. p. 314–15. https://doi.org/10.1145/3302509.3313318.
75. J. Liu and L. Zhang, "QoS Modeling for Cyber-Physical Systems Using Aspect-Oriented Approach," 2011 Second International Conference on Networking and Distributed Computing, Beijing, China, 2011, pp. 154-158. https://doi.org/10.1109/ICNDC.2011.38.
76. Iglesias-Urkia M, Iglesias A, López-Davalillo B, Charramendieta S, Casado-Mansilla D, Sagardui G, Urbieta A. TRILATERAL: a model-based approach for industrial CPS—monitoring and control. Communications in computer and information science. 1161 CCIS. 2020. p. 376–398. https://doi.org/10.1007/978-3-030-37873-8_16.
77. Matt Bunting and Jonathan Sprinkle. 2019. A meta-metamodel for dynamic constraint feedback in modeling languages. In Proceedings of the 17th ACM SIGPLAN International Workshop on Domain-Specific Modeling (DSM 2019). Association for Computing Machinery, New York, NY, USA, 11–19. https://doi.org/10.1145/3358501.3361239.
78. Smarsly, K., Fitz, T., & Legatiuk, D. (2018). Metamodeling Wireless Communication in Cyber-Physical Systems. In EG-ICE.
79. Zhang H, Liu J, Kato N. Threshold tuning-based wearable sensor fault detection for reliable medical monitoring using Bayesian network model. IEEE Syst J. 2018;12:1886–96. https://doi.org/10.1109/JSYST.2016.2600582.
80. M. Walch, "Knowledge-driven enrichment of cyber-physical systems for industrial applications using the KbR modelling approach," 2017 IEEE International Conference on Agents (ICA), Beijing, China, 2017, pp. 84-89. https://doi.org/10.1109/AGENTS.2017.8015307.
81. Smarsly K, Theiler M, Dragos K. IFC-based modeling of cyber-physical systems in civil engineering. 2017. p. 269–78.
82. Wang J, Abid H, Lee S, Shu L, Xia F. A secured health care application architecture for cyber-physical systems. arXiv:1201.0213 [Cs]. 2011. http://arxiv.org/abs/1201.0213. Accessed 19 May 2020.
83. Cao X, Cheng P, Chen J, Sun Y. An online optimization approach for control and communication codesign in networked cyber-physical systems. IEEE Trans Ind Inf. 2013;9:439–50. https://doi.org/10.1109/TII.2012.2216537.
84. Sampigethaya K, Poovendran R. Aviation cyber-physical systems: foundations for future aircraft and air transport. Proc IEEE. 2013;101:1834–55. https://doi.org/10.1109/JPROC.2012.2235131.
85. Banerjee A, Kandula S, Mukherjee T, Gupta SKS. BAND-AiDe: a tool for cyber-physical oriented analysis and design of body area networks and devices. ACM Trans Embed Comput Syst. 2012;11:49:1-49:29. https://doi.org/10.1145/2331147.2331159.
86. Xiong G, Zhu F, Liu X, Dong X, Huang W, Chen S, Zhao K. Cyber-physical-social system in intelligent transportation. IEEE/CAA J Autom Sin. 2015;2:320–33. https://doi.org/10.1109/JAS.2015.7152667.
87. Wan J, Chen M, Xia F, Di L, Zhou K. From machine-to-machine communications towards cyber-physical systems. Comput Sci Inf Syst. 2013;10:1105–28.
88. Leitão P, Colombo AW, Karnouskos S. Industrial automation based on cyber-physical systems technologies: prototype implementations and challenges. Comput Ind. 2016;81:11–25. https://doi.org/10.1016/j.compind.2015.08.004.
89. Eyisi E, Zhang Z, Koutsoukos X, Porter J, Karsai G, Sztipanovits J. Model-based control design and integration of cyberphysical systems: an adaptive cruise control case study. J Control Sci Eng. 2013;2013: e678016. https://doi.org/10.1155/2013/678016.
90. Lai C-F, Ma Y-W, Chang S-Y, Chao H-C, Huang Y-M. OSGi-based services architecture for cyber-physical home control systems. Comput Commun. 2011;34:184–91. https://doi.org/10.1016/j.comcom.2010.03.034.
91. Sangiovanni-Vincentelli A, Damm W, Passerone R. Taming Dr. Frankenstein: contract-based design for cyber-physical systems. Eur J Control. 2012;18:217–38. https://doi.org/10.3166/ejc.18.217-238.
92. Sztipanovits J, Koutsoukos X, Karsai G, Kottenstette N, Antsaklis P, Gupta V, Goodwine B, Baras J, Wang S. Toward a science of cyber-physical system integration. Proc IEEE. 2012;100:29–44. https://doi.org/10.1109/JPROC.2011.2161529.
93. Sampath Kumar VR, Shanmugavel M, Ganapathy V, Shirinzadeh B. Unified meta-modeling framework using bond graph grammars for conceptual modelling. Robot Auton Syst. 2015;72:114–30. https://doi.org/10.1016/j.robot.2015.05.003.
94. Bagheri B, Yang S, Kao H-A, Lee J. Cyber-physical systems architecture for self-aware machines in industry 4.0 environment. IFAC PapersOnLine. 2015;28:1622–7. https://doi.org/10.1016/j.ifacol.2015.06.318.
95. Dillon TS, Zhuge H, Wu C, Singh J, Chang E. Web-of-things framework for cyber-physical systems. Concurr Comput Pract Exp. 2011;23:905–23. https://doi.org/10.1002/cpe.1629.
96. Hu F, Lu Y, Vasilakos AV, Hao Q, Ma R, Patil Y, Zhang T, Lu J, Li X, Xiong NN. Robust cyber-physical systems: concept, models, and implementation. Futur Gener Comput Syst. 2016;56:449–75. https://doi.org/10.1016/j.future.2015.06.006.
97. Luis E. Salazar and Alvaro A. Cardenas. 2019. Enhancing the Resiliency of Cyber-Physical Systems with Software-Defined Networks. In Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC'19). Association for Computing Machinery, New York, NY, USA, 15–26. https://doi.org/10.1145/3338499.3357356.
98. P. Buason, H. Choi, A. Valdes and H. J. Liu, "Cyber-Physical Systems of Microgrids for Electrical Grid Resiliency," 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 2019, pp. 492-497. https://doi.org/10.1109/ICPHYS.2019.8780336.
99. Potteiger B, Zhang Z, Koutsoukos X. Integrated moving target defense and control reconfiguration for securing cyber-physical systems. Microprocess Microsyst. 2020. https://doi.org/10.1016/j.micpro.2019.102954.
100. Zhang M, Ali S, Yue T, Norgren R, Okariz O. Uncertainty-wise cyber-physical system test modeling. Softw Syst Model. 2019;18:1379–418. https://doi.org/10.1007/s10270-017-0609-6.
101. A. Bin Masood, H. K. Qureshi, S. M. Danish and M. Lestas, "Realizing an Implementation Platform for Closed Loop Cyber-Physical Systems Using Blockchain," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 2019, pp. 1-5. https://doi.org/10.1109/VTCSpring.2019.8746372.
102. Mussard-Afcari Y, Rawat DB, Garuba M. Y. Mussard-Afcari, D. B. Rawat and M. Garuba, "Data Validation and Correction for Resiliency in Mobile Cyber-Physical Systems," 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2019, pp. 1-4. https://doi.org/10.1109/CCNC.2019.8651853.
103. Sierla S, O'Halloran BM, Karhela T, Papakonstantinou N, Tumer IY. Common cause failure analysis of cyber-physical systems situated in constructed environments. Res Eng Des. 2013;24:375–94. https://doi.org/10.1007/s00163-013-0156-2.

104. Wan K, Alagar V. Context-aware security solutions for cyber-physical systems. Mob Netw Appl. 2014;19:212–26. https://doi.org/10.1007/s11036-014-0495-x.
105. Kantarci B. Cyber-physical alternate route recommendation system for paramedics in an urban area. In: 2015 IEEE wireless communications and networking conference (WCNC). 2015. p. 2155–2160. https://doi.org/10.1109/WCNC.2015.7127801.
106. Wiesner S, Marilungo E, Thoben K-D. Cyber-physical product-service systems—challenges for requirements engineering. Int J Autom Technol. 2017;11:17–28. https://doi.org/10.20965/ijat.2017.p0017.
107. Mo Y, Sinopoli B. Integrity attacks on cyber-physical systems. In: Proceedings of the 1st international conference on high confidence networked systems, association for computing machinery. Beijing, China; 2012. p. 47–54. https://doi.org/10.1145/2185505.2185514.
108. Burmester M, Magkos E, Chrissikopoulos V. Modeling security in cyber–physical systems. Int J Crit Infrastruct Prot. 2012;5:118–26. https://doi.org/10.1016/j.ijcip.2012.08.002.
109. Smart Systems and Cyber Physical Systems paradigms in an IoT and Industry/ie4.0 context, (n.d.). https://scholar.googleusercontent.com/scholar?q=cache:8NNXnBZaMc8J:scholar.google.com/+Smart+Systems+and+Cyber+Physical+Systems+paradigms+in+an+IoT+and+Industry/ie4.+0+context&hl=en&as_sdt=0,5. Accessed 30 June 2020.
110. Boyes HA. Trustworthy cyber-physical systems—a review (2013) 31. https://doi.org/10.1049/cp.2013.1707.
111. Ratasich D, Platzer M, Grosu R, Bartocci E. D. Ratasich, M. Platzer, R. Grosu and E. Bartocci, "Adaptive Fault Detection Exploiting Redundancy with Uncertainties in Space and Time," 2019 IEEE 13th International Conference on Self-Adaptive and Self-Organizing Systems (SASO), Umea, Sweden, 2019, pp. 23-32. https://doi.org/10.1109/SASO.2019.00013.
112. G. Na, J. Park and Y. Eun, "Attack Resilient State Estimation by Sensor Output Coding," 2019 19th International Conference on Control, Automation and Systems (ICCAS), Jeju, Korea (South), 2019, pp. 1015-1020. https://doi.org/10.23919/ICCAS47443.2019.8971675.
113. A. A. Jahromi, A. Kemmeugne, D. Kundur and A. Haddadi, Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes. In IEEE Transactions on Power Systems 2020;35(1):440-450. https://doi.org/10.1109/TPWRS.2019.2924441.
114. F. Y. Chemashkin and A. A. Zhilenkov, "Fault Tolerance Control in Cyber-Physical Systems," 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, Russia, 2019, pp. 1169-1171. https://doi.org/10.1109/EIConRus.2019.8656639.
115. B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-purry and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR), Charleston, SC, USA, 2015, pp. 1-6. https://doi.org/10.1109/CQR.2015.7129084.
116. Wu, M, & Moon, YB. "Intrusion Detection of Cyber-Physical Attacks in Manufacturing Systems: A Review." Proceedings of the ASME 2019 International Mechanical Engineering Congress and Exposition. Volume 2B: Advanced Manufacturing. Salt Lake City, Utah, USA. November 11–14, 2019. V02BT02A001. ASME. https://doi.org/10.1115/IMECE2019-10135.
117. Lee C, Shim H, Eun Y. On redundant observability: from security index to attack detection and resilient state estimation. IEEE Trans Autom Control. 2019;64:775–82. https://doi.org/10.1109/TAC.2018.2837107.
118. Dyka Z, Kabin I, Langendorfer P. Researching resilience a holistic approach. 2019. Z. Dyka, I. Kabin and P. Langendörfer, "Researching Resilience a Holistic Approach," 2019 IEEE East-West Design & Test Symposium (EWDTS), Batumi, Georgia, 2019, pp. 1-4. https://doi.org/10.1109/EWDTS.2019.8884447.
119. Laszka, A., Abbas, W., Vorobeychik, Y., & Koutsoukos, X.D. (2018). Synergistic Security for the Industrial Internet of Things: Integrating Redundancy, Diversity, and Hardening. 2018 IEEE International Conference on Industrial Internet (ICII), 153-158.
120. Colombo A, Karnouskos S, Kaynak O, Shi Y, Yin S. Industrial cyberphysical systems: a backbone of the fourth industrial revolution. IEEE Ind Electron Mag. 2017;11:6–16. https://doi.org/10.1109/MIE.2017.2648857.
121. Kopetz H. Real-time systems: design principles for distributed embedded applications. Berlin: Springer Science & Business Media; 2011.
122. Poledna S. Fault-tolerant real-time systems: the problem of replica determinism. Berlin: Springer Science & Business Media; 2007.
123. Ntalampiras S. Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling. IEEE Trans Ind Inf. 2015;11:104–11. https://doi.org/10.1109/TII.2014.2367322.
124. Bakirtzis G, Sherburne T, Adams S, Horowitz BM, Beling PA, Fleming CH. An ontological metamodel for cyber-physical system safety, security, and resilience coengineering. arXiv:2006.05304 [Cs]. (2020). http://arxiv.org/abs/2006.05304. Accessed 18 June 2020.