PalArch's Journal of Archaeology of Egypt / Egyptology

Security and Safety of Industrial Cyber-Physical System: Systematic Literature Review

[1]*Haqi Khalid*, [2]*Shaiful Jahari Hashim*, [3]*Sharifah Mumtazah Syed Ahmad*, [4]*Fazirulhisyam Hashim*, [5]*Muhammad Akmal Chaudhary*

[1,2,3,4] Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, Serdang, Malaysia
[5] Department of Electrical & Computer Engineering, College of Engineering & Information Technology, Ajman University, Ajman, 346, United Arab Emirates Affiliation
E-mail: haqikhalid1@gmail.com, sjh@upm.edu.my, s_mumtazah@upm.edu.my, fazirul@upm.edu.my, m.akmal@ajman.ac.ae.

Haqi Khalid, Shaiful Jahari Hashim, Sharifah Mumtazah Syed Ahmad, Fazirulhisyam Hashim, Muhammad Akmal Chaudhary: Security and Safety of Industrial Cyber-Physical System: Systematic Literature Review -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x

Keywords: Security and Safety, Industrial Cyber-Physical System

ABSTRACT

The Cyber-Physical Systems (CPS) are complicated networked systems which comprise of computing and communicating cyber components and interact closely with physical components, such as sensors and actuators. The integration of CPS, on the other hand, presents additional threats that might be catastrophic for society. However, this study intends to examine the efforts of researchers in response to CPS-based current industrial applications ' new and harmful tech, map the literature-based research landscape, and determine the essential features of this growing research. This research also examines the desire behind the use of Cyber-physical systems in various industrial environments and the Open challenges that negatively affect this technology's usefulness. The study of this offers the use of Cyber-Physical System / Industrial CPS valuable recommendations by designers/developers, researchers, and industries/factories. Finally, the whole study contributes to this field of research by offering a comprehensive description of options and issues that will enable other researchers and participants to further improve the cyber-physical framework, which outlines the new directions for this research.

1. Introduction

The aim of Cyber-Physical Systems (CPS) is to combine computer services with physical methods to provide reliable and intelligent services. In the

meantime, CPS is distributed and hybrid real-time dynamic systems, which run on several loops at various time and space scales with different application degrees [1]. The definition of a 'system of cooperation entities with computation capacities with an intense relation to physical environment and the physical phenomena around them, all of which use and supply network data transmission and processing services.' Apart from smart factories, various CPS-based applications, for example healthcare, smart grid, smart transportation, intelligent homes, etc. In order to enhance the monitoring and control capability of the physical system (equipment development and workflow, cyber and physical areas integration, however, greatly decreases external isolation of the physical system and increases its vulnerability, resulting in a variety of cyber security concerns. Transmission and generation of an electrical network, etc.) cyber-physical systems like smart grid [2] of modern information communication technology (computation, control, commu nication, etc.) can be used. However, in some of the last decade's most popular security breaches, CPSs have been key targets for this. CPS can neither be protected by cyber nor by physical concepts of security alone as the cross-over effect could bring unusual vulnerabilities;

The device information system can be damaged or disrupted by physical attacks and cyber attacks can cause material failures. With the many important applications in which CPSs are used, an attack can have dire effects in the real world [3]–[6]. As standard I-IoT CPS, the I-IoT consists of two principal components: cyber and physical systems and involves the industrial systems' service, communication and intelligence infrastructure. Physical systems are systems used to carry out specified manufacturing and automation roles by industrial equipment [2]. As ICPS is an essential part of the free economy, any malicious uprising may have disastrous consequences on human safety, the environment and property [7]. Consequently, security and confidentiality must be of vital importance in the configuration, design and operation of the CPS. Many security technologies, for instances, used various technologies such as: (fault tolerant, IDS, ADS and various security and privacy technologies, have therefore been implemented to protect, monitor and provide excellent quality of service and security in many areas, including smart cities / building and factories. The aim of the paper is to clarify the research efforts previously noted in response to emerging and problem technology and to map the literature research landscape into a consolidated taxonomy and determine its essential characteristics and explain in detail the new direction of research. The rest of this paper has been structured accordingly. Section 2 introduces the Systematic Literature Review (SLR) method. Section 3 provides key SLR results from a more general perspective and a more specific perspective — the analysis of keywords and source journals. Section 4 provides insights from the SLR based on these results and defines open challenges and recommendations for research CPS. Part 5 ends with this work and discusses its limitations.

2. Research methodology

Cyber-physical system is the keyword of the area covered by this paper. Non-security systems, such as manufacturing equipment, workflow, transmission and generation of electrical networks are exempt from our cyber-physical system search. We also look at all cyber physical systems in the field of security and research applications that restrict our reach to English.

A. Source

The authors conducted a full survey to identify the best and most accurate databases for all papers relating to a cyber-physical system. Such as (1) The IEEE Xplore Technical Literature Library of Engineering and Technology, (2) The Web of Science Service (WoS) indexing underdisciplined science, social sciences, art and science (3) SpringerLink allows authors to access one million scientific resources (4) Science Direct Database, which provides access to article science, technical and medical journals. This selection encompasses the modern cyber physics and technical literature and gives a wide range of disciplines a broad overview of researchers ' efforts.

B. The Procedure of Study Selection

Includes the selection procedure of the studies concerned by searching literature sources with two iterations: screening and filtering. By scanning titles and abstracts, duplicates and irrelevant items were excluded from the first iteration. The second iteration filtered the papers after reading the full text of the papers. Both iterations used the same criterion for eligibility.

C. Search

Research was carried out on search engines (e.g. ScienceDirect, IEEE Xplore, SpringerLink, and WoS) from early 2012 to 2020. Several keywords in the search boxes have been entered. We have used a mixture of keywords with the terms: the 'Applied Industrial,' '\ Industrial Techniques,' '\cyber physical system,' '\CPS, '\industrial cyber-physical system and '\ICPS in different variants, combined with \OR' operator. In Figure 1, the exact query text is shown.

3. Existing studies

As shown in Figure 3, we followed the above models, took the general categories of articles and refinement of the literary taxonomy classification. The first search was conducted in 113 articles from 2012–2019: ScienceDirect's 34 articles, IEEE's 40 papers, 26 SpringerLink articles, and WoS ' 13 articles. All four libraries had just eight items duplicating them. Thirty-eight other articles produced in 71 papers After the titles and abstracts are scanned have been removed. Thirteen other papers were omitted in complete reading. 58 materials from this final collection have been read extensively for the creation of a general plan of the research on this new subject. Of the 58 papers, 4 (2.32 per cent) consisted of analyses and surveys of cyber-physical security technologies or literature detailing the CPS for particular data protection or other illnesses or providing a summary of the technology in general. Secondly, 54 (97.68%) articles were focused on

applying different security applications on the cyber-physical system. This section contains 6 out of 54 articles related to smart cities and buildings, 6 out of 54 related to intrusion detection (ID). 7 out of 54 items contains paper related to Anomaly detection (AD), the section of fault-tolerant includes seven papers. 14 articles were related to security and privacy in CPS, and four reports contain other applications of CPS. As shown in Figure 2, we followed the above models, took the general categories of articles and refinement of the literary taxonomy classification.

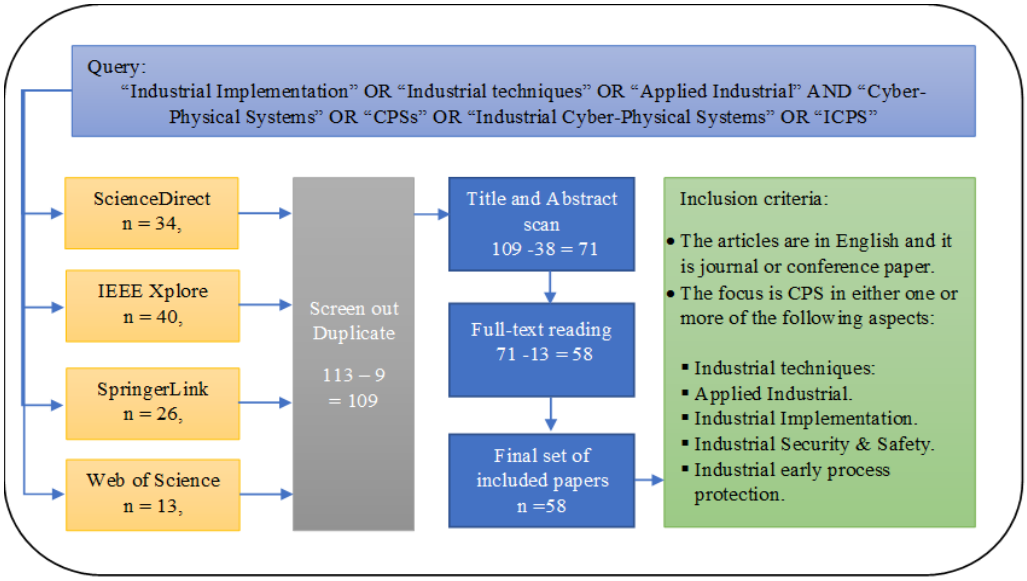

Figure 1. *Study selection flowchart that includes search queries and criteria for inclusion.*

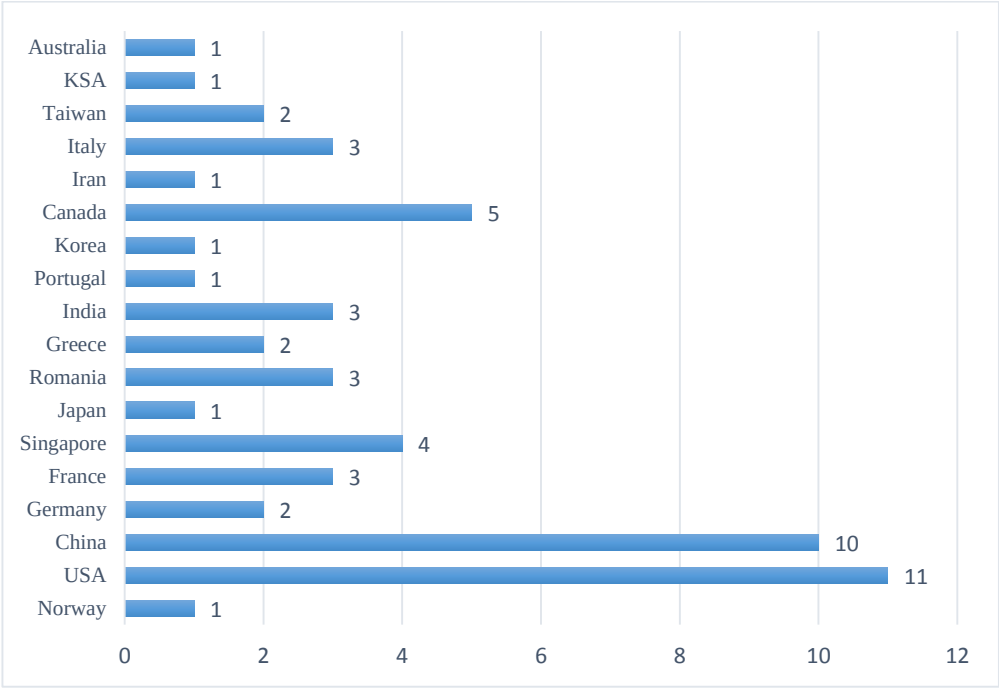

Figure 2. *The number of included articles based on countries of origin.*

A. Survey and Review

Where a cyber-attack had in the past been mainly concerned with information collection or authorization, this network and system has recently been paralyzed and even destroyed. In the future, cyber-attacks are anticipated to be prevented, and cyber measures are expected to be aggressive and active [1]. The primary goal of a cyber-physical system review or survey paper is to understand current ideas in this field and to justify further research on related topics overlooked or undervalued. Of the 58 articles selected, 4 (2,32 percent) have been reviewed and surveyed. The literature on Cyber-Physical Systems (CPS) has increased over the last few years. The existing CPS research body has been thoroughly surveyed. I-IoT architecture, I-IoT application, and its characteristics (i.e., factory automation, process automation). Consider the existing research efforts of three essential control, networking, and computing system aspects. Concerning monitoring, industrial control systems are initially categorized, and recent and relevant research efforts are then presented in [2]. There has been a considerable publication of literature on [8].

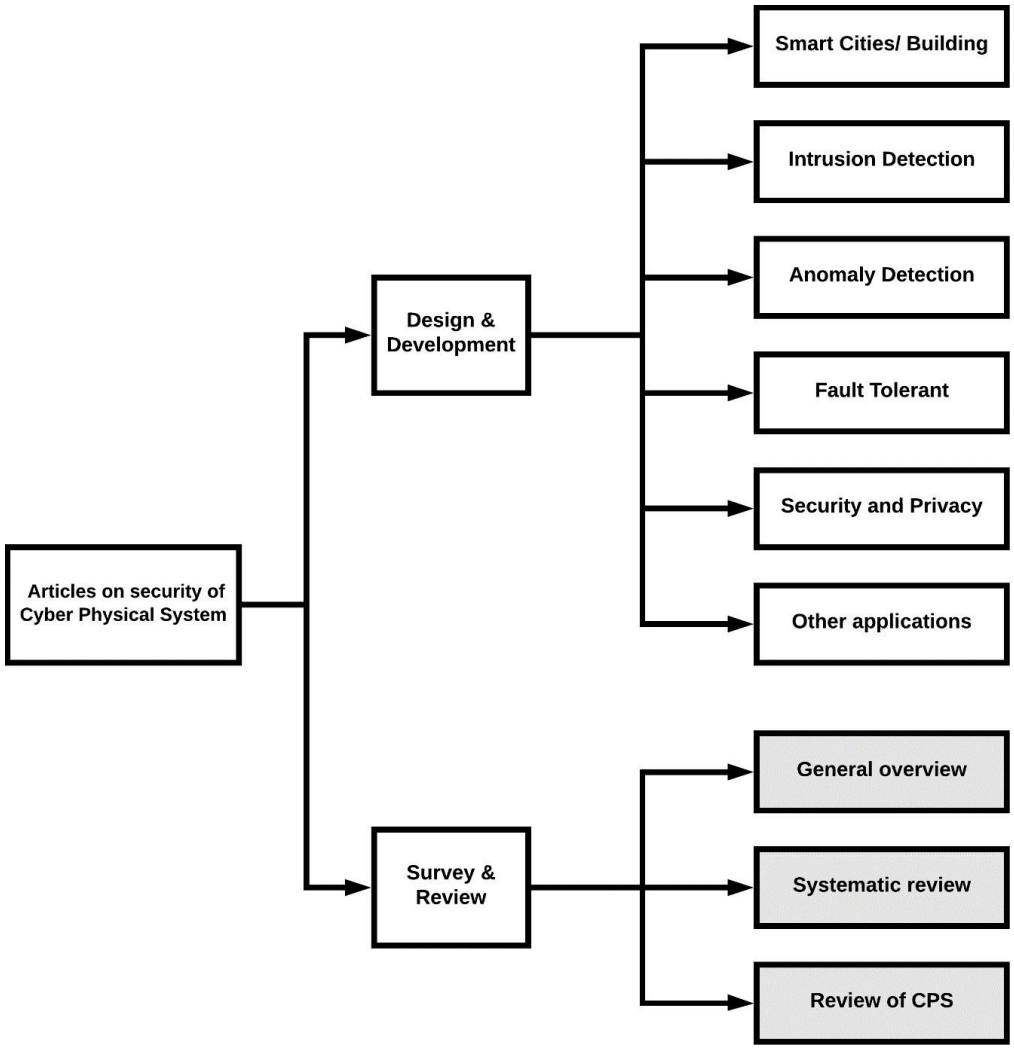

Figure 3. Taxonomy of research literature on Cyber-Physical System (CPS).

These studies analysed the findings of a comprehensive mapping study of modern cyber-physical systems engineering (MBSE4CPS) models. The findings could provide some insight into an evolving research area that is interdisciplinary in research, such as system engineering, software engineering, and security technologies. In particular, the study has been developed and performed on the basis of a stringent SMS protocol in order to identify three major MBSE4CPS studies and answer the relevant general questions.

CPS and IP integration have weaknesses and strengths, as has been shown in [9]. Their combination is advantageous for many industrial scenarios. Two real industrial examples, namely the manufacturer of trains (Bombardier) and the manufacturer of washing machines (Whirlpool) are presented which cover the different phases of the product life cycle, demonstrating the strengths and weaknesses in CPS and IP, two revolutionary concepts. A new risk measure by modifying existing methods for estimating risk and uncertainties identifies several major challenges in the estimation of the economic effect of IT cyber risk [10]. The research integrates requirements and management of Industry 4.0 and provides an improved understanding of models I-4.0 for economic impact

assessments. The paper [11], Presents aspects of the emerging industrial cyber-physical system (ICPSs) era, highlight highly successful programs and countrywide activities, and present essential challenges.
Figure 2 shows the geographical distribution of industrial CPS, and CPS Number and percentage applications show the furthermost creative authors are from the USA with 11 case studies, followed by China with 10 case studies, Canada with 5 case studies, Singapore with 4 case studies, Korea with 13 case studies, Italy, France, India, and Romania with 3 case studies each. Taiwan, Greece, and Germany with 2 case studies. Australia, KSA, Iran, Korea, Portugal, Japan, and Norway with 1 case study each.

B. Statistical Findings of CPS

The term "cyber-physical system" implies a new generation of computer and physical systems which can communicate in various specific ways with people. Future technological developments are crucial for the ability to communicate with and extend physical world capacities via computation, communication, and management. Research opportunities and challenges include the creation of next-generation aircraft, space vehicles, hybrid gas-electric vehicles, fully independent urban driving, and prostheses which permit brain signals to control items [12]. Over the years, system and control technical experts have developed potent science and engineering methods and tools such as time and frequency domain techniques, state-space analysis , system detection, filtering, estimation, optimization, robust control and stochastic monitoring. In the interim, computer scientists are dramatically advancing in new programming languages, in real-time computation, visualization, compiler design, embedded systems and computer applications, and innovative approaches to ensuring computer system reliability, cyber security and failure tolerance. Computer scientists also developed a range of potent formalities and verification tools for modeling [12]–[14]. Cyber-physical systems research seeks to integrate input information and engineering concepts in all areas (network, controls and software, human interaction, learning theory, electrical , mechanical, chemical, biomedical, materials and other fields in engineering) in order to establish new science and technology supporting CPS [14]. We provide the popular categories that used based on the cyber-physical system, followed by the explanation of each type, such as (middleware, Smart Factory, Smart Grid, Privacy Preserving, Fault tolerant, and intuition detection).

1. Middleware

The Internet of Things (IoT) and cyber-physical systems (CPS) technology can be used in many fields of use. Smart garden, intelligent transport, energy, smart home and smart city buildings, are an example. Some of these application domains, like smart home systems and smart transport systems, have been extensively explored. In this section, we provide some of the presented methods of smart cities and building in the cyber-physical. The Cyber-physical systems (CPS) are complicated networked systems which comprise of computing and communicating cyber components and interact closely with

physical components, such as sensors and actuators. The integration of CPS, on the other hand, presents additional threats that might be catastrophic for society. However, this study intends to examine the efforts of researchers in response to CPS-based current industrial applications ' new and harmful tech, map the literature-based research landscape, and determine the essential features of this growing research. This research also examines the desire behind the use of the Cyber-physical system in various industrial environments and the Open challenges that negatively affect this technology's usefulness. The study of this offers the use of Cyber-Physical System / Industrial CPS valuable recommendations by designers/developers, researchers, and industries/factories.

In recent years, [1], The development and challenges of the smart buildings and cities CPS / IoT application in five topics have been studied. They are middleware, computer model, failure tolerance, data quality, and virtual worktime. The Study of [14], Proposed a framework for coordination and integration supporting smart transport operations every day in intelligent cities in connection with the Internet of Things. It also examined the operating of these pillars and how they can be used to deliver integrated smart transport systems. It can formalize different aspects of the cyber policy and the physical system in graphic form. Secondly, identify challenges for the proposed graph-based designs introduced by extending traditional algorithms to the CPS presented in [13]. Data driven energy efficiency control strategies for smart buildings such as cyber-physical systems by examining new works and putting them in context with the current and advanced inter-related topics presented in [15] such data processing, building automation and distributed control. Furthermore, [16], Propose an early assessment modeling strategy for the performance of Cyber-Physical Systems Photovoltaic Array (PV) in the smart cities. The accuracy and efficiency of the proposed model have been tested. A new, non-intrusive and integrated middleware based on open source building management software for cities of the future is introduced [17].

2. Intrusion Detection

The IDS is a firewall for data encryption and other conventional security measures protecting the privacy of emerging technologies [18]. Though, Cyber-Physical System (CPS) is one of the techniques using Intrusion Detection in a particular application. This section will mainly focus on the intrusion detection correlation with CPS's. Speaking of IDS, [18], Focuses on ID techniques and proposed a new attack / defense game model of malicious nodes with the multi-game approach. Develop a three-phase methodology to reduce the intrusion detection system (IDS) complexity, and the cost provided by emerging Industry 4.0 systems is presented in [19]. In the study of [20], the CUSUM algorithm is proposed to counteract a new detection policy and abnormal behavior control, as well as DoS attacks. A new CPS intrusion detection system (called SIDS) was introduced in [21]. SIDS detects three types of abnormalities (attacks): abnormal conditions, abnormal transitions between standard laws, and unusual periods between normal changes. A

scholar of [22], Proposes a new distributed blind intrusion detection model by designing the graph signal target measurements, utilizing the graph-signal statistical characteristics to detect the intrusion. Another work [23], Presents classification and survey of specially built and tested vehicle and vehicle network intrusion detection systems. Its aim is to help the industry recognize current methods, their advantages and drawbacks and to recognize literary holes in future study, which are attractive and important.

3. Anomaly Detection

Anomaly detection has been widely studied in ICPSs, both in the cyber-and physical domain in recent years. The focus of cyber domain analysis is primarily on traffic analysis, protocols, comportments, etc. using statistical, model-based, machine-learning, methods, etc. [24]. Lately, [25] It proposes the application of an outlier detection method in the CPS log and evaluation by analysis of outliers detected in an aquarium management system of the usefulness of the technique. It also recognizes several important events, like mutual exclusion failures, unexpected reboots, and single-purpose failures.
Besides, [26], Proposes an unmonitored approach for the detection of anomalies in the CPS area. It also leads to the fact that attacks occurring in other processes can be detected between themselves through experiments.
The paper also contributes to the development of a cross-layer anomaly sensor system (ADS) for ICPS, to deduce the status of the system, to fuse evidence from a variety of monitored parameters and to implement a complete and scalable detection system introduced in [27]. The paper of [28], Present an on-line monitoring system (Illiad), that model the CPS status in relation to their inter-relationship between the components by combining model-based approaches (Kalman philtre) with data-driven approaches to improve the status representation of the controlled system (self-regression and latent factor-based approaches). A zone partition-based anomaly detection approach is for the ICPSs presented in [24]. An algorithm for the zone partition is designed to divide physical environments into many areas. A zone function is extracted for observing key states in each region. Anomaly detection countermeasures in CPSs based on Transfer-Entropy are introduced in [29]. For sensors and innovation sequences, the data-driven evaluation can be carried out without relying on the dynamic system model.
Last but not least, [30], Orpheus, a new CPS control program security system in defense against data-based attacks, was first introduced. Secondly, the *eFSA* model of program behavior, which promotes state of the art modeling of programmed, was proposed. Thirdly, to demonstrate the feasibility of an approach implemented a prototype of proof of concept.

4. Fault-Tolerant

Fault tolerance can be described as a property that enables a device to continue to operate properly if any of their components fail. Fault tolerance in critical systems is particularly requested, making it an important feature of CPS, where

failure can cause a complete system breakdown for some components. [31], [32].

Latterly, it Presents a new CPPS semantic fault detection framework that combines model analyses and semantic data analysis with the reasoning of a given domain model and faults prognostic fault network through a formal compliance analysis with timed hybrid automatic analyses [33]. The work of [34], describes a modular HILS Field Programmable Gate Array (FPGA) modular framework for mechanical systems capable of injecting sensor malfunction and deploying cyber-physical system (CPS) attacks. The model for describing a cyber-physical sensor model representing sensors and actuators and creating virtual objects for the regeneration of data in the absence of the physical devices presented in [35]. The algorithm for data regeneration is based on the virtual facility attributed to contexts of the physical methods used. Additionally,[32], Present a proposal that uses robust fractional controls for a cryogenic cascade separating column to build an architecture with multi-agent fault tolerant control. A highly critical cyber physical device to achieve an efficient, fault-tolerant control of the isotope separation cascade. In [36], A fast control failure recovery mechanism was proposed by authors for a fault-tolerant CPS using SDN with multiple controllers. The primary and backup controls have been enabled to utilize the same IP address. A fault-tolerating resource-cost-aware design technique for end-to-end computation for functional security on ACP Screen Cyber Systems presented in [37].

5. Security and Privacy

Security innovative and valuable cyber-physical systems (CPSs) services is a critical factor in developing. In recent years, the CPS security research sector, which deals with the development of various architectures, security protocols and political models, has received considerable attention. However, in addition to data publication surveillance, CPSs can provide management related services and the required finer and versatile model of access control remains challenging due to its criticality and feasibility [3], [6], [38]. This section will be describing the security and the privacy of the cyber-physical system, and the latest research works have chosen. The authors of [3], In terms of security, privacy and implementation in the evolving CPS domain, all the classic principles from both cyber and physical domains have been established. It demonstrates how interactions between systems of both types mean that security and privacy across the entire infrastructure are needed. The report shows numerous safety and privacy criteria between infrastructural and personal CPS. A classification in CPS fields, threats, defence, developments in science, network security, safety level growth and computer strategies that makes this survey a unique item and, I think, very helpful provided in [4]. In [39], presented a summary of the essential features of cyber-physical networks, infrastructure, security problems and attacks. A typical Lateral Channel attacks with countermeasures the implementation of cryptographic algorithms (symmetric: AES, asymmetric: RSA).

Additionally,[40], examines CPSS's privacy preservation problem, which inherits cyber-physical and social network features and faces novel privacy issues. The privacy issues in physical data will be dealt with thoroughly and with a useful utility as in social networks. A reliable CPS data source architecture and use a block-chain to protect data integrity and detect disturbance introduced in [41]. A minimum information exposure attribute-based verification is used for the conservation of privacy, especially for unique CPS business-driven scenarios. In [6], the authors deal with problems of security and privacy in cyber-physical systems and IoT. Develop a Q-CFA learning algorithm, which works efficiently without prior knowledge in a large order.

On the other hand, [42], emphasis on the urgent need to make a paradigm shift to multi-agent CPS software development. Also, CPS runtime monitoring identifies security violations and attempts by attackers to compromise security and privacy and CPS execution to ensure safety and security. Exploring the role of functional reduction and protection of privacy with CPS data from the ICA technology is presented in [43]. With the technique, high dimensional and sensitive data can be transformed and reduced into representative information without breaking confidential data characteristics. Besides,[44], Data aggregation studied privacy preservation in CPSS. In particular, propose the algorithm that enables an untrusted aggregator to aggregate data about a user's physical environment accurately and efficiently in the premise that privacy is well protected. In [45], Authors provide a systemic basis for further development of CPSs, aimed at providing a research site to explore distributing signal-processing techniques with adaptive, cooperative, and learning skills that protect against cyberattacks and privacy leaks.

Moreover,[46], To protect the data collected by buildings, the PAD Open Source Data Publication System is provided. From PAD's interactions with the data publication system, information of interest is learned by data users, and then processes of data publication are customized for the purposeful use of data. Propose a lightweight privacy and security verification system for the protection of privacy by using FHMT. The model is successful and can maintain integrity and confidentiality, given in [47]. Likewise,[38], Comes

with a variety of IoT-suitable network architectures. They are designed to address specific network requirements by combining different optimization techniques into single network design. Identify threats to the CPS due to the vulnerabilities in the system, discuss recent successful system attacks, problems in system security control, investigate deficiencies and present a number of challenges to improve the security of cyber physics systems is presented in [5]. According to the security of the cyber physical system, many recent research work highlighted the objectives to secure the system [3]–[6], [38], [39]. The main security objectives of the CPS have explained in Figure 4.

Table 1.
Classification of the Proposed Solution, Tools, Datasets, and Validation Metrics

Ref	Method	Tool Used	Dataset (If any)	Evaluation Metrics
[25]	Local Outlier Factor (LOF).	ELKI tool	Aquatan	▪ Failure Rate. ▪ The mixture of anomalous.
[27]	A cross-layer anomaly detection system (ADS).	Matlab/ Modbus/TCP	PROTECT- G	▪ Attack Rate. ▪ Network traffic. ▪ Detection Rate.
[21]	State-based Intrusion Detection System (SIDS).	Matlab/ Modbus/TCP	National Instrument (NI) LabVIEW.	▪ True Positive Rate. ▪ False Positive Rate.
[30]	Orpheus/ event-aware Finite-State Automaton (eFSA)	Prototype (Raspberry Pi+ Sense HAT)	Solard/ SyringePump	▪ Average delay. ▪ Run Time. ▪ Detection Rate.
[48]	Long Short-Term Memory Recurrent Neural Network (LSTM-RNN)/ Cumulative Sum (CUSUM)	XEON server/ SWaT testbed	SWaT Dataset	▪ Attack Rate. ▪ False Positive Rates.
[29]	Transfer-entropy-based causality.	Tennessee-Eastman control	N/A	▪ Detection Rate. ▪ False Positive Rate. ▪ Sensitivity.
[24]	The zone-partition-based anomaly detection approach	Testbed (Coupling Tank Control System (CTCS))	N/A	▪ False Negative Rate. ▪ False Positive Rate.

[28]	Model-based and data-driven strategies	IEEE 33 Bus	Intel Berkeley Research lab/ National Renewable Energy Laboratory Wind Prospector Data Set/ National Solar Radiation Data Base	▪ Energy Consumption. ▪ Detection Rate.
[33]	Model-based analysis and semantic data analysis	3D simulation tools (FlexSim1)/ AJAN/ SPARQL 1.1	SmartFactoryKL	▪ Execution Time. ▪ Behaviour Detection.
[20]	Cumulative Sum (CUSUM) algorithm	Matlab	N/A	▪ Detection Rate. ▪ False Positive Rate. ▪ Detection Rate. ▪ Accuracy Rate.
[18]	The game-theory-based intrusion detection system	Simulation (actual embedded network)	N/A	▪ Energy Consumption. ▪ Detection Rate
[49]	Rough Set Theory and Hyper-clique based Binary Whale Optimization Algorithm (RST-HCBWoA)	WEKA tool	Power system attack dataset	▪ Accuracy. ▪ Reduct Size. ▪ Time Complexity. ▪ Precision. ▪ Recall.
[19]	Embracing sensitivity analysis, Cross-association, and Optimal IDS design	Matlab / AIMMS software/Realistic Vinyl Acetate Monomer (VAM)	N/A	▪ Complexity. ▪ Detection Cost.
[36]	Software-Defined Networking (SDN)	OpenFlow 1.3/ OpenDaylight SDN controller.	N/A	▪ Recovery Time.
[37]	Functional Safety Requirement Verification (FSRV), Resource-Cost-aware Fault-Tolerant Optimization (RCFO)	Simulation (heterogeneous ECU/Java)	N/A	▪ Resource Cost. ▪ Response Time.
[35]	Reinforcement Sensing (RS).	Simulation (Semantics-based meta-modelling)	N/A	▪ Power Consumption. ▪ Cost.
[32]	Fault tolerant multi-agent fractional order control system	Matlab/ MACSimJX	N/A	▪ Complexity.

[44]	A bit-choosing algorithm	Matlab	N/A	▪ Accuracy. ▪ Communication cost. ▪ Error rate.
[40]	A heuristic algorithm.	Matlab	Yelp dataset.	▪ The total number of records. ▪ Ratio.
[41]	A decentralized Blockchain	Hyperledger Fabric/ Identity Mixer technology.	Open source cloud platform Owncloud.	▪ Response time. ▪ Overhead.
[17]	Non-intrusive and integrated middleware	Prototype (Grafana, InfluxD)	3for2 office building in Singapore.	▪ Power Consumption.
[14]	Three-Pillar Framework.	Jboss Esb/ ONE-ITS [37]/ GoeEvent Server/ Apache Kafka/ Amazon Kinesis	Smooks framework	▪ Response Time. ▪ Ratio.
[1]	Well-designed IoT/CPS.	Java (LISP/ Connected Device Limited Configuration)	N/A	▪ Energy consumption.
[46]	PAD technique.	Keras / Tensorflow /Monte Carlo	OU44 plug load dataset	▪ Complexity. ▪ Trade-of. ▪ Response Time.

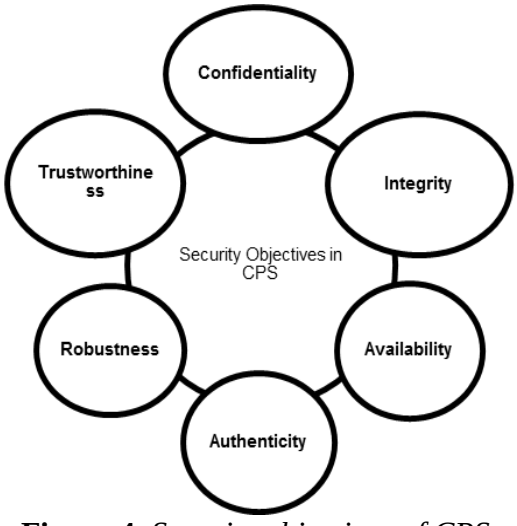

Figure 4. *Security objectives of CPS.*

- ***Confidentiality:*** The ability to prevent information and data from being exposed to any unauthorized person or group inside or outside the system. The privacy of data and data is protected by applying encryption algorithms to stored and forwarded data and limiting access to data locations [3]. In CPS, the protection of communications channels against eavesdropping will ensure confidentiality to prevent a system status that can occur due to eavesdropping. [6].
- ***Integrity:*** The ability to maintain information as it stands and stop improper manipulation. In other words, both the external and insiders who want to modify it must be kept away from the data. Thus, a destination gets the wrong data and treats it correctly. At CPS, integrity is guaranteed by taking all possible attacks to ruin the environmental objectives of CPS and by changing the data which the sensors gather and send.
- ***Availability:*** This is typically the system's ability to deliver services and goods on time. All subsystems are available so that they can work correctly and do their work on time and if necessary [3]. In other words, availability ensures that all CPS subsystems operate properly and avoids any kind of corruption such as hardware and software failures, power failures or attacks by DoS.
- ***Authenticity:*** This makes it easier to ensure that all parties involved in the CPS process. The validity of the genuine CPS must be realised in any subsystem and process [39].
- ***Robustness*** is the degree to which, even in case of limited disturbances, CPS may continue to operate appropriately. There are two types of failures: limited failure with limited consequences and sometimes low time impact crashes.
- ***Trustworthiness:*** It is how many people (for example, owner, user and individual) may use CPS to carry out the required tasks through various domain restrictions and time scales [5]. To be feasible and trusted for a CPS, the software, hardware, and data collection must all demonstrate confidence.

Cyber-physical systems (CPS) emerge; many uses have been used in this technique. This section summarizes some other applications in CPS. Lately,[50], Suggested 8C-CPS architecture for smart factory construction. The architecture is based on 5 levels of 5C architecture: communication, conversion, cybersecurity, cognition and configuration. As well,[51], the emphasis will be on CPSS device level optimization in the critical area of protection, energy consumption, reliability and user satisfaction, through using DVFS. A system of localization of a specific Automated Guided Vehicle (AGV), namely an LGV, that benefits by RSSI data, is presented in [52].

Technical Problems in Existing studies

In previous research, seven types of technical problems were encountered and shown in this section. The first category of technical problems that have been

addressed in many studies is the identification of CPS intrusions and irregularities by means of Intrusion Detection System (IDS) or ADS.

1. Detecting: The issues were how to detect anomalies in the ever-changing nature and lack of a precise model, also identify abnormal behaviour in the early attack stages and an early warning system in ICPS. However, in the waveform of normal data, there are many states, which can reduce prediction accuracy. Also, it may cause losses of property, and electricity loss, and damages to physical systems [29, 50]. The impacts of not reflecting the actual state of the CPS and irreparable damages to physical networks are addressed by [21], [30], since the system fails to detect run time data-oriented exploits against control programs, due to the lack of run time execution semantics checking and addressing anomalous transitions or time-intervals.
2. Security: The problem of identifying anomalies and at- tacks in a replicate of a water treatment plant that causes many false positives [48]. Potential sources of process anomalies are attacks, equipment errors, software design and coding errors as well as human error. Inconsistency and non-attack of the CPS component may lead to an in- variant generating an alert. Whereas, [29], [24] Based on how to detect attacks targeting noise or trouble-affected dynamic process processes, because the system cannot catch stealthy attacks and can lead the entire system to failure.
3. Monitoring: Monitoring problems could have a significant impact on CPS in terms of power consumption, price manipulation, high complexity, and cause considerable changes in demand. Nevertheless, [28], [33] studied the need for the ability to monitor the progression of the system, tracking relationships, issuing anomaly alerts to operators that ensure safe and high-quality pro- duction. Also, monitor and detect any misbehaving node and lethal attacks that could cause price manipulation addressed in [20].
4. Efficiency: Efficiency increases the capacity, storage, cost, processing and complexity limitations, which can lead to a high false alert rate. Though, [18] the number of transmissions that have a major impact on Embedded Sensor Networks (ESN) energy efficiency have been studied. In addition , improved performance on complexity, a compensation for CPS Supervisory Control and Data Acquisition (SCADA) systems are conducted by [49]. The study of [19] focus on reducing the number of process variables used by ICPS and reducing cost.
5. Failure: Failure issues in CPSs were obtained by several studies. For example, [36], [37] concentrate on achieving resilience against node or controller and also systematic failures and random hardware failures caused by malfunctioning behaviour. While [35] tried to solve the shortcoming of sensors and actuators, thus creating the void for data collection and action propagation. Like- wise, the work of [32] CPS argued that the fault tolerance is necessary to improve reliability even though faults exist. The mentioned above issues have impacts on CPSs such as data packets loss, system failure, and improves response time resource cost in which could cause total system breakdown and high complexity.

6. Privacy: The issues of privacy with the CPSs era that may bring up a serious impact on user's information when sharing/transmitting data for unauthorized access and data leak out. The work of [19], [41], [45] studied the problem of data aggregation while providing privacy-preserving and data leakage. As well, [49], [44] studied the need to provide a well-designed method for users to control their publishing actions in CPS was examined. Also, [36], [37], focusing on protecting sensitive information from illegal users and prevent data leakage from preserving user privacy.
7. Integration: Finally, a problem of integration systems was considered by several researchers to over- come the impacts that may lead to misinterpretation, low system performance, response time, and unsatisfactory data utility. While, [1], [14], [17] studied the lack of middle-ware integration and improve the quality and efficiency for direct interactions between physical subsystem enti- ties. The study of [46], [32] focused on the problem of High- dimensional streaming data that is often adding too much noise.

Proposed solutions in Existing studies

In this section, we explain the existing solutions in previous research studies. Table 1. shows the current techniques alongside used tools, datasets, and validation parameters to give a better understanding to readers who are new to the CPS environment. However, [25] Applied a CPS detection method for the detection of mutual exclusion failures of the control system and the detection of temporary functional losses and accidental reboots. A novel cross-layer anomaly detection system (ADS) developed in [27] to reduce the number of parameters sent to the central monitoring host and to derive a comprehensive system state. State-based IDS (SIDS) is proposed [21] to identify such anomalies as regular status, healthy transitions between standard rules and regular changes time intervals. The study [30] In order to detect irregular control programme behaviours mainly due to data dependent attacks on CPS, Orpheus provided that leverages the event driven nature in the characterisation of CPS control programme behaviours and eFSA model. The Cumulative Sum approach in [48] is used to classify irregularities in a water treatment plant replicate. In addition, entropy tests dependent on sensor tests and novelty sequences are applied in order to detect attacks on Gaussian linear systems for discrete time [29].

The work [24] introduces the zone partition algorithm that divides the physical states into several areas and extracts the zone function to observe the first rules in each zone. Moreover, the anomaly detection algorithm (KASE) that combines model-based and data-driven strategies presented in [28] to improve the computational complexity of inference and renders. The study [33], CPPS semantic fault analysis system was demonstrated to detect behavioral anomalies in a model-based approach and to predict a plant standard â continuous â discrete expression. A detection model based on Cumulative Sum (CUSUM) and an abnormal behavior detection algorithm developed by [20] for monitoring change detection and identify DoS attacks. The study [18] proposed

a new game model of attack-defense to detect malicious nodes using a repetitive method. A modern feature selection method based on a filter proposed [49] Based on the theory of Rough Set and the hyper-clique binary whale optimization algorithm (RST-HCBWoA), optimum reduction without loss of knowledge can be found. Moreover, a three-phase design strategy that involves sensitivity analysis, cross-associations and optimal IDS design will minimize the number of monitored parameters addressed in [19]. Another study [36] Proposed SDN fast controller failure recovery mechanism for multi-controller CPS fault tolerant. Likewise, A functional safety requirement verification (FSRV) and resource-cost-aware fault-tolerant optimization (RCFO) proposed in [37] to reduce the resource cost verify the technical safety requirement consisting of reliability and response time requirements. A model to describe the sensor model to represent sensors and actuators, and to create virtual objects that can regenerate data if physical devices fail introduced in [35]. Whereas [32] a multi-agent defect tolerant control architecture was developed to enhance dependability even in the case of defects. But, [44] proposed a bit-chosen algorithm which allows the untrusted aggregator to aggregate the physical environment data accurately and efficiently. Likewise, [40] proposed a new structure heuristic algorithm to address the issue of record publishing in CPSSs, taking account of user privacy and benefits. The study [41] suggested a reliable CPS generalized data provenance architecture and use the blockchain for data integrity privacy and manipulation detection. A non-intrusive middleware based on open-source building management tools are introduced [17] for future cities. The paper [14] Proposed a 3-pillar structure for the dynamic provision of integrated smart transportation system systems. A middleware architecture proposed in [1] for the changes in the functionality and cope with temporary faults at run-time. The study [46] extended PAD to nonlinear functionality to increase the utility and remain highly vulnerable to privacy threats.

4. Discussion

The purpose of this study is to bring up to date the cyber-physical system infrastructure and highlight trends in research on the subject. Our extensive survey focuses rather than the applications themselves on previous articles on CPS security and privacy applications. We also provide a taxonomy for researchers of things related to this topic.

A taxonomy based on literature may have many advantages. An organization produces a taxonomy on different publications. The large number of papers on the subject in which there is no organizational structure and the actual practices in the field are not appropriately understood is likely to be resolved by a new researcher interested in CPS / ICPS security trends. In an introductory perspective, several articles discuss the subject, while others discuss selected technologies already in place. The provision of a taxonomy assists with a meaningful, manageable, coherent framework for the various literary works and activities. A taxonomy may also provide a wide range of insights into a topic to researchers.

First, a taxonomy may be used to evaluate possible research directions in a specific field. This research on the taxonomy of cyber-physical systems aims to inspire researchers to concentrate on this kind of application that is driving a new trend in this field. Other research directions defined in the taxonomy involve evaluating current applications or sharing the experience with real applications. Second, a taxonomy enables future scientists to detect literature gaps in a specific subject. We highlight some of the critical aspects of cyber-physical systems, such as privacy, security, confidentiality, control of access, etc., which researchers have been very attentive compared to traditional technologies. These works may include a development paper, a comparative analysis or an outline, for instance, for detecting CPS protection and device failures. The following sections address the articles included in the analysis to help research into cyber-physical system security , privacy and even failure detection and alert software to technology users' challenges and some primary future research to avoid these issues.

A. Limitations

The research advances can be speeded up by identifying limitations, and future directions in several industries and by supporting collaborative multidisciplinary research between academia and industry. There are several limitations remained open as shown below:

- **Privacy Control:** For smart buildings and clever cities IoT gathers user activity with or without an identification. It is important to preserve, publish, store and use the data collected in buildings and cities. A mechanism for protecting the privacy and controlling data flows should be provided by the middle ware itself to fulfill developer or user privacy requirements. CPS / IoT systems should be subject to the privacy control policy defined in the middle ware. A machine-readable privacy control representation was therefore missing, and all participating de- vices in the system should be defined to follow [1], [12]. Access Control Policy provides authorizations for access to data resources or devices similar to the Privacy Control Policy. Data obtained in smart city and smart cities are available in location and time. Consequently, access checks should include not only the data collection services, but also other features, including location and time, in order to allow data access [1].
- **Scalability:** The devices and services in buildings and cities in one building or one city can be more than tens or hundreds of thousands. Services of this size cannot be designed as one service with complex links be- tween service components and complex connectivity be- tween devices. It is therefore desirable on middleware that one service should be designed for devices of the same kind and the service should be deployed on all de- vices in buildings and cities. According to various rules, the links between services must be connected by middle- ware. An example can be an intelligent smoke detector that can provide the right direction of evacuation according to the data collected in the same building by other smoke detectors. Naturally, the data flow connections between smoke

detectors depend on the location. The middleware can, therefore, connect the devices installed nearby automatically to share data collected [1].

- **Service management:** The management of services per- formed in a single system on thousands or hundreds of thousands of devices is challenging. Not every device has the above capabilities in the CPS / IoT systems. Many devices have limited communication ability, with certain devices available only at certain times due to limited energy resources. The smart CPS / IoT middleware building / smart city should be able to control system services remotely and handle it. Thus, fail-services can be detected and replaced for short-term faults, whether in hardware or software, and when the configuration or specifications change, services can be replaced with a minimal overhead management level [1].
- **Lack of Integration:** The feedback received showed the lack of embedded middleware in common concern. Other findings include the lack of connectivity between different buildings, the lack of useful view of data from energy end users, the ability to compare and compare certain building efficiency ratings on the online dash- board [17]..
- **Confidentiality:** Most IDSs for vehicles largely have omitted security threats related to confidentiality. This is due to two reasons. The greater the accessibility, the location of your address books and even your biometrics, the greater the risk to the privacy of passengers or drivers. Second, current INSs depend heavily on physical effects, such as a UAV deviation from the classification or excessive energy consumption in a robotic vehicle which could lead to a breach of security. How- ever, violations of confidentiality do not require physical signs and so it is not possible to identify strategies that rely heavily on physical monitoring [23]. Thus, IDS techniques should focus less on physical features and waiting for the physical manifestation of an attack, and more on the search for (cyber) traces of earlier attack phases (for instance, testing or trying to install malware). However, methods based on signatures use a database or fixed signatures to recognize attacks and usually work with the attempts of known intrusion. However, they do not detect new or unknown attacks because of their nature. Integrating the cyber and physical domains considerably reduces the isolation from the outside world of the physical system, increasing its vulnerabilities and causing some cybersecurity problems [24].
- **Availability and Reliability:** The unavailability of ser- vice or information could seriously influence the business of customers. In communications between de- vices such as sensors, actuators etc. it is therefore necessary to include security mechanisms in order to enhance data protection and data security [53]. A wide range of devices, systems, components, and systems combined leads to decentralized security disruption in- put points. Security, property verification, and the expected comportment of the system require a regular re- assessment [53] . System users and network resources need a reliable environment to exchange information and services. In the CPS environment, the development of a

trustworthy defect tolerant system must ensure the protection of communications, how integration and confidentiality can be ensured, authenticity, control of access, permission, etc. A lack of data integrity and privacy could lead to a failure of the CPS system.

- **Security and Privacy:** As always, security, privacy, and confidence are the main concerns for all modern technologies. However, for the processing unit, CPS data volume could be heavily loaded. The block chain needs to manage frequent data records and to manage larger data sets over a short period to handle multiples compete for data streams and operating records. However, the Blockchain-based architecture requires time costs for both Block mining and a Consensus system; during the construction, sharing and storage phase data from various CPS areas are formatted differently. Data sent through numerous subsystem boundaries are much more difficult to process, understand and handle. The interoperability of the data is a challenging challenge for the integration of the blockchain and in particular the logic of the blockchain program [41]. The public existence of blockchain architecture in the business and customer sector presents a huge challenge in coping with sensitive data. Security measures are needed to ensure that only permitted access can be given and that the privacy of the user is not at risk. Some blockchain implementations, such as the Hyperledger sup-port framework, provide a remote communication tool, but also add the risk of data leakage when using the channel [42].

Since a multi-agent CPS consists of a network of sensors, driving units, and calculation nodes connected via communication canals, this system presents numerous attack surfaces from a security point of view. Software and physical attacks can be attracted to direct attacks on such systems as to la- tent vulnerabilities. Here we mean traditional cyber-attacks by software attacks that target a CPS agent's communication with its external world, seeking to seriously damage the avail- ability, corrupt data integrity, or lose its data privacy. Physical attacks represent an adverse reaction that either learns the system's internal physical condition by monitoring its in- put/output behavior, by injecting commands or controlling activities to change its internal physical state, or by using actual physical phenomena to cause unsafe behavior [47].

B. Future Directions

We give briefly future directions that mitigate the challenges facing developer/design, researchers, and factories and facilitate the use in a variety of technologies (e.g. intrusion detection, anomaly detection, security & privacy, etc.) to ensure a secure industry CPS as it shown in Figure 5.

1. Directions to Developers

Studies in the CPS have shown a range of suggestions for the improvement of the CPS recommendations relating to cyber and integrated physical systems. To reduce energy consumption, improve the security of buildings and cities, or

in- crease comfort in buildings, the development of prototype or business services is necessary for two scenarios [1]. Integration of robust reliability mechanisms to enable IoT to monitor sensors and services throughout their lives to address any inconsistencies that result from unexpected operational failures [14]. To test an overview, zoom, and filter, a detailed-on request concept where users can select different nodes in the hierarchy and expand these level by level, a node visualization prototype should be examined [17]. An embedded scenario can be used to protect the information and further guarantee ESN security in the CPESs by a game-theoretical IDS [21], [22]. To correctly correlate and analyze false positives (FPs), an application is needed to test behavioral intrusion detection on CPSs for the whole Secure Water Treatment (SWaT) testbed [48]. A proof-of-concept prototype is also still not provided to show the scalability of the CPS control on program dimensions and complexity [30]. To understand the components by well-known physics and electric power law, the real-time dashboard and the alerting system aid, and the increased anomaly detection process would help [28]. It is needed to integrate cyber information and physical intrusion detection functionality in ICPSs [24]. It is essential to develop more sensors, more hardware failures, and ways to create advanced attack vectors that penetrate CPS defense and the ability to test a cyber-attack resilient FCS [34]. CPS based on Blockchain can be deployed in an emulated smart grid environment, and the performance can be evaluated [41].

2. Directions to Researchers

Recommendations for researchers in specific fields in this section are provided. First, there is no readable machine representation of the privacy management in the CPS, and all participating devices in the system should be defined to be followed [1], [17], [54]. The smart system and the smart - city middleware CPS / IoT should be able to track and administer services on devices remote [1]. Besides, it should be better to solve inconsistencies caused by unexpected failures in operation by integrating more robust confidence assurance mechanisms that IoT monitors sensors and services through- out their life cycle [14]. A semi-empirical model for arrays can be used for rapid assessing the energy system, the quality of ranges (e.g., module flaws, faults, etc.) [16]. Lethal attacks to the power grid, including load-redeployment and jamming attacks should be addressed [20]. Anomalies in the sensor measurement should be addressed over time [22] . Also, anticipate IDS techniques should emphasize features less and wait for physical manifestation and seek (cyber) traces of previous attack stages (e.g., testing or trying to install [23] malware). Anomalies that are frequently detected and clusters can be overcome by using Principal Component Analysis (PCA) and forest insulation methods [25]. Support the integrated action for fine-graining detection of anomalies at the instructions level without using the Orpheus design paradigm to trace facilities [30]. Distributed optimization and adaptive learning are needed to improve the formulation of the problem of entropy transfer into an issue of adaptive estimation [29]. The use of semantic-based meta-modeling languages for

virtualization and data regeneration can provide a technically sound solution for sensors [35].

The protection of the privacy of users should be addressed when sharing their physical data with others in CLASs [40]. More security functions, such as mutual authentication and data coordination from multiple body-wearing sensors, should be considered [47]. Scientists should also explore trade-offs between multiple privacy dataset releases and the privacy vulnerabilities of possible linkage and correlation attacks [46].

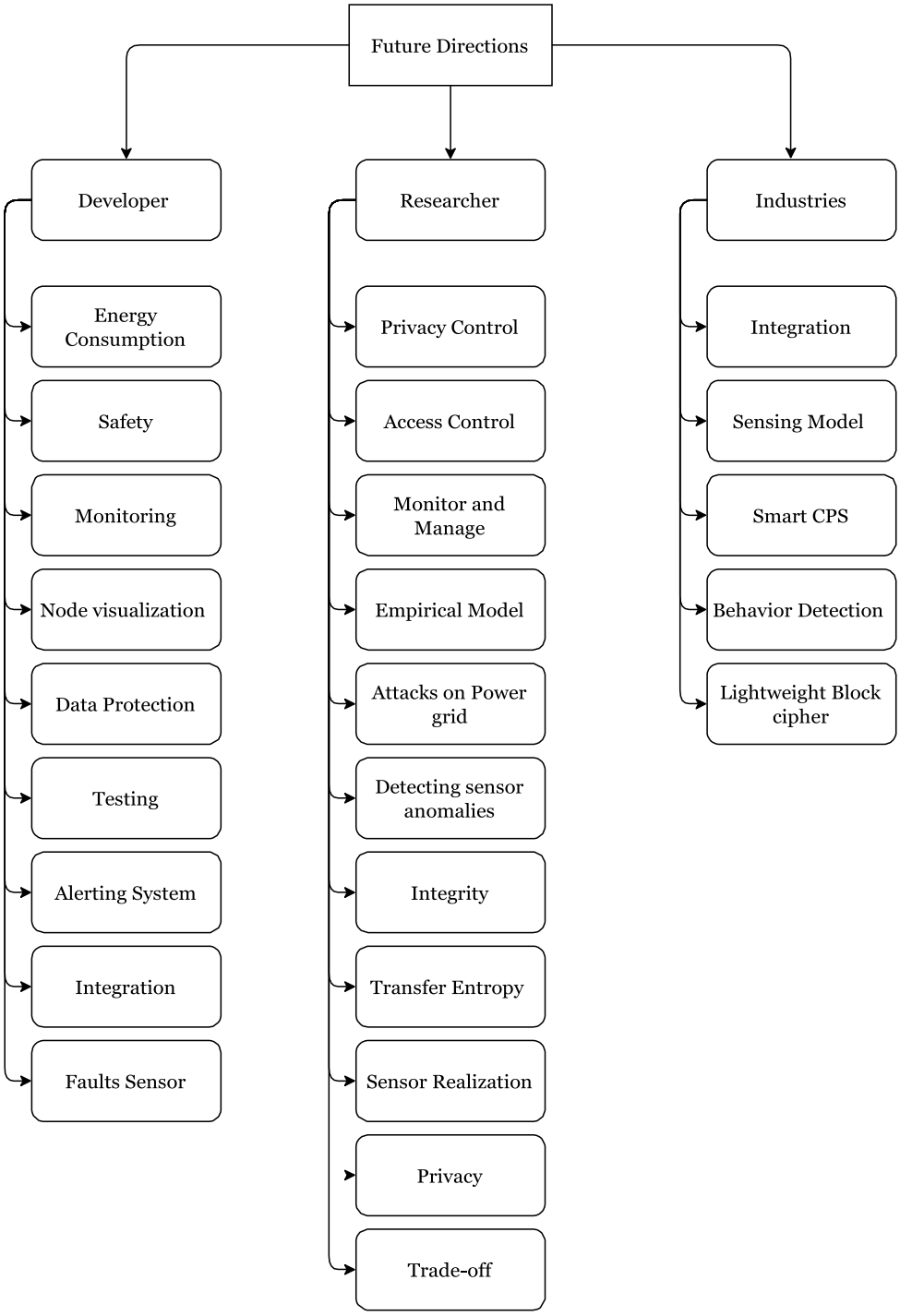

Figure 5. Further Research Directions.

3. Directions to Industries

This section introduces critical guidelines for various industries and factories in the field of research. Most of the recommendations concern security, data protection, CPS, and technology for secure communications. First, future research on cyber information integration and the physical functionality for ICPS intrusion detection should be studied in the CPSs environment [24]. Conduct

further experiments on the definition sensing system for reinforcement sensing by
considering specific industrial uses within the scope of the VF- OS project [35]. A new study could study the confidentiality in the CPS architecture to build the CPS for intelligent factories so that the CPS is confidential [50]. Industrial may use the method of anomaly detection for deficient ICS device behavior [55]. The implementation of lightweight block cipher on the WIA-FA hardware platforms should also be considered under the specific requirements for factory automation [56].

5. Conclusion and Limitation of Study

The study provided a clear literary review, focusing mainly on the security applications of CPS in a systematic way. The data was collected from the full-text screening, based on a well-defined inclusion and exclusion test of 58 journal articles. For the general data analysis of keyword and journals and the particular data analysis, the contents of these articles had been used. Based on the discussion of their works, the importance of this study was underlined. It contains CPS open challenges based on the literature articles, as well as future research future directions. The limitations of the present study were examined. In addition to the above contributions, the limitations of this work should be noted. The number and Identity of Source Databases are the most applicable limit in this survey, although the sources selected to represent an ex- tensive and useful collection. Besides, rapid progress in this area does not make a study timely. In addition , research activities do not generally expose the reality of the use of protective systems or the effect that this research has on the research community.

References

C.-S. Shih, J.-J. Chou, N. Reijers, and T.-W. Kuo, "Designing CPS/IoT applications for smart buildings and cities," *IET Cyber-Physical Syst. Theory Appl.*, vol. 1, no. 1, pp. 3–12, 2016.

H. Xu, W. E. I. Yu, D. Griffith, and N. Golmie, "A Survey on Industrial Internet of Things : A Cyber-Physical Systems Perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

G. A. Fink, T. W. Edgar, T. R. Rice, D. G. MacDonald, and C. E. Crawford, *Security and Privacy in Cyber-Physical Systems*. Elsevier Inc., 2016.

J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and Privacy in Cyber-Physical Systems: A Survey of Surveys," *IEEE Des. Test*, vol. 34, no. 4, pp. 7–17, 2017.

S. Majumder, A. Mathur, and A. Y. Javaid, *Cyber-Physical System Security Controls: A Review*, Chapter 8. 2019.

C. Science, "Security and Privacy of Cyber-Physical Systems," *Electron. Thesis or Diss.*, 2018.

X. Huang, Y. Zhang, Y. Liu, and Z. Hu, "Effect of small amount of nitrogen on carbide characteristics in unidirectional Ni-base superalloy,"

Metallurgical and Materials Transactions A: Physical Metallurgy and Materials Science, vol. 28, no. 10. pp. 2143–2147, 1997.

P. H. Nguyen, S. Ali, and T. Yue, "Model-based security engineering for cyber-physical systems : A systematic mapping study," *Inf. Softw. Technol.*, vol. 83, pp. 116–135, 2017.

J. Barbosa, P. Leitao, D. Trentesaux, A. W. Colombo, and S. Karnouskos, "Cross Benefits from Cyber-Physical Systems and Intelligent Products for Future Smart Industries," *2016 Ieee 14Th Int. Conf. Ind. Informatics*, pp. 504–509, 2016.

P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, "Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," *Living Internet Things Cybersecurity IoT - 2018*, pp. 3 (9 pp.)-3 (9 pp.), 2018.

B. O. Cheng, J. Zhang, and G. P. Hancke, "Industrial Cyberphysical Systems," *Living Internet Things Cybersecurity IoT - 2018*, no. March, pp. 25–35, 2018.

R. B. and H. Gill, "Cyber-Physical Systems," *IEEE Access*, vol. 12, no. 1, 2011.

S. Gujrati, H. Zhu, and G. Singh, "Designing cyber-physical systems middleware for smart cities applications," *Proc. Work. Progr. 19th Int. Conf. Distrib. Comput. Netw. - Work. ICDCN '18*, pp. 1–6, 2018.

M. Elshenawy, B. Abdulhai, and M. El-Darieby, "Towards a service-oriented cyber–physical systems of systems for smart city mobility applications," *Futur. Gener. Comput. Syst.*, vol. 79, no. 2, pp. 575–587, 2018.

M. Schmidt and C. Åhlund, "Smart buildings as Cyber-Physical Systems: Data-driven predictive control strategies for energy efficiency," *Renew. Sustain. Energy Rev.*, vol. 90, no. April, pp. 742–756, 2018.

S. Vinco, L. Bottaccioli, E. Patti, A. Acquaviva, and M. Poncino, "A Compact PV Panel Model for Cyber-Physical Systems in Smart Cities," *2018 IEEE Int. Symp. Circuits Syst.*, no. i, pp. 1–5, 2018.

B. Kalluri, C. Miller, B. Seshadri, and A. Schlueter, *A Cyber-Physical Middleware Platform for Buildings in Smart Cities*. Springer International Publishing, 2018.

K. Wang, M. Du, D. Yang, C. Zhu, J. Shen, and Y. Zhang, "Game-Theory-Based Active Defense for Intrusion Detection in Cyber-Physical Embedded Systems," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 1, pp. 1–21, 2016.

P. Haller and B. Genge, "Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems," *IEEE Access*, vol. 5, pp. 9336–9347, 2017.

M. Attia, S. M. Senouci, H. Sedjelmaci, E. H. Aglzim, and D. Chrenko, "An efficient Intrusion Detection System against cyber-physical attacks in the smart grid," *Comput. Electr. Eng.*, vol. 68, no. May, pp. 499–512, 2018.

A. Khalili, A. Sami, A. Khozaei, and S. Pouresmaeeli, "SIDS: State-based intrusion detection for stage-based cyber physical systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 22, pp. 113–124, 2018.

H. Sadreazami, A. Mohammadi, A. Asif, and K. N. Plataniotis, "Distributed-Graph-Based Statistical Approach for Intrusion Detection in Cyber-Physical Systems," *IEEE Trans. Signal Inf. Process. over Networks*, vol. 4, no. 1, pp. 137–147, 2018.

G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Networks*, vol. 84, pp. 124–147, 2019.

J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 5, pp. 4257–4267, 2018.

Y. Harada, Y. Yamagata, O. Mizuno, and E. H. Choi, "Log-based anomaly detection of CPS using a statistical method," *Proc. - 8th IEEE Int. Work. Empir. Softw. Eng. Pract. IWESEP 2017*, pp. 1–6, 2017.

B. Belchev and M. A. Walton, "Anomaly Detection in Cyber Physical Systems using Recurrent Neural Networks," *2017 IEEE 18th Int. Symp. High Assur. Syst. Eng.*, pp. 140–145, 2017.

H. Sandor, B. Genge, P. Haller, A. V. Duka, and B. Crainicu, "Cross-layer anomaly detection in industrial cyber-physical systems," *2017 25th Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2017*, 2017.

N. Muralidhar *et al.*, "Illiad: InteLLigent Invariant and Anomaly Detection in Cyber-Physical Systems," *ACM Trans. Intell. Syst. Technol.*, vol. 9, no. 3, pp. 35:1--35:20, 2018.

D. Shi, Z. Guo, K. H. Johansson, and L. Shi, "Causality Countermeasures for Anomaly Detection in Cyber-Physical Systems," *IEEE Trans. Automat. Contr.*, vol. 63, no. 2, pp. 386–401, 2018.

L. Cheng, K. Tian, Danfeng, Yao, L. Sha, and R. A. Beyah, "Checking is Believing: Event-Aware Program Anomaly Detection in Cyber-Physical Systems," *arXiv e-prints*, pp. 1–15, 2018.

M. Broy, "Safety-critical, dependable and fault-tolerant cyber-physical systems," *Cyber-Physical Syst. Next-Generation Networks*, vol. 14, pp. 54–78, 2018.

R. B. Roxana and D. Eva-Henrietta, "Fault-tolerant Control of a Cyber-physical System," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 261, no. 1, 2017.

I. Zinnikus *et al.*, "Integrated semantic fault analysis and worker support for cyber-physical production systems," *Proc. - 2017 IEEE 19th Conf. Bus. Informatics, CBI 2017*, vol. 1, pp. 207–216, 2017.

T. Bakker, M. T. Leccadito, and R. H. Klenke, "Flexible FPGA based Hardware In the Loop Simulator for Control, Fault-Tolerant and Cyber-Physical Systems," *55th AIAA Aerosp. Sci. Meet.*, no. January, pp. 1–12, 2017.

S. Ghimire, J. Sarraipa, C. Agostinho, and R. Jardim-Goncalves, “Fault tolerant sensing model for cyber-physical systems,” *Simul. Ser.*, vol. 49, no. 7, pp. 104–112, 2017.

S. Yoon, J. Lee, Y. Kim, S. Kim, and H. Lim, “Fast controller switching for fault-tolerant cyber-physical systems on software-defined networks,” *Proc. IEEE Pacific Rim Int. Symp. Dependable Comput. PRDC*, pp. 211–212, 2017.

G. Xie, J. An, R. Li, G. Zeng, and K. Li, “Resource-Cost-Aware Fault-Tolerant Design Methodology for End-to-End Functional Safety Computation on Automotive Cyber-Physical Systems,” *ACM Trans. Cyber-Physical Syst.*, vol. 3, no. 1, 2018.

S. Guo and D. Zeng, *Cyber-Physical Systems : Architecture , Security and application*. 2019.

F. AlDosari, “Security and Privacy Challenges in Cyber-Physical Systems,” *J. Inf. Secur.*, vol. 08, no. 04, pp. 285–295, 2017.

X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li, “Follow but No Track: Privacy Preserved Profile Publishing in Cyber-Physical Social Systems,” *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1868–1878, 2017.

X. Liang, S. Shetty, D. K. Tosh, J. Zhao, D. Li, and J. Liu, “A reliable data provenance and privacy preservation architecture for business-driven cyber-physical systems using blockchain,” *Int. J. Inf. Secur. Priv.*, vol. 12, no. 4, pp. 68–81, 2018.

B. B. B, J. V Deshmukh, and M. Pajic, *Opportunities and Challenges in Monitoring Cyber-Physical Systems Security*, vol. 11247. Springer International Publishing, 2018.

M. Keshk, N. Moustafa, E. Sitnikova, and B. Turnbull, “Privacy-preserving big data analytics for cyber-physical systems,” *Wirel. Networks*, vol. 5, 2018.

J. Yu, K. U. N. Wang, D. Zeng, C. Zhu, and S. Guo, “Privacy-preserving Data Aggregation Computing in Cyber-Physical Social Systems,” *ACM Trans. Cyber-Physical Syst.*, vol. 3, no. 1, 2018.

A. Mohammadi, P. Cheng, V. Piuri, K. N. Plataniotis, and P. Campisi, “Guest Editorial Distributed Signal Processing for Security and Privacy in Networked Cyber-Physical Systems,” *IEEE Trans. Signal Inf. Process. over Networks*, vol. 4, no. 1, pp. 1–3, 2018.

F. C. Sangogboye, R. Jia, T. Hong, C. Spanos, and M. B. Kjærgaard, “A Framework for Privacy-Preserving Data Publishing with Enhanced Utility for Cyber-Physical Systems,” *ACM Trans. Sens. Netw.*, vol. 14, no. 3, pp. 1–22, 2018.

J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, “Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system,” *Futur. Gener. Comput. Syst.*, 2018.

J. Goh, S. Adepu, M. Tan, and Z. S. Lee, “Anomaly detection in cyber physical systems using recurrent neural networks,” *Proc. IEEE Int. Symp. High Assur. Syst. Eng.*, pp. 140–145, 2017.

S. Priyanga, M. R. Gauthama Raman, S. S. Jagtap, N. Aswin, K. Kirthivasan, and V. S. Shankar Sriram, "An improved rough set theory based feature selection approach for intrusion detection in SCADA systems," *J. Intell. Fuzzy Syst.*, vol. 36, no. 5, pp. 3993–4003, 2019.

J. R. Jiang, "An improved Cyber-Physical Systems architecture for Industry 4.0 smart factories," *Proc. 2017 IEEE Int. Conf. Appl. Syst. Innov. Appl. Syst. Innov. Mod. Technol. ICASI 2017*, vol. 10, no. 300, pp. 918–920, 2017.

J. Zeng, L. T. Yang, M. Lin, Z. Shao, and D. Zhu, "System-Level Design Optimization for Security-Critical Cyber-Physical-Social Systems," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 2, pp. 1–21, 2017.

L. Cavanini *et al.*, "A Preliminary Study of a Cyber Physical System for Industry 4.0: Modelling and Co-Simulation of an AGV for Smart Factories," *2018 Work. Metrol. Ind. 4.0 IoT, MetroInd 4.0 IoT 2018 - Proc.*, pp. 169–174, 2018.

W. Wolf, "Cyber-physical Systems," *Computer (Long. Beach. Calif).*, vol. 42, no. 3, pp. 88–89, 2009.

M. Schmidt and C. Åhlund, "Smart buildings as Cyber-Physical Systems: Data-driven predictive control strategies for energy efficiency," *Renew. Sustain. Energy Rev.*, vol. 90, no. March 2017, pp. 742–756, 2018.

M. Kravchik and A. Shabtai, "Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks," *Proc. 2018 Work. Cyber-Physical Syst. Secur. Priv. - CPS-SPC '18*, no. 1, pp. 72–83, 2018.

C. Pei, Y. Xiao, W. Liang, and X. Han, "Trade-off of security and performance of lightweight block ciphers in Industrial Wireless Sensor Networks," *Eurasip J. Wirel. Commun. Netw.*, vol. 2018, no. 1, 2018.